Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Date de création : 18-06-2025

Projet de loi 8395

Projet de loi
1) relatif à la valorisation des données dans un environnement de confiance ;
2) relatif à la mise en oeuvre du principe « once only » ;
3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;
4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Date de dépôt : 12-06-2024
Auteur(s) : Madame Stéphanie Obertin, Ministre de la Digitalisation

Liste des documents

Date	Description	Nom du document	Page
12-06-2024	Déposé	20250515_Depôt	3
23-10-2024	Avis de la Chambre des Fonctionnaires et Employés publics (21.10.2024)	20250514_Avis	80
25-10-2024	Avis de la Chambre des Salariés (23.10.2024)	20250514_Avis_2	85
30-10-2024	Avis de l'Ordre des Architectes et des Ingénieurs-Conseils (28.10.2024)	20250514_Avis_4	98
23-12-2024	Avis de la Commission nationale pour la protection des données (20.12.2024)	20250515_Avis_2	103
06-01-2025	Avis de la Chambre de Commerce (6.12.2024)	20250515_Avis	136
07-01-2025	Avis de la Chambre des Métiers (7.1.2025)	20250514_Avis_3	149
23-04-2025	Amendements adoptés par la/les commission(s) : Commission de l'Enseignement supérieur, de la Recherche et de la Digitalisation	20250522_AmendementParlementaire	162
29-04-2025	Avis du Syndicat des Villes et Communes Luxembourgeoises (31.3.2025)	20250516_Avis	203
15-05-2025	Avis d’une chambre professionnelle : Chambre d'Agriculture (12.5.2025)	20250515_Avis_3	212

20250515_Depôt

Nº 8395

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

Document de dépôt

Dépôt: le 11.6.2024

*

Le Premier ministre,

Vu les articles 76 et 95, alinéa 1er, de la Constitution ;

Vu l'article 10 du Règlement interne du Gouvernement ;

Vu l'article 58, paragraphe 1er, du Règlement de la Chambre des Députés ;

Vu l'article 1er, paragraphe 1er, de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État ;

Considérant la décision du Gouvernement en conseil du 5 juin 2024 approuvant sur proposition de la Ministre de la Digitalisation le projet de loi ci-après ;

Arrête :

Art. 1er. La Ministre de la Digitalisation est autorisée à déposer au nom du Gouvernement à la Chambre des Députés le projet de loi

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvredu principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

et à demander l'avis y relatif au Conseil d'État.

Art. 2. La Ministre déléguée auprès du Premier ministre, chargée des Relations avec le Parlement est chargée, pour le compte du Premier ministre et de la Ministre de la Digitalisation, de l'exécution du présent arrêté.

Luxembourg, le 11 juin 2024

Le Premier ministre,
Luc FRIEDEN

La Ministre de la Digitalisation,
Stéphanie OBERTIN

*

TITRE I^er^ – Dispositions préliminaires

Art. 1. Objet

(1) La présente loi vise :

1° le traitement de données à caractère personnel par les entités publiques dans le cadre de l'exécution des missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies, agissant en leur qualité de responsable du traitement ;

2° l'échange d'informations et de données à caractère personnel obtenues par une entité publique auprès d'une autre entité publique dans le cadre du traitement d'une demande ou d'une déclaration d'un administré, ou pour informer l'administré sur ses droits au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir lui attribuer éventuellement lesdits prestations ou avantages ;

3° le traitement ultérieur de données à caractère personnel par les entités publiques pour les finalités déterminées dans la présente loi ;

4° l'accès et la réutilisation de certaines catégories de données collectées par les organismes du secteur public, en application du chapitre II du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), désigné ci-après par le terme « règlement (UE) 2022/868 » ;

5° la fourniture de services d'intermédiation de données, en application du chapitre III du règlement (UE) 2022/868 ; et

6° la mise à disposition de données à des fins altruistes, en application du chapitre IV du règlement (UE) 2022/868.

(2) Les dispositions de la présente loi s'appliquent sans préjudice des dispositions plus spécifiques relatives au traitement de données à caractère personnel.

Art. 2. Définitions

(1) Sauf dispositions particulières contraires au paragraphe 2 du présent article, les termes et expressions utilisés dans la présente loi ont la signification que leur donnent le règlement (UE) 2022/868 et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre

circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après désigné par le terme « règlement (UE) 2016/679 ».

(2) Aux fins de la présente loi, on entend par :

1° « anonymisation » : le processus consistant à rendre anonymes des données à caractère personnel de telle sorte que la personne concernée à laquelle celles-ci se rapportent ne soit pas ou plus identifiée ou identifiable, compte tenu de l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique directement ou indirectement ;

2° « entité publique » : un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal aux fins d'application des dispositions des titres IV et V. Toutefois, ne sont pas considérées comme entité publique aux fins d'application de la présente loi :

a) les autorités compétentes visées par l'article 2, point 7° de loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale lorsqu'elles effectuent un traitement de données à caractère personnel relevant du champ d'application de la loi du 1er août 2018 ;

b) les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif, lorsqu'elles effectuent un traitement de données à caractère personnel dans l'exercice de leurs fonctions juridictionnelles ;

3° « tiers de confiance » : toute entité fonctionnellement indépendante des entités publiques visées au titre V, des organismes du secteur public détenant les données et du réutilisateur de données visés au titre VI, qui remplit les conditions prévues à l'article 6.

TITRE II – Traitement de données à caractère personnel par les entités publiques nécessaire à l'exécution de la mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Art. 3. Licéité du traitement de données à caractère personnel par les entités publiques nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Les entités publiques sont habilitées à traiter les données à caractère personnel nécessaires aux fins relevant de l'exécution de leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies par une disposition de droit de l'Union européenne ou de droit national applicable.

TITRE III – Acteurs compétents en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données

Art. 4. Autorité des données

(1) Le Commissariat du Gouvernement à la protection des données auprès de l'État est chargé des missions attribuées à l'Autorité des données par la présente loi. Dans l'exercice de ces missions, le Commissariat du Gouvernement à la protection des données auprès de l'État est désigné ci-après par le terme « Autorité des données ».

(2) L'Autorité des données est désignée organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868, habilité, conformément à l'article 7, paragraphe 2, du même règlement, à octroyer ou refuser l'accès aux fins de réutilisation des données conformément aux dispositions des titres VI et VII.

(3) L'Autorité des données est habilitée à autoriser ou refuser le traitement ultérieur de données à caractère personnel par les entités publiques conformément aux dispositions des titres V et VII.

(4) L'Autorité des données a pour missions :

a) de mettre en œuvre les missions lui conférées par la présente loi ;

b) de collaborer étroitement avec le Centre des technologies de l'information de l'État, dénommé ci-après par le terme « Centre », le tiers de confiance mandaté par le Centre et le groupement d'intérêt économique PNED G.I.E. – Plateforme nationale d'échange de données, désigné ci-après par le terme « LNDS » ;

c) de fonctionner comme organe de réflexion et d'impulsion dans le domaine du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation de données et de formuler des avis et des propositions en la matière au ministre ayant la digitalisation dans ses attributions ;

d) de proposer au ministre ayant la digitalisation dans ses attributions des mesures en matière de politique de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données ;

e) de conseiller, sur demande, le ministre ayant la digitalisation dans ses attributions sur les mesures en matière de traitement ultérieur de données à caractère personnel ;

f) de promouvoir les bonnes pratiques à travers les entités publiques, en matière de traitement ultérieur de données à caractère personnel, et à travers les organismes de droit public en matière d'accès et de réutilisation de données ;

g) de sensibiliser les entités publiques, les organismes de droit public et le public en matière de traitement ultérieur de données à caractère personnel et en matière d'accès et de réutilisation de données.

(5) L'Autorité des données dispose des ressources nécessaires pour exercer ses missions. Elle peut recourir aux services d'experts.

(6) L'Autorité des données veille à ce que son personnel chargé des missions prévues aux paragraphes 2 et 3 ne soit pas impliqué dans la préparation des demandes visées à la section II du titre VII dans l'exercice de ses missions prévues aux articles 57 et 58 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Art. 5. Assistance technique

(1) Le Centre et le LNDS, sont désignés organismes compétents au sens de l'article 7, paragraphe 1er, du règlement (UE) 2022/868 pour aider l'Autorité des données dans l'exercice de ses missions conformément aux dispositions de la présente loi.

(2) Le Centre a pour missions :

a) de mettre en œuvre les missions lui conférées par la présente loi ;

b) de mettre à disposition l'environnement de traitement sécurisé prévu à l'article 36 ;

c) de fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles ;

d) de s'assurer de la mise en œuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou à de modification, d'agrégation, de suppression et de traitement des informations et données selon toute autre méthode de contrôle de la divulgation des données conformément au plan de confidentialité, préalablement à la mise à disposition des données dans l'environnement de traitement sécurisé ;

e) de collaborer étroitement avec l'Autorité des données, le tiers de confiance mandaté par le Centre, et le LNDS ;

f) de proposer, sur décision du ministre ayant le Centre dans ses attributions, des services au LNDS relatifs à la mise en œuvre des dispositions de la présente loi.

(3) Le LNDS a pour missions :

a) de mettre en œuvre les missions lui conférées par la présente loi ;

b) d'aider les organismes du secteur public, le cas échéant, à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des

détenteurs de données conformément à leurs décisions spécifiques, y compris en ce qui concerne le territoire où le traitement des données est prévu et à aider les organismes du secteur public à mettre en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation des réutilisateurs, lorsque cela est réalisable en pratique ;

c) de fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur en vertu de l'article 5, paragraphe 10 du règlement (UE) 2022/868 ;

d) de collaborer étroitement avec l'Autorité des données, le Centre et le tiers de confiance mandaté par le Centre ;

e) de fournir, sur demande, une assistance aux entités publiques et aux réutilisateurs de données dans le cadre de la préparation des demandes visées aux articles 27 et 28 et du plan de confidentialité visé à l'article 35.

(4) Le Centre et le LNDS :

a) veillent à ce que le personnel chargé des missions conférées par la présente loi soit fonctionnellement indépendant des entités publiques visées au titre V, des organismes du secteur public détenant les données et des réutilisateurs de données visés au titre VI ;

b) ne divulguent aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données ou permettant la divulgation de données qui sont protégées pour des motifs de protection des données à caractère personnel, de confidentialité commerciale, y compris le secret d'affaire, le secret professionnel, et le secret d'entreprise, de secrets statistique ou de protection de droits de propriété intellectuelle de tiers. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation ;

c) désignent le personnel chargé des missions qui leurs sont conférées par la présente loi. Le personnel est désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données ;

d) veillent à ce que le personnel chargé des missions qui leurs sont conférées par la présente loi ne soit pas chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données visés par la présente loi ;

e) veillent à ce que le personnel chargé des missions qui leurs sont conférées par la présente loi n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui leurs sont conférés par la présente loi ou s'il y a incompatibilité, de fait ou de droit, avec l'exercice des tâches qui leurs sont conférées en application de la présente loi.

(5) Il est interdit au personnel du Centre et du LNDS chargé de l'exécution des missions qui leurs sont conférées par la présente loi d'avoir un intérêt quelconque, par lui-même ou par personne interposée, et sous quelque forme juridique que ce soit, dans une entité publique, dans un organisme du secteur public détenant les données ou dans un réutilisateur de données visées aux titres V et VI.

(6) Sans préjudice de l'article 23 du Code de procédure pénale, le personnel du Centre, du LNDS et du tiers de confiance chargé de l'exécution des missions conférées à ce dernier au sens de la présente loi est tenu au secret professionnel et passible des peines prévues à l'article 458 du Code pénal.

Art. 6. Tiers de confiance

(1) Le tiers de confiance a pour missions :

a) de mettre en œuvre les missions lui conférées par la présente loi ;

b) d'effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données ;

c) de collaborer étroitement avec l'Autorité des données, le Centre et le LNDS.

(2) Le tiers de confiance :

a) dispose de ressources humaines et techniques suffisantes et de l'expertise adéquate pour s'acquitter efficacement des missions dont il est chargé conformément à la présente loi ;

b) ne divulgue aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données, ou susceptible de porter préjudice aux droits à la protection des données, à la propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation ;

c) désigne le personnel chargé des missions qui lui sont conférées par la présente loi. Le personnel est désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données ;

d) veille à ce que le personnel chargé des missions qui lui sont conférées par la présente loi ne soit pas chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données visés par la présente loi ;

e) veille à ce que le personnel chargé des missions qui lui sont conférées par la présente loi n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui lui sont conférés par la présente loi ou s'il y a incompatibilité, de fait ou de droit, avec l'exercice des tâches qui lui sont conférées en application de la présente loi.

(3) Il est interdit au personnel du tiers de confiance chargé de l'exécution des missions conférées à ce dernier par la présente loi d'avoir un intérêt quelconque, par lui-même ou par personne interposée, et sous quelque forme juridique que ce soit, dans une entité publique, dans un organisme du secteur public détenant les données ou dans un réutilisateur de données visées aux titres V et VI.

(4) Sans préjudice de l'article 23 du Code de procédure pénale, le personnel du tiers de confiance chargé de l'exécution des missions conférées à ce dernier au sens de la présente loi est tenu au secret professionnel et passible des peines prévues à l'article 458 du Code pénal.

Art. 7. Point d'information unique

(1) Sous l'autorité du ministre ayant la digitalisation dans ses attributions est instauré un point d'information unique conformément à l'article 8 du règlement (UE) 2022/868, ci-après désigné par le terme « point d'information unique ».

(2) Le point d'information unique a pour missions :

a) de recevoir les demandes d'accès et de réutilisation de données visées par le titre VI, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;

b) de rendre disponibles au public toutes les informations pertinentes concernant l'application des articles 5 et 6 du règlement (UE) 2022/868 ainsi que toute autre information dont la publication est sollicitée par l'Autorité des données ;

c) de mettre à disposition, conformément à l'article 8, paragraphe 2 du règlement (UE) 2022/868, par voie électronique une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données conformément au titre VI, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

(3) Pour les cas visés au titre V, le point d'information unique a pour mission :

a) de recevoir les demandes de traitement ultérieur de données à caractère personnel visées par le titre V, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;

b) de mettre à disposition par voie électronique la liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles en vue de leur traitement ultérieur, visée à l'article 18, paragraphe 3 ;

c) de rendre disponibles au public toutes les informations dont la publication est demandée par l'Autorité des données.

Art. 8. Conseil consultatif de la valorisation des données dans un environnement de confiance

(1) Il est institué, sous l'autorité du ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions, un Conseil consultatif de la valorisation des données dans un environnement de confiance, ci-après désigné par le terme « Conseil consultatif ».

(2) Le Conseil consultatif a pour mission :

1° de fonctionner comme organe consultatif de l'Autorité des données ;

2° de soumettre un avis motivé dans les cas où ce dernier est sollicité conformément aux dispositions de la présente loi ;

3° de se prononcer sur toute question en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données qui lui est soumise par le ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions ;

4° de promouvoir l'accès et la réutilisation des données visés au titre VI.

(3) Le Conseil consultatif est composé de représentants issus des ministères et administrations de l'État. Un règlement grand-ducal précise la composition et le mode de fonctionnement du Conseil consultatif.

TITRE IV – Informations et données à caractère personnel obtenues par les entités publiques auprès d'une autre entité publique (« *once only* »)

Art. 9. Obligation du « *once only* »

(1) Un administré présentant une demande ou produisant une déclaration à une entité publique ne peut être tenu de produire des informations ou des données à caractère personnel que celle-ci détient déjà ou qu'elle peut obtenir auprès d'une autre entité publique conformément à l'article 11.

(2) Les entités publiques échangent entre elles toutes les informations ou les données à caractère personnel nécessaires pour traiter une demande présentée par l'administré ou une déclaration présentée par celui-ci en application d'une disposition législative ou réglementaire.

Elles échangent entre elles les informations ou les données à caractère personnel nécessaires pour pouvoir informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

(3) L'obtention des informations et données à caractère personnel auprès d'une autre entité publique au sens du présent titre a pour finalités :

a) d'assurer la mise à disposition d'informations et de données à caractère personnel aux entités publiques pour l'exécution de leurs obligations et de leurs missions d'intérêt public ;

b) d'alléger la charge administrative des administrés dans le cadre de leurs demandes et déclarations ;

c) d'éviter aux entités publiques de devoir organiser elles-mêmes la collecte d'informations et de données à caractère personnel auprès des administrés.

Art. 10. Certification de l'exactitude des informations et données à caractère personnel

(1) Lorsque les informations ou données à caractère personnel nécessaires pour traiter la demande présentée par l'administré ou la déclaration présentée par celui-ci doivent être obtenues auprès d'une autre entité publique, dans les conditions prévues aux articles 11 et 12, l'administré ou son tuteur, son

curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial certifie l'exactitude des informations et des données à caractère personnel ainsi obtenues.

(2) Dans les cas où les informations et les données à caractère personnel s'avèrent inexactes, l'administré est tenu de demander leur rectification auprès de l'entité publique d'où elles proviennent et de communiquer les informations et les données à caractère personnel rectifiées à l'entité publique en charge du traitement de la demande ou de la déclaration présentée par l'administré.

Art. 11. Conditions applicables au « *once only* »

(1) L'entité publique ne sollicite pas l'échange d'informations et de données à caractère personnel auprès d'une autre entité publique s'il est manifeste qu'elle n'est pas compétente pour traiter la demande ou la déclaration présentée par l'administré ou pour l'informer sur ses droits au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir lui attribuer éventuellement lesdits prestations ou avantages.

(2) L'entité publique chargée de traiter la demande ou la déclaration fait connaître à l'administré les informations ou les données à caractère personnel nécessaires au traitement de la demande ou de la déclaration qu'elle se procure auprès d'autres entités publiques. L'information contient, pour chaque catégorie d'informations et de données à caractère personnel, les coordonnées des entités publiques d'où proviennent les informations et les données à caractère personnel.

L'obligation prévue à l'alinéa qui précède s'applique également dans les cas où l'entité publique se procure des informations ou des données à caractère personnel auprès d'autres entités publiques pour informer les administrés sur leurs droits au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

(3) Les informations et les données à caractère personnel collectées et échangées en application du présent titre ne peuvent être utilisées ultérieurement à des fins de détection systématique d'une fraude. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à procéder auxdites détections et ce pour les détections sur lesquelles porte cette habilitation.

Pour les cas visés à l'article 9, paragraphe 2, alinéa 2, au plus tard au moment de la première communication individuelle avec l'administré, celui-ci est avisé de son droit de s'opposer à la poursuite du traitement des données à caractère personnel. En cas d'opposition exprimée par l'administré de poursuivre le traitement, les informations et les données à caractère personnel obtenues à la suite de cet échange sont détruites sans délai.

(4) En cas d'impossibilité dûment motivée pour les entités publiques d'échanger les informations ou les données à caractère personnel nécessaires pour traiter la demande ou la déclaration dans les conditions prévues au présent titre :

a) les entités publiques ne sont pas tenues de procéder à l'échange d'informations et de données à caractère personnel visé à l'article 9 ; et
b) l'administré les communique à l'entité publique chargée du traitement de la demande ou de la déclaration.

Dans les cas visés à l'alinéa qui précède, l'entité publique chargée du traitement de la demande ou de la déclaration et l'entité publique détentrice des informations et données à caractère personnel remédient dans les meilleurs délais à l'impossibilité d'échanger les informations et les données à caractère personnel en question.

(5) Les entités publiques destinataires des informations et des données à caractère personnel ne peuvent se voir opposer le secret professionnel dès lors qu'elles sont, dans le cadre de leurs missions légales, habilitées à avoir connaissance des informations ou des données à caractère personnel ainsi échangées.

(6) Un règlement grand-ducal détermine les informations ou données à caractère personnel, qui en raison de leur nature, ne peuvent faire l'objet de ces échanges entre entités publiques.

Art. 12. Recensement des informations et des données à caractère personnel disponibles auprès d'une autre entité publique

(1) Les entités publiques sont tenues d'identifier, dans les meilleurs délais, les informations et données à caractère personnel qu'elles peuvent obtenir auprès d'une autre entité publique :

a) dans le cadre du traitement effectué dans l'exercice de leurs missions des demandes et déclarations présentées par un administré ;

b) pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

(2) Les entités publiques notifient, sans délai, les échanges d'informations et de données à caractère personnel identifiées conformément au paragraphe 1er aux entités publiques auprès desquelles les informations et données à caractère personnel pourraient être obtenues.

Dans un délai d'un mois à partir de la notification visée à l'alinéa qui précède, les entités publiques notifiées :

a) certifient la disponibilité des informations et des données à caractère personnel à l'entité publique demanderesse et confirment que l'échange d'informations et de données à caractère personnel n'est pas impossible ; ou

b) informent l'entité publique demanderesse du fait qu'elles ne détiennent pas les informations et les données à caractère personnel sollicitées ou que l'échange d'informations et de données à caractère personnel est impossible.

Une copie de l'information visée aux points a) et b) du présent paragraphe est transmise au ministre ayant la digitalisation dans ses attributions.

(3) Dans les cas visés au point a) du paragraphe qui précède, les entités publiques concluent dans les meilleurs délais, et au plus tard après trois mois, le protocole visé à l'article 13.

Art. 13. Protocole « *once only* »

(1) Chaque type d'échange d'informations et de données à caractère personnel visé à l'article 9 est formalisé dans un protocole signé entre les entités publiques concernées préalablement à l'échange des informations et des données à caractère personnel.

Le protocole contient, au moins, les éléments suivants :

1° les coordonnées des entités publiques d'où proviennent les informations et les données à caractère personnel et des entités publiques destinataires des informations et les données à caractère personnel ;

2° une description détaillée du contexte du traitement des informations et des données à caractère personnel ainsi que les motifs pour lesquels les informations et les données à caractère personnel sont nécessaires pour le respect des obligations prévues à l'article 9 ;

3° une description détaillée des catégories d'informations et de données à caractère personnel visées par l'échange à l'entité publique destinataire ;

4° une description détaillée des catégories de personnes concernées ;

5° une description détaillée des finalités du traitement ;

6° le cas échéant, l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers et les pays tiers à destination desquels des transferts de données à caractère personnel sont envisagés ainsi que l'existence ou l'absence de garanties appropriées conformément au chapitre V du règlement (UE) 2016/679 ;

7° les motifs pour lesquels les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies.

(2) Tout changement des éléments liés à l'obtention des informations et des données à caractère personnel auprès d'une entité publique doit être formalisé par avenant du protocole visé au paragraphe qui précède.

(3) Le protocole ainsi que tout avenant sont transmis sans délai à l'Autorité des données qui les publie par voie électronique. L'Autorité des données n'est pas responsable du contenu du protocole.

Les entités publiques informent sans délai l'Autorité des données lorsqu'un protocole n'est plus applicable. L'Autorité des données maintient la publication des protocoles pendant une durée de deux ans à partir de la réception de l'information visée au présent alinéa. Pendant cette période, elle indique que le protocole n'est plus applicable.

Art. 14. Identification des sources authentiques d'informations et de données à caractère personnel

(1) L'Autorité des données tient un registre de tous les protocoles qui lui sont transmis pour publication conformément à l'article 13, paragraphe 3.

(2) En vue d'identifier des sources authentiques d'informations et de données à caractère personnel disponibles au sein des entités publiques, le ministre ayant la digitalisation dans ses attributions dispose d'un accès direct au registre des protocoles visés au paragraphe qui précède.

TITRE V – Traitement ultérieur de données à caractère personnel par les entités publiques

Section I – Dispositions générales

Art. 15. Finalités du traitement ultérieur autorisées et licéité du traitement

(1) Le traitement ultérieur de données à caractère personnel par des entités publiques est autorisé si :

1° les conditions énoncées au présent titre sont remplies ; et

2° que le traitement des données à caractère personnel est effectué exclusivement pour une ou plusieurs des finalités suivantes :

a) l'analyse statistique ;

b) les activités d'éducation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;

c) la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;

d) l'évaluation et la planification des politiques envisagées ou planifiées par le Gouvernement et approuvées par décision du Gouvernement en conseil, ou en ce qui concerne les communes, envisagées ou planifiées par le Conseil communal ;

e) lorsque la mise en œuvre d'un accord international requiert la communication d'informations ou lorsque le traitement ultérieur des données à caractère personnel permet de répondre aux demandes d'informations officielles provenant de gouvernements étrangers ou d'organisations internationales approuvées par décision du Gouvernement en conseil ;

f) les activités de développement, d'évaluation, de démonstration, de sécurité et d'innovation de dispositifs ou de services ;

g) la formation, le test et l'évaluation d'algorithmes, y compris dans les dispositifs, les systèmes d'intelligence artificielle et les applications numériques.

(2) Le traitement ultérieur des données à caractère personnel, y compris leur partage et leur mise à disposition, par les entités publiques conformément au présent titre, est licite au sens de l'article 6, paragraphe 1er, lettre e) et, si applicable, de l'article 9, paragraphe 2, lettre g) ou j) du règlement (UE) 2016/679.

Art. 16. Conditions d'anonymisation et de pseudonymisation des données à caractère personnel

(1) Les données à caractère personnel détenues par des entités publiques doivent être anonymisées préalablement à leur traitement ultérieur aux fins énoncées à l'article 15, paragraphe 1er point 2°.

(2) Lorsque le traitement de données anonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel doivent être pseudonymisées préalablement à leur traitement ultérieur aux fins énoncées à l'article 15, paragraphe 1er point 2°.

(3) Lorsque le traitement ultérieur de données à caractère personnel pseudonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel peuvent être traitées ultérieurement aux fins énoncées à l'article 15, paragraphe 1er point 2° de manière nonpseudonymisées dans les limites du strict nécessaire.

(4) Les entités publiques qui détiennent les données à caractère personnel sont tenus d'identifier les informations protégées pour des motifs de protection des données à caractère personnel.

Elles renseignent les motifs pour lesquels les données doivent être protégées dans le plan de confidentialité prévu à l'article 35 et indiquent sur quelles parties des informations porte cette protection.

(5) Les entités publiques effectuant le traitement ultérieur de données à caractère personnel sont tenues d'une obligation de confidentialité interdisant la divulgation de toute information compromettant les droits et intérêts de la personne concernée qu'elles peuvent avoir acquise malgré les garanties mises en place conformément aux dispositions de la présente loi.

Sans préjudice du paragraphe 3, il est interdit aux entités publiques effectuant le traitement ultérieur de données à caractère personnel de rétablir l'identité de toute personne concernée à laquelle se rapportent les données à caractère personnel. Les entités publiques prennent des mesures techniques et opérationnelles pour empêcher toute réidentification.

Section II – Traitement ultérieur de données à caractère personnel par la même entité publique

Art. 17. Conditions spécifiques applicables au traitement ultérieur de données à caractère personnel par la même entité publique

(1) Une entité publique est autorisée à traiter ultérieurement les données à caractère personnel qu'elle détient pour les finalités énoncées à l'article 15, paragraphe 1er, point 2°, sous réserve du respect des dispositions de l'article 16.

(2) Lorsque le traitement ultérieur porte sur des données à caractère personnel visées aux articles 9, paragraphe 1er et 10 du règlement (UE) 2016/679, les données à caractère personnel ne peuvent pas être traitées ultérieurement de manière non-anonymisées ou non-pseudonymisées.

Section III – Traitement ultérieur de données à caractère personnel par une autre entité publique ou par plusieurs entités publiques

Art. 18. Conditions spécifiques applicables au traitement ultérieur de données à caractère personnel par une autre entité publique ou par plusieurs entités publiques

(1) Une entité publique est autorisée à traiter ultérieurement les données à caractère personnel détenues par une autre entité publique pour les finalités énoncées à l'article 15, paragraphe 1er, point 2°, aux conditions suivantes :

1° l'entité publique qui détient les données à caractère personnel :

a) a marqué son accord de principe au traitement ultérieur, y compris le partage et la mise à disposition en inscrivant les données à caractère personnel disponibles sur la liste des ressources consultables tenues par le point d'information unique, conformément au paragraphe 3 ; ou

b) a marqué son accord spécifique au traitement ultérieur, y compris le partage et la mise à disposition, en contresignant la demande visée à l'article 27 ;

2° le traitement ultérieur de données à caractère personnel ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard des finalités poursuivies ;

3° les données à caractère personnel sont anonymisées préalablement au traitement ultérieur des données à caractère personnel, ou lorsque le traitement de données anonymisées ne permet pas d'atteindre la finalité poursuivie, si :

a) l'Autorité des données autorise le traitement ultérieur de données à caractère personnel conformément à l'article 31 ;

b) les données à caractère personnel sont pseudonymisées préalablement à leur traitement ultérieur ;

c) le traitement ultérieur de données à caractère personnel est effectué dans l'environnement de traitement sécurisé prévu à l'article 36.

(2) L'entité publique sollicitant le traitement ultérieur de données à caractère personnel détenues par une autre entité publique qui se voit opposer un refus de partage par l'entité publique détenant les données à caractère personnel sollicitées peut saisir pour avis le Conseil consultatif. Le Conseil consultatif émet un avis quant à la demande de partage dans un délai de trois semaines. L'avis du Conseil consultatif est communiqué à l'entité publique qui sollicite le partage ainsi qu'à l'entité publique détenant les données à caractère personnel, qui est appelée à considérer à nouveau la demande de partage.

L'entité publique détenant les données à caractère personnel sollicitées acte sa décision finale par écrit dans un délai de trois semaines. Elle transmet une copie de sa décision finale sans délai à l'entité publique qui sollicite le partage et au Conseil consultatif. L'absence de décision finale de l'entité publique détenant les données à caractère personnel sollicitées dans le délai imparti vaut refus.

En cas d'accord, l'entité publique détentrice des données à caractère personnel contresigne la demande visée à l'article 27.

(3) Le point d'information unique met à disposition par voie électronique une liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles en vue de leur traitement ultérieur conformément au présent titre, avec des informations pertinentes décrivant les données à caractère personnel disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur traitement ultérieur.

TITRE VI – Accès et réutilisation des données détenues par des organismes du secteur public par des réutilisateurs de données

Section I – Dispositions générales

Art. 19. Catégories de données protégées disponibles à l'accès et à la réutilisation

(1) Le présent titre s'applique à l'accès et à la réutilisation, par un réutilisateur de données, des données détenues par des organismes du secteur public, conformément au règlement (UE) 2022/868, qui sont protégées pour des motifs :

1° de confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise ;

2° de secret statistique ;

3° de protection des droits de propriété intellectuelle de tiers ; ou

4° de protection des données à caractère personnel, dans la mesure où de telles données ne relèvent pas du champ d'application de la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public.

(2) Le présent titre ne s'applique pas :

1° aux données énoncées à l'article 3, paragraphe 2, du règlement (UE) 2022/868 ;

2° aux cas visés par les autres titres de la présente loi.

Art. 20. Finalités d'accès et réutilisation des données autorisées

L'accès et la réutilisation des données par des réutilisateurs de données sont autorisés si :

1° les conditions énoncées à la section II du présent titre sont remplies ; et

2° l'accès et la réutilisation des données est effectué exclusivement pour une ou plusieurs des finalités suivantes :

a) l'analyse statistique ;

b) les activités d'éducation, de formation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;

c) la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;

d) le développement, l'évaluation, la démonstration, la sécurité et l'innovation de technologies ;

e) le développement, l'évaluation, la démonstration, la sécurité et l'innovation de produits ;

f) l'évaluation des politiques publiques luxembourgeoises ou européennes.

Art. 21. Conditions d'anonymisation, de pseudonymisation et de méthodes de contrôle de divulgation des données

(1) Les données à caractère personnel détenues par des organismes du secteur public doivent être anonymisées préalablement à l'accès et à la réutilisation par le réutilisateur de données.

(2) Lorsque l'accès et la réutilisation de données à caractère personnel anonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel doivent être pseudonymisées préalablement à l'accès et à la réutilisation par le réutilisateur de données.

(3) Les accès et réutilisations effectués conformément au présent titre, par des réutilisateurs de données, de données à caractère personnel détenues par les organismes du secteur public, sous une forme non anonymisée ou non pseudonymisée, sont interdits.

(4) Les données détenues par des organismes du secteur public doivent être modifiées, agrégées, supprimées ou traitées selon toute autre méthode de contrôle de la divulgation préalablement à l'accès et à la réutilisation par le réutilisateur de données, pour éviter toute atteinte disproportionnée aux droits de propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique.

(5) Les organismes du secteur public qui détiennent les données à caractère personnel et les données à caractère non personnel sont tenus d'identifier les données protégées pour les motifs visés à l'article 19, paragraphe 1er.

Ils renseignent les motifs pour lesquels les données doivent être protégées dans le plan de confidentialité prévu à l'article 35 et indiquent sur quelles parties des informations porte cette protection.

(6) Les réutilisateurs de données sont tenus d'une obligation de confidentialité interdisant la divulgation de toute information compromettant les droits et intérêts protégés par la présente loi qu'ils peuvent avoir acquis malgré les garanties mises en place conformément aux dispositions de la présente loi.

Il est interdit aux réutilisateurs de données de rétablir l'identité de toute personne concernée à laquelle se rapportent les données. Les réutilisateurs de données prennent les mesures techniques et opérationnelles nécessaires pour empêcher toute réidentification.

Section II – Conditions applicables à la réutilisation de données à caractère personnel

Art. 22. L'accès et la réutilisation de données à caractère personnel par des réutilisateurs de données

(1) Un réutilisateur de données peut accéder et réutiliser les données à caractère personnel détenues par un organisme du secteur public pour les finalités énoncées à l'article 20, paragraphe 1er, point 2° aux conditions cumulatives suivantes :

1° l'Autorité des données autorise l'accès et la réutilisation conformément à l'article 31 ;

2° l'organisme du secteur public qui détient les données :

a) a marqué son accord de principe à la mise à disposition des données à caractère personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en inscrivant les données disponibles sur la liste des ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2 du règlement (UE) 2022/868 ; ou

b) a marqué son accord spécifique à la mise à disposition des données à caractère personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en contresignant la demande visée à l'article 28 ;

3° l'accès et la réutilisation ne portent pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ;

4° les données à caractère personnel sont anonymisées ou pseudonymisées préalablement à leur accès et à leur réutilisation ;

5° l'accès et la réutilisation des données à caractère personnel se font dans l'environnement de traitement sécurisé visé à l'article 36.

(2) Le traitement de données à caractère personnel, y compris leur partage et leur mise à disposition, par les organismes du secteur public conformément au présent titre, est licite au sens de l'article 6, paragraphe 1er, lettre e) et, si applicable, de l'article 9, paragraphe 2, lettre g) ou j) du règlement (UE) 2016/679.

(3) Le réutilisateur de données qui se voit opposer un refus d'accès de réutilisation des données par l'organisme du secteur public détenant les données sollicitées peut saisir le Conseil consultatif, qui émet un avis quant à la demande d'accès et de réutilisation dans un délai de trois semaines. L'avis du Conseil consultatif est communiqué au réutilisateur de données et à l'organisme du secteur public détenant les données, qui est appelé à considérer à nouveau la demande d'accès et de réutilisation.

L'organisme du secteur public détenant les données sollicitées acte sa décision finale par écrit dans un délai de trois semaines. Il transmet une copie de sa décision finale sans délai au réutilisateur de données et au Conseil consultatif. L'absence de décision finale de l'organisme du secteur public détenant les données sollicitées dans les délais impartis vaut refus.

En cas d'accord, l'organisme du secteur public détenant les données contresigne la demande visée à l'article 28.

Section III – Conditions applicables à la réutilisation de données à caractère non personnel

Art. 23. L'accès et la réutilisation de données à caractère non personnel détenues par les organismes du secteur public

(1) Un réutilisateur de données peut accéder et réutiliser les données à caractère non personnel détenues par un autre organisme du secteur public et protégées pour les motifs visés à l'article 19, paragraphe 1er, points 1° à 3° aux conditions cumulatives suivantes :

1° l'Autorité des données autorise l'accès et la réutilisation conformément à l'article 31 ;

2° l'organisme du secteur public qui détient les données :

a) a marqué son accord de principe à la mise à disposition des données à caractère non personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en inscrivant les données disponibles sur la liste des ressources consultables tenue par le point d'information unique conformément à l'article 8, paragraphe 2 du règlement (UE) 2022/868 ; ou

b) a marqué son accord spécifique à la mise à disposition des données à caractère non personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en contresignant la demande visée à l'article 28 ;

3° l'accès et la réutilisation ne portent pas une atteinte disproportionnée aux droits protégés pour les motifs visés à l'article 19, paragraphe 1er, points 1° à 3°;

4° les données à caractère non personnel sont modifiées, agrégées, supprimées ou traitées selon toute autre méthode de contrôle de la divulgation préalablement à leurs accès et à leur réutilisation ;

5° l'accès et la réutilisation des données à caractère non personnel se font dans l'environnement de traitement sécurisé visé à l'article 36.

(2) Le réutilisateur de données sollicitant l'accès et la réutilisation de données détenues par un organisme du secteur public qui se voit opposer un refus d'accès de réutilisation des données par les organismes du secteur public détenant les données sollicitées peut saisir le Conseil consultatif, qui émet un avis quant à la demande d'accès et de réutilisation dans un délai de trois semaines. L'avis du Conseil consultatif est communiqué au réutilisateur de données et à l'organisme du secteur public détenant les données, qui est appelé à considérer à nouveau la demande d'accès et de réutilisation.

L'organisme du secteur public détenant les données sollicitées acte sa décision finale par écrit dans un délai de trois semaines. Il transmet une copie de sa décision finale sans délai au réutilisateur de

données et au Conseil consultatif. L'absence de décision finale de l'organisme du secteur public détenant les données sollicitées dans les délais impartis vaut refus.

En cas d'accord, l'organisme du secteur public détenant les données contresigne la demande visée à l'article 28.

Section IV – Conditions applicables à la réutilisation d'ensembles contenant des données à caractère personnel et des données à caractère non personnel

Art. 24. Conditions applicables à la réutilisation d'ensembles mixtes de données détenus par les organismes du secteur public

Lorsque l'accès et la réutilisation portent sur un ensemble de données détenu par un organisme du secteur public qui contient des données à caractère personnel et des données à caractère non personnel, l'accès et la réutilisation sont soumis aux conditions énoncées aux articles 19 à 23.

TITRE VII – Modalités applicables au traitement ultérieur des données à caractère personnel par les entités publiques et à l'accès et à la réutilisation de données par des réutilisateurs de données

Section I – Dispositions générales

Art. 25. Champ d'application

Les dispositions du présent titre s'appliquent aux traitements ultérieurs de données à caractère personnel visés au titre V et aux accès et réutilisation de données prévus au titre VI, qui sont soumis à autorisation de l'Autorité des données.

Section II – Demande de traitement ultérieur ou d'accès et de réutilisation des données

Art. 26. Forme de la demande de traitement ultérieur ou d'accès et de réutilisation des données

(1) Les demandes de traitement ultérieur de données à caractère personnel visées au titre V ainsi que les demandes d'accès et de réutilisation visées au titre VI à présenter à l'Autorité des données doivent être formulées de façon précise et revêtir une forme écrite.

(2) Toute modification substantielle de la demande intervenant au cours de l'instruction de la demande par l'Autorité des données qui affecte les informations et pièces visées aux articles 27 et 28 nécessite le dépôt d'une nouvelle demande conformément à l'article 29.

Art. 27. Contenu de la demande de traitement ultérieur de données à caractère personnel

(1) Dans les cas visés au titre V, la demande à présenter par les entités publiques effectuant le traitement ultérieur des données à caractère personnel doit contenir les informations suivantes :

1° les coordonnées des entités publiques effectuant le traitement ultérieur des données à caractère personnel ;

2° les coordonnées des entités publiques détentrices des données à caractère personnel ;

3° une description détaillée du contexte du traitement de données à caractère personnel envisagé ;

4° une description détaillée des catégories de données à caractère personnel et des catégories de personnes concernées ;

5° la base de licéité du traitement ainsi qu'une description détaillée des finalités du traitement ;

6° une description détaillée des mesures appropriées qui permettent d'apprécier le respect des exigences en matière d'anonymisation et de pseudonymisation des données à caractère personnel, en particulier la justification du respect des conditions visées à l'article 16 ;

7° la durée du traitement de données à caractère personnel envisagée dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le

système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

8° les destinataires de données à caractère personnel et, le cas échéant, l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers et les pays tiers à destination desquels des transferts de données sont envisagés ainsi que l'existence ou l'absence de garanties appropriées conformément au chapitre V du règlement (UE) 2016/679 ;

9° les motifs pour lesquels le traitement ultérieur des données à caractère personnel ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ;

10° les motifs pour lesquels les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies ;

11° le cas échéant, une description détaillée des données à caractère personnel provenant de sources autres que les entités publiques effectuant le traitement ultérieur de données à caractère personnel et les entités publiques détenant les données à caractère personnel, dont l'introduction dans l'environnement de traitement sécurisé est sollicitée ;

12° les obligations respectives des responsables du traitement aux fins d'assurer le respect des exigences du règlement (UE) 2016/679, notamment en ce qui concerne l'exercice des droits de la personne concernée ;

13° la signature de la demande par toutes les entités publiques visées au point 1° du présent paragraphe ;

14° pour les cas visés à l'article 18, paragraphe 1er, point 1°, lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 18, paragraphe 3 ;

15° pour les cas visés à l'article 18, paragraphe 1, point 1°, lettre b), la signature de la demande par toutes les entités publiques visées au point 2° du présent paragraphe.

(2) Les entités publiques effectuant le traitement ultérieur de données à caractère personnel, en leur qualité de responsables du traitement, joignent les documents suivants à leur demande :

1° si applicable, l'analyse d'impact relative à la protection des données à caractère personnel visée par l'article 35 du règlement (UE) 2016/679 ;

2° l'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679 ;

3° le plan de confidentialité signé par toutes les parties visées à l'article 35, paragraphe 2 ;

4° l'attestation de faisabilité visée à l'article 35, paragraphe 3 émise par le Centre ;

5° si applicable, une copie de l'avis du Conseil consultatif visé à l'article 18, paragraphe 2.

(3) Les entités publiques effectuant le traitement ultérieur de données à caractère personnel :

a) certifient l'exactitude des informations contenues dans la demande et les pièces jointes visées au présent article ;

b) certifient que le plan de confidentialité correspond aux informations contenues dans la demande présentée à l'Autorité des données ;

c) s'engagent formellement à respecter les termes de l'autorisation de l'Autorité des données et du plan de confidentialité.

Art. 28. Contenu de la demande d'accès et de réutilisation de données

(1) Dans les cas visés au titre VI, la demande à présenter par les réutilisateurs des données doit contenir les informations suivantes :

1° les coordonnées des réutilisateurs des données ;

2° les coordonnées des organismes du secteur public détenant les données ;

3° une description détaillée du contexte de l'accès et de la réutilisation des données ;

4° une description détaillée des données et des catégories de personnes visées par la demande ;

5° une description détaillée des mesures appropriées qui permettent d'apprécier le respect des exigences en matière d'anonymisation, de pseudonymisation et d'agrégation des données visées à l'article 21, en particulier la justification du respect des conditions visées à l'article 21 ;

6° les motifs pour lesquels les données sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies ;

7° les motifs pour lesquels l'accès et la réutilisation des données ne portent pas une atteinte disproportionnée aux droits protégés pour les motifs visés à l'article 19, paragraphe 1er ;

8° les destinataires de données ;

9° le cas échéant, une description détaillée des données provenant des réutilisateurs de données et/ou de détenteurs de données autres que les organismes du secteur public, dont l'introduction dans l'environnement de traitement sécurisé est sollicitée par le réutilisateur de données ;

10° la durée d'accès et de réutilisation des données dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

11° le cas échéant, l'intention d'effectuer un transfert de données vers un pays tiers et les pays tiers à destination desquels des transferts de données sont envisagés ;

12° la signature de la demande par tous les réutilisateurs des données visés au point 1° du présent paragraphe ;

13° pour les cas visés à l'article 22, paragraphe 2, point 2°, lettre a) et à l'article 23, paragraphe (2) point 2°, lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2 du règlement (UE) 2022/868 ;

14° pour les cas visés à l'article 22, paragraphe 2, point 2°, lettre b) et à l'article 23, paragraphe 2 point 2°, lettre b), la signature de la demande par tous les organismes du secteur public visés au point 2° du présent paragraphe.

(2) Lorsque la demande porte sur des données à caractère personnel, elle contient également les informations suivantes :

1° la base de licéité du traitement de données à caractère personnel ainsi qu'une description détaillée des finalités du traitement de données à caractère personnel ;

2° les motifs pour lesquels l'accès et la réutilisation des données ne portent pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ;

3° les obligations respectives des responsables du traitement aux fins d'assurer le respect des exigences du règlement (UE) 2016/679, notamment en ce qui concerne l'exercice des droits de la personne concernée ;

4° le cas échéant, l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence de garanties appropriées conformément au chapitre V du règlement (UE) 2016/679.

(3) La demande doit être accompagnée du plan de confidentialité signé par toutes les parties visées à l'article 35, paragraphe 2 et de l'attestation de faisabilité visée à l'article 35, paragraphe 3 émise par le Centre.

(4) Les réutilisateurs de données effectuant l'accès et la réutilisation des données à caractère personnel, en leur qualité de responsables du traitement, joignent les documents suivants à leur demande :

1° si applicable, l'analyse d'impact relative à la protection des données visée par l'article 35 du règlement (UE) 2016/679 ;

2° l'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679 ;

3° si applicable, une copie de l'avis du Conseil consultatif visé aux articles 22, paragraphe 3 et 23, paragraphe 2.

(5) Les réutilisateurs de données :

a) certifient l'exactitude des informations contenues dans la demande et les pièces jointes visées au présent article ;

b) certifient que le plan de confidentialité correspond aux informations contenues dans la demande présentée à l'Autorité des données ;

c) s'engagent formellement à respecter les termes de l'autorisation de l'Autorité des données et du plan de confidentialité.

Section III – Instruction de la demande par l'Autorité des données

Art. 29. Dépôt et procédure d'instruction de la demande

(1) Le dépôt des demandes visées à la section II du présent titre, ci-après désignées la « demande », se fait auprès de l'Autorité des données.

(2) L'Autorité des données statue dans un délai de deux mois à compter du dépôt de la demande.

En cas de demande exceptionnellement détaillée et complexe, le délai de deux mois peut être prolongé de trente jours au maximum. L'Autorité des données informe le demandeur dès que possible de la nécessité du délai supplémentaire pour instruire la demande, ainsi que des raisons qui justifient ce délai.

(3) Pour les cas visés à l'article 31, paragraphe 5, l'Autorité des données statue dans un délai d'un mois à compter du dépôt de la demande de modification ponctuelle.

Dans les cas où le délai d'instruction de la demande par l'Autorité des données excède la durée couverte par l'autorisation initiale adoptée par cette dernière, les données disponibles dans l'environnement de traitement sécurisé sont conservées dans un système d'archivage intermédiaire à accès restreint pendant le délai d'instruction de la demande par l'Autorité des données, et ce jusqu'à adoption de la décision finale.

Le système d'archivage intermédiaire et les systèmes informatiques par lesquels le traitement ultérieur des données à caractère personnel ou l'accès et la réutilisation des données sont opérés, doivent être aménagés de sorte que leur accès est sécurisé, moyennant une authentification forte, et que les informations relatives au gestionnaire du dossier ayant initié la requête, les informations demandées, la date et l'heure puissent être retracées.

(4) La demande ne comprenant pas tous les éléments énoncés aux articles 27 ou 28 est déclarée irrecevable.

(5) L'Autorité des données peut demander des renseignements complémentaires aux demandeurs. En pareil cas, les délais visés aux paragraphes 2 et 3 sont suspendus à compter de la transmission de la demande de renseignements complémentaires, et ce jusqu'à réception par l'Autorité des données des renseignements sollicités. Faute de réponse du demandeur dans un délai d'un mois, la demande est rejetée d'office.

(6) Les échanges et démarches visés au présent article se font par voie électronique via le point d'information unique.

(7) L'Autorité des données peut transmettre la demande de traitement ultérieur de données à caractère personnel visée à l'article 27 et la demande d'accès et de réutilisation visée à l'article 28 au Conseil consultatif pour avis. Elle y joint toute autre pièce dont elle dispose qui est sollicitée par le Conseil consultatif. L'absence d'avis du Conseil consultatif dans un délai de trois semaines à compter de la transmission de la demande et de la décision de l'organisme du secteur public détenant les données, vaut avis favorable.

Art. 30. Redevances

Pour chaque demande visée à l'article 28, une redevance est fixée par l'Autorité des données pour couvrir les frais administratifs occasionnés par le traitement de la demande et par la mise à disposition des données dans l'environnement de traitement sécurisé.

Un règlement grand-ducal détermine la procédure applicable à la perception de la redevance.

Art. 31. Autorisation par l'Autorité des données

(1) Dans les cas visés au titre V, l'Autorité des données autorise le traitement ultérieur de données à caractère personnel lorsque :

a) la demande visée à l'article 27 est complète et accompagnée de toutes les pièces visées à l'article 27, paragraphe 2 ;

b) l'entité publique détentrice des données à caractère personnel a donné son accord écrit spécifique au traitement ultérieur de données à caractère personnel, y compris au partage et à la mise à disposition, en contresignant la demande visée à l'article 27 ;

c) le traitement ultérieur de données à caractère personnel est exclusivement effectué pour une ou plusieurs finalités visées à l'article 15, paragraphe 1er, point 2 ;

d) le traitement ultérieur de données à caractère personnel ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie.

(2) Dans les cas visés au titre VI, l'Autorité des données autorise l'accès et la réutilisation de données :

1° dans le cas où la demande vise l'accès et la réutilisation de données à caractère personnel, lorsque :

a) la demande visée à l'article 28 est complète et accompagnée de toutes les pièces visées à l'article 28, paragraphes 3 et 4 ;

b) pour les cas visés à l'article 22, paragraphe 2, point 2°:

i. lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2 du règlement (UE) 2022/868 ;

ii. lettre b), la signature de la demande par tous les organismes du secteur public visés au point 2° du présent paragraphe ;

c) l'accès et la réutilisation de données est exclusivement effectuée pour une ou plusieurs finalités visées à l'article 20, paragraphe 1er, point 2° ;

d) l'accès et la réutilisation ne portent pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ;

e) la réutilisation des données n'entraine pas un risque pour la défense nationale, la sécurité publique ou l'ordre public.

2° dans les cas où la demande vise l'accès et la réutilisation de données à caractère non personnel, lorsque :

a) la demande visée à l'article 28 est complète et est accompagnée de toutes les pièces visées à l'article 28, paragraphes 3 et 4 ;

b) pour les cas visés à l'article 23, paragraphe 2 point 2° :

i. lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2 du règlement (UE) 2022/868 ;

ii. lettre b), la signature de la demande par tous les organismes du secteur public visés au point 2° du présent paragraphe ;

c) la réutilisation est exclusivement effectuée pour une ou plusieurs finalités visées à l'article 20, paragraphe 1er, point 2 ;

d) l'accès et la réutilisation ne portent pas une atteinte disproportionnée aux droits protégés pour les motifs visés à l'article 20, paragraphe 1er, points 1° à 3° ;

e) la réutilisation des données n'entraine pas un risque pour la défense nationale, la sécurité publique ou l'ordre public.

3° dans le cas où la demande vise l'accès et la réutilisation d'ensembles mixtes de données, les conditions prévues aux points 1° et 2° du présent paragraphe s'appliquent.

(3) La décision d'autorisation ou de refus de l'Autorité des données est motivée. L'Autorité des données joint la demande et, si applicable, l'avis du Conseil consultatif à sa décision.

(4) Toute modification substantielle du traitement ultérieur de données à caractère personnel visé au titre V ou de l'accès et de la réutilisation des données visés au titre VI couverts par une autorisation de l'Autorité des données conformément au présent article, doit faire l'objet d'une nouvelle demande

et d'une nouvelle autorisation par l'Autorité des données, conformément aux dispositions des articles 27 à 31.

(5) Si la modification sollicitée porte exclusivement sur les éléments visés à l'article 27, paragraphe 1er, point 7° ou à l'article 28, paragraphe 1er, point 10° autorisés par l'Autorité des données, l'Autorité des données statue sur le bien-fondé de la demande de modification dans le cadre de la procédure accélérée visée à l'article 29, paragraphe 3.

La demande de modification visée au présent paragraphe contient :

1° dans le cas visé au titre V :

a) les coordonnées des entités publiques effectuant le traitement ultérieur des données à caractère personnel et des entités publiques détentrices des données à caractère personnel ;

b) la nouvelle durée du traitement de données à caractère personnel envisagée dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

c) l'attestation du Centre, ou du tiers de confiance mandaté par le Centre, que la modification sollicitée ne porte pas préjudice à l'efficacité des mesures consignées dans le plan de confidentialité ;

d) la signature de la demande par toutes les entités publiques visées au point a).

2° dans le cas visé au titre VI :

a) les coordonnées des organismes du secteur public détenant les données et des réutilisateurs des données ;

b) la nouvelle durée d'accès et de réutilisation des données dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

c) l'attestation du Centre, ou du tiers de confiance mandaté par le Centre, que la modification sollicitée ne porte pas préjudice à l'efficacité des mesures consignées dans le plan de confidentialité ;

d) la signature de la demande par tous les organismes du secteur public détenant les données et des réutilisateurs des données visés au point a).

(6) Les entités publiques et les organismes du secteur public mettent les données à caractère personnel et les données à caractère non personnel visées par l'autorisation de l'Autorité des données à disposition de celle-ci en vue de la mise en œuvre des mesures prévues au présent titre et de leur mise à disposition dans l'environnement de traitement sécurisé.

(7) Les entités publiques traitant ultérieurement les données à caractère personnel et les réutilisateurs de données sont tenus de traiter les données uniquement conformément aux termes de l'autorisation de l'Autorité des données.

(8) Chaque fois que les réutilisateurs de données utilisent les données conformément aux titres VI et VII, ils citent les sources de données et mentionnent que les données ont été obtenues dans le cadre de la présente loi.

Art. 32. Contrôle par l'Autorité des données

(1) L'Autorité des données a le droit de vérifier le processus, les moyens et tout résultat du traitement ultérieur de données à caractère personnel effectué par les entités publiques conformément au titre V et des accès et réutilisation des données effectués par les réutilisateurs de données conformément au titre VI, afin de préserver l'intégrité de la protection des données et le respect des conditions prévues par la présente loi, notamment en ce qui concerne les droits de propriété intellectuelle, la confidentialité commerciale et le secret statistique.

(2) L'Autorité des données a le droit d'interdire l'utilisation des résultats qui contiennent des informations portant une atteinte disproportionnée aux droits et aux intérêts de tiers. La décision d'interdire l'utilisation des résultats est transparente et compréhensible pour le réutilisateur de données.

(3) L'Autorité des données peut demander tous renseignements et informations nécessaires pour l'accomplissement des missions prévues par la présente loi au Centre, au tiers de confiance mandaté par le Centre, au LNDS, aux entités publiques, aux organismes du secteur public qui détiennent les données, aux réutilisateurs ainsi qu'à tout autre entité impliquée dans la mise en œuvre de la loi.

Section IV – Publicité par l'Autorité des données

Art. 33. Publicité des conditions d'accès et de réutilisation de données détenues par les organismes du secteur public et procédure applicable

Pour les cas visés au titre VI, l'Autorité des données rend publiques les conditions d'autorisation d'accès et de réutilisation de données détenues par les organismes du secteur public et la procédure prévue à la section III du présent titre par l'intermédiaire du point d'information unique.

Art. 34. Publicité des autorisations adoptées par l'Autorité des données

(1) L'Autorité des données tient un registre public des traitements ultérieurs de données à caractère personnel et des accès et réutilisations de données autorisées.

Le registre contient pour chaque autorisation accordée par l'Autorité des données conformément au titre VII les informations suivantes :

1° une copie de la décision adoptée par l'Autorité des données conformément à l'article 31 ;

2° si applicable, l'avis du Conseil consultatif ;

3 dans le cas de données à caractère personnel, l'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679, communiquée par le demandeur.

(2) La publication par l'Autorité des données des éléments d'information à destination des personnes concernées, telle que visée au paragraphe 1er, alinéa 2, point 3°, vaut information de la personne concernée au sens des articles 12 à 14 du règlement (UE) 2016/679 pour les traitements ultérieurs de données visés au titre V et les accès et réutilisations visés au titre VI.

Section V – Mesures appropriées et mise à disposition des données dans un environnement de traitement sécurisé

Art. 35. Mesures appropriées

(1) Les mesures d'anonymisation et/ou de pseudonymisation des données à caractère personnel et/ou de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données requises par les dispositions de la présente loi et par les dispositions du règlement (UE) 2022/868 doivent être mises en œuvre préalablement au traitement ultérieur de données à caractère personnel et à l'accès et la réutilisation de données visés aux titres V et VI.

Ces mesures doivent être effectives et efficaces pour éviter toute réidentification des personnes concernées ainsi que toute atteinte aux droits d'autrui, tels que la confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise, le secret statistique et de propriété intellectuelle, compte tenu de l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour réaliser la réidentification ou pour compromettre la confidentialité des informations.

La mise en œuvre des mesures visées au présent paragraphe doit être opérée de sorte que nul autre que l'entité publique ou l'organisme du secteur public duquel proviennent les données n'ait accès aux données dans un format non anonymisé, non pseudonymisé ou non agrégé.

(2) Pour chaque demande visée aux articles 27 et 28, il est établi une évaluation spécifique des méthodes et des modalités de mise en œuvre des mesures visées au paragraphe qui précède.

L'évaluation est initiée, dans les cas visés au titre V, par les entités publiques effectuant le traitement ultérieur de données à caractère personnel et, dans les cas visés au titre VI, par les réutilisateurs de données. Elle est consignée dans un plan de confidentialité.

Le plan de confidentialité est préparé par les parties visées à l'alinéa qui précède. Il précise les conditions et les modalités, y compris les opérations et procédures de mise en œuvre, des mesures visées au paragraphe 1er.

Le projet de plan de confidentialité est amendé jusqu'à validation finale et signature commune par le Centre, ou par le tiers de confiance mandaté par le Centre, et :

a) pour les cas visés au titre V, les entités publiques effectuant le traitement ultérieur de données à caractère personnel et les entités publiques détenant les données à caractère personnel ;

b) pour les cas visés au titre VI, les réutilisateurs de données et les organismes du secteur public détenant les données.

Toutes les parties visées au présent paragraphe fournissent au Centre, ou au tiers de confiance mandaté par le Centre, et, dans les cas visés à l'article 5, paragraphe 3, point d) au LNDS, toute information nécessaire pour la mise en place du plan de confidentialité, qui les traitent pour les seules finalités visées au présent article ou à des fins de preuve. Le tiers de confiance et le Centre se concertent étroitement.

En signant le plan de confidentialité, le Centre, ou le tiers de confiance mandaté par le Centre, certifie que les mesures prévues au paragraphe 1er consignées dans le plan de confidentialité sont effectives et efficaces pour éviter toute réidentification des personnes concernées ainsi que toute atteinte aux droits d'autrui, tels que la confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise, le secret statistique et de propriété intellectuelle, compte tenu de l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour réaliser la réidentification ou pour compromettre la confidentialité des informations.

(3) Sur présentation du plan de confidentialité signé par toutes les parties, le Centre atteste de la faisabilité :

a) de la mise en œuvre des mesures énoncées dans le plan de confidentialité ;

b) de la mise à disposition des données dans l'environnement de traitement sécurisé.

L'attestation du Centre est jointe à la demande visée aux articles 27 et 28.

(4) Sous réserve d'autorisation de l'Autorité des données visée à l'article 31 et d'acquittement par le demandeur de la redevance visée à l'article 30 :

a) le Centre, ou le tiers de confiance mandaté par le Centre, s'assure de la mise en œuvre les mesures visées au présent article conformément aux stipulations du plan de confidentialité ;

b) le Centre :

i. combine et traite les données provenant des entités publiques et des organismes du secteur public visés au paragraphe 1er, alinéa 3, pour lesquelles le traitement ultérieur et/ou l'accès et la réutilisation a été autorisé par l'Autorité des données ;

ii. procède à la mise à disposition des données à caractère personnel visées au titre V et des données visées au titre VI dans l'environnement de traitement sécurisé, sous réserve des exigences prévues dans le plan de confidentialité et dans l'autorisation de l'Autorité des données.

Art. 36. Environnement de traitement sécurisé

(1) Le traitement ultérieur de données à caractère personnel visé au titre V et l'accès et la réutilisation de données visés au titre VI se font dans un environnement de traitement sécurisé mis à disposition par l'Autorité des données et géré par le Centre.

L'environnement de traitement sécurisé respecte notamment les mesures de sécurité suivantes:

a) restreindre aux personnes physiques autorisées indiquées dans l'autorisation correspondante visée à l'article 31 l'accès à l'environnement de traitement sécurisé ;

b) réduire au minimum le risque de lecture, de copie, de modification ou de suppression non autorisées des données hébergées dans l'environnement de traitement sécurisé par des mesures techniques et organisationnelles de pointe ;

c) restreindre à un nombre limité d'individus identifiables autorisés l'introduction de données et l'inspection, la modification ou la suppression de données hébergées dans l'environnement de traitement sécurisé ;

d) veiller à ce que les personnes visées au point a) n'aient accès qu'aux données couvertes par leur autorisation correspondante visée à l'article 31, au moyen d'identifiants individuelles et uniques et de modes d'accès confidentiels uniquement ;

e) tenir des registres identifiables de l'accès à l'environnement de traitement sécurisé et des activités qui y sont menées pendant la période nécessaire pour vérifier et contrôler toutes les opérations de traitement dans cet environnement. Les registres d'accès devraient être conservés pendant au moins un an ;

f) veiller à la conformité et contrôler les mesures de sécurité énumérées au présent article afin d'atténuer les menaces potentielles pour la sécurité.

(2) L'environnement de traitement sécurisé doit être aménagé de sorte à ce qu'il ne permet pas :

a) de reproduire les données à l'extérieur de l'environnement et ainsi de les réutiliser dans un autre contexte ou pour des finalités autres qu'autorisées ;

b) d'introduire des solutions technologiques, y compris d'intelligence artificielle, à moins qu'elles aient expressément été inclues dans le plan de confidentialité, ou préalablement été évaluées et certifiées par le Centre, ou par le tiers de confiance mandaté par le Centre, comme ne présentant aucun risque d'atteinte aux exigences visées à l'article 35, paragraphe 1er ;

c) d'introduire des données, à moins que cette introduction ait expressément été demandée conformément à l'article 27, paragraphe 1, point 10° et à l'article 28, paragraphe 1, point 8° et autorisée par l'Autorité des données conformément aux dispositions du présent titre ;

d) d'extraire les données de l'environnement de traitement sécurisé, à moins qu'elles aient préalablement été anonymisées.

(3) Dans les cas visés au paragraphe 2, point b), la certification établie par le Centre, ou par le tiers de confiance mandaté par le Centre, est jointe au plan de confidentialité. Une copie est transmise sans délai à l'Autorité des données.

Pour établir la certification, le Centre, ou le tiers de confiance mandaté par le Centre, peut exiger une évaluation préalable, le cas échéant, sous forme d'audit, établie par un organisme spécialisé, à présenter, dans les cas visés au titre V, par les entités publiques effectuant le traitement de données à caractère personnel ou dans les cas visés au titre VI par les réutilisateurs de données.

(4) Sous réserve de l'autorisation de l'Autorité des données et du respect des conditions prévues par le présent titre, le Centre peut, dans le cadre d'une demande spécifique visée aux articles 27 ou 28 :

a) créer un environnement de traitement sécurisé commun, ensemble avec des organismes compétents désignés conformément à l'article 7 du règlement (UE) 2022/868, afin de mettre les données à disposition des entités publiques ou des réutilisateurs de données ;

b) combiner et traiter les données visées au titre VI avec des données provenant d'environnements de traitement sécurisés d'autres États membres gérés par des organismes compétents désignés conformément à l'article 7 du règlement (UE) 2022/868 afin de les mettre à disposition des réutilisateurs de données.

Art. 37. Responsabilité du traitement

(1) Les entités publiques détenant les données à caractère personnel et les organismes du secteur public détenant les données ont la qualité de responsable du traitement pour la mise à disposition des données à caractère personnel sollicitées à l'Autorité des données conformément à l'article 31, paragraphe 6.

(2) L'Autorité des données a la qualité de responsable du traitement pour le traitement de données à caractère personnel pour l'accomplissement des missions conformément à la présente loi.

(3) Les entités publiques qui traitent ultérieurement les données à caractère personnel et les réutilisateurs de données ont la qualité de responsable du traitement pour les traitements de données à caractère personnel dans l'environnement de traitement sécurisé.

(4) Dans les cas visés aux articles 35 et 36, le Centre agit comme sous-traitant de l'Autorité des données. Le Centre peut sous-traiter ultérieurement les tâches et missions lui attribués conformément à la présente loi.

Section VI – Recours

Art. 38. Recours

Un recours contre les décisions de l'Autorité des données peut être exercé devant le Tribunal administratif qui statue comme juge du fond.

TITRE VIII – Gouvernance en matière de services d'intermédiation de données et d'altruisme des données

Section I – Services d'intermédiation de données

Art. 39. Autorité compétente

La Commission nationale pour la protection des données, désignée ci-après par le terme « CNPD », est l'autorité compétente pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données, telle que visée à l'article 13 du règlement (UE) 2022/868.

Art. 40. Pouvoirs

Dans le cadre des tâches qui lui sont assignées à l'article 39, la CNPD dispose des pouvoirs de contrôle tels que prévus à l'article 14 du règlement (UE) 2022/868.

Art. 41. Procédure

Un règlement interne de la CNPD définit la procédure en matière de notification pour les services d'intermédiation de données, conformément à l'article 11 du règlement (UE) 2022/868.

Art. 42. Redevances

La CNPD peut imposer des redevances proportionnées et objectives pour la notification des services d'intermédiation, conformément à l'article 11, paragraphe 11, du règlement (UE) 2022/868. Un règlement de la CNPD détermine le montant et les modalités de paiement des redevances.

Art. 43. Sanctions

(1) Dans le cadre d'une violation de l'obligation de notification incombant aux prestataires de services d'intermédiation de données en vertu de l'article 11 du règlement (UE) 2022/868 ou des conditions liées à la fourniture de services d'intermédiation de données en vertu de l'article 12 du règlement (UE) 2022/868, la CNPD peut, par voie de décision, imposer des amendes administratives à hauteur de 500 à 100.000 euros aux prestataires de services d'intermédiation de données.

(2) La CNPD peut, par voie de décision, infliger au prestataire de services d'intermédiation de données des astreintes jusqu'à concurrence de 250 euros par jour de retard à compter de la date qu'elle fixe dans sa décision, pour le contraindre :

1° à communiquer toute information demandée par la CNPD en vertu de l'article 14, paragraphe 2, du règlement (UE) 2022/868 ;

2° à respecter une demande de cessation prononcée en vertu de l'article 14, paragraphe 4, du règlement (UE) 2022/868.

(3) Le recouvrement des amendes ou astreintes est confié à l'Administration de l'enregistrement, des domaines et de la TVA. Il se fait comme en matière d'enregistrement.

Section II – Altruisme des données

Art. 44. Autorité compétente

La CNPD est l'autorité compétente responsable du registre public national des organisations altruistes en matière de données reconnues, tel que visé à l'article 23 du règlement (UE) 2022/868.

La CNPD tient et met à jour régulièrement le registre public national des organisations altruistes en matière de données reconnues, conformément à l'article 17, paragraphe 1er, du règlement (UE) 2022/868.

Art. 45. Pouvoirs

Dans le cadre des missions qui lui sont assignées à l'article 44, la CNPD dispose des pouvoirs de contrôle, tels que prévus à l'article 24 du règlement (UE) 2022/868.

Section III – Recours

Art. 46. Recours

Un recours contre les décisions de la CNPD prises en application des sections I et II du présent titre est ouvert devant le Tribunal administratif qui statue comme juge du fond.

TITRE IX – Dispositions finales

Art. 47. Intitulé de citation

La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : « loi du […] relative à la valorisation des données dans un environnement de confiance ».

*

EXPOSE DES MOTIFS

L'évolution rapide des technologies numériques et la mondialisation ont, au cours des dernières années, transformé l'économie et la société, touchant tous les secteurs d'activité et la vie quotidienne. Les données sont au cœur de cette transformation et l'innovation fondée sur celles-ci apportera des avantages considérables aussi bien aux citoyens qu'à l'économie, tout en favorisant les activités de recherche scientifique dans l'intérêt public.

Afin que l'économie et la recherche fondées sur les données soient inclusives à l'égard de tous les citoyens, il faut veiller tout particulièrement à réduire la fracture numérique et à promouvoir une expertise de pointe nationale dans le secteur des technologies. L'économie des données doit être construite de manière à permettre aux entreprises de prospérer, en garantissant la neutralité de l'accès aux données ainsi que la portabilité et l'interopérabilité des données, et en évitant les effets de verrouillage.

Ces évolutions requièrent un cadre de réutilisation des données solide et plus cohérent, assorti d'un contrôle rigoureux des règles via l'intervention d'un organisme compétent autorisant ou refusant les accès et les réutilisation des données détenues par les organismes du secteur public, car il importe de susciter la confiance citoyenne qui permettra à l'économie numérique et à la recherche scientifique de se développer.

C'est pourquoi le règlement (UE) 2022/868 sur la gouvernance des données a pour objectif d'instaurer la confiance entre les citoyens et les acteurs impliqués dans l'accès et la réutilisation des données, en particulier en concevant des mécanismes appropriés permettant le respect des droits individuels dans le contexte de l'accès et de la réutilisation des données à caractère personnel et à caractère non personnel détenues par les organismes du secteur public.

Le règlement (UE) 2022/868 – dont la mise en œuvre relève, depuis l'arrêté grand-ducal du 27 novembre 2023 portant approbation et publication du règlement interne du Gouvernement, du ressort du Ministère de la Digitalisation – est applicable dès le 24 septembre 2023.

Comme il s'agit d'un règlement européen d'application directe, c'est le règlement (UE) 2022/868 qui déterminera la majorité des dispositions de fond, en particulier pour les aspects de l'intermédiation des données (chapitre III) et de l'altruisme des données (chapitre IV). Cependant, il convient de préciser au niveau national les conditions applicables à l'accès et à la réutilisation des données détenues par les organismes du secteur public (chapitre II). Ces conditions doivent être non discriminatoires, transparentes, proportionnées et objectivement justifiées en ce qui concerne les catégories de données et les finalités de la réutilisation, ainsi que la nature des données pour lesquelles la réutilisation est autorisée.

Le projet de loi sous rubrique, qui doit se lire conjointement avec le règlement (UE) 2022/868, complète ainsi ce cadre européen par les dispositions nationales qui s'imposent, en particulier la désignation des organismes compétents, la procédure à suivre pour l'octroi des autorisations d'accès et de réutilisation des données, et les conditions applicables à l'accès et à la réutilisation des données.

Pour des raisons d'économie budgétaire et de gestion efficace des finances publiques, le Commissariat du gouvernement à la protection des données auprès de l'État est désigné comme organisme compétent pour octroyer ou refuser les accès et les réutilisations des données détenues par les organismes du secteur public. En cette qualité, et vu sa longue expérience en tant que structure spécialisée dans le conseil en matière de traitement et de réutilisation de données, il agira comme Autorité des données centralisée conformément au règlement (UE) 2022/868.

En effet, il s'avère excessif de recruter un spécialiste disposant des connaissances et de l'expérience pratique afférente auprès de chacune des plus d'une centaine d'entités étatiques, de chacune des plus d'une centaine de communes luxembourgeoises ainsi qu'auprès de tous les autres organismes de droit public relevant du champ d'application du règlement (UE) 2022/868. De ce fait, il ne reviendrait pas à chaque organisme du secteur public individuellement, mais à l'Autorité des données agissant comme organe central, de veiller au respect des conditions liées à la réutilisation des données. En cette fonction, l'Autorité des données a pour vocation de veiller à une application cohérente de la loi et de mettre à disposition de toutes les entités publiques son expertise juridique dans cette matière complexe à laquelle les administrés sont de plus en plus attentifs au vu des progrès rapides des technologies numériques.

Le Centre des technologies de l'information de l'État et le « *Luxembourg National Data Service* » sont désignés organismes compétents conformément au règlement (UE) 2022/868 pour aider l'Autorité des données dans l'exercice des missions d'octroyer et de refuser les accès et les réutilisations. En outre, ils ont pour mission de mettre en œuvre les mesures imposées par le règlement (UE) 2022/868 et la loi.

Pour éviter d'éventuels conflits d'intérêts et pour maintenir la confiance des citoyens dans une gestion prudente de leurs données par les acteurs publics, la loi prévoit la possibilité pour le Centre des technologies de l'information de l'État de recourir aux services d'un tiers de confiance.

En complément du règlement (UE) 2022/868, et afin de faciliter la mise en œuvre de traitements ultérieurs de données dans le secteur public, le projet de loi sous rubrique prévoit des dispositions spécifiques visant la mise en œuvre du règlement (UE) 2016/679, notamment du chapitre IX. Ainsi, il énonce les finalités pour lesquelles le traitement ultérieur de données à caractère personnel est autorisé, sous réserve du respect des conditions prévues par le projet de loi, et ce nonobstant leur compatibilité avec les finalités initiales du traitement de données à caractère personnel. Dans un objectif d'approche cohérente garantissant l'efficacité du processus décisionnel, la procédure applicable et la répartition des rôles de l'Autorité des données et des organismes compétents susmentionnés sont identiques à celles sous le régime visant la mise en œuvre du règlement (UE) 2022/868.

Dans un objectif de rendre plus rapides et plus efficaces les procédures pour les citoyens et les entreprises, le projet de loi instaure également le principe du « *once only* », qui constitue une priorité du Gouvernement, et selon lequel une personne fournit une seule fois des données aux autorités, au lieu de devoir le faire à plusieurs reprises. Le système proposé fera économiser beaucoup de temps, de ressources et d'argent à tous les acteurs concernés, qu'il s'agisse des citoyens et des entreprises ou de l'administration publique. Le système « *once only* » constitue ainsi une vraie mesure de simplification administrative qui permettra de diminuer les dépenses et favorisera une gestion plus efficace des ressources des entités publiques.

Pour renforcer la sécurité juridique et pour assurer une gestion efficiente des données par les entités publiques dans le respect de la protection des données, le projet de loi sous rubrique explicite, à l'instar des dispositions du « *Bundesdatenschutzgesetz* », la lecture quasi unanime du fondement de licéité prévu par l'article 6, paragraphes 1, point e) et 3 du règlement (UE) 2016/679, des traitements de données opérés par les entités publiques en lien avec l'exécution des missions d'intérêt public ou relevant de l'exercice de l'autorité publique leurs conférées par les dispositions applicables.

Toutes les propositions ont été élaborées en concertation étroite avec les acteurs concernés.

*

COMMENTAIRE DES ARTICLES

Titre I^er – Dispositions préliminaires

Ad article 1^er

Cette disposition précise l'objet de la loi. Il énonce les différents titres prévus par la loi.

Le point 1° précise l'objet du titre II de la loi. La loi vise à renforcer la sécurité juridique en complétant le cadre législatif national concernant le traitement de données à caractère personnel en introduisant en droit luxembourgeois des précisions quant aux traitements de données à caractère personnel effectués par les entités publiques dans le cadre de l'exécution de leurs missions d'intérêts public ou relevant de l'autorité publique dont elles sont investies. L'article 1, paragraphe 1^er, point 1° est sans préjudice des bases de licéité prévues aux articles 6 et 9 du règlement (UE) 2016/679, telles que le traitement de données à caractère personnel qui est nécessaire à l'exécution d'un contrat.

Le point 2° renvoie au titre IV, qui instaure le principe du « *once only* ».

Le point 3° énonce l'objet du titre V de la loi, qui règle le traitement ultérieur de données à caractère personnel mis en œuvre par les entités publiques pour les finalités que la loi autorise.

Le point 4° renvoie au titre VI qui met en œuvre le règlement (UE) 2022/868 en prévoyant un cadre spécifique à la réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public.

La loi contient aussi des précisions relatives aux services d'intermédiation de données et à l'altruisme en matière de données (points 5° et 6°).

En revanche, la loi s'applique sans préjudice des dispositions plus spécifiques relatives au traitement de données à caractère personnel. De ce fait, les traitements de données à caractère personnel opérés sur base d'un autre fondement de licéité prévu par le règlement (UE) 2016/679, notamment parce qu'ils sont prévus par une disposition légale, restent possibles.

A titre d'exemple, l'Inspection générale de la sécurité sociale est tenue de réaliser des analyses et des études à des fins d'évaluation et de planification des régimes de protection sociale et de recueillir à ces fins les données auxquelles elle a accès en vertu des dispositions légales et réglementaires en vigueur, de les centraliser, de les traiter et de les gérer sous forme pseudonymisée (article 423, point 4° du Code de la sécurité sociale). Encore peut-on citer, à titre d'illustration des traitements de données à caractère personnel qui restent intouchés par les dispositions de la présente loi, les traitements de données nécessaires à l'exécution des missions conférées à l'Observatoire national de la Santé par la loi du 2 mars 2021 portant création d'un Observatoire national de la santé ou ceux relatifs à la gestion et à la tenue du registre national des personnes physiques opérés par le Centre des technologies de l'information de l'État, sous l'autorité du ministre ayant le Centre dans ses attributions.

Dans ce contexte, il échet également de noter que la loi s'applique sans préjudice de la possibilité d'effectuer des traitements ultérieurs de données à caractère personnel effectué dans le respect du principe de compatibilité des finalités prévu à l'article 5, paragraphe 1^er, point b) du règlement (UE) 2016/679, lu en combinaison avec l'article 6, paragraphe 4 du même règlement.

Par ailleurs, les dispositions de la loi n'ont pas vocation à remplacer la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public, ni à remplacer la loi modifiée du 14 septembre 2018 relative à une administration transparente et ouverte, ou de porter préjudice aux dispositions sectorielles, telles que la loi du 17 août 2018 relative à l'archivage.

Ad article 2

Cet article définit les notions employées dans la loi.

A moins que disposées autrement, les définitions prévues par le règlement (UE) 2022/868 et le règlement (UE) 2016/679 s'appliquent à la loi.

L'article prévoit, pour des raisons de sécurité juridique, une définition en droit interne du terme « anonymisation ». La définition repose sur le texte du considérant (26) du règlement (UE) 2016/679 et s'inspire des enseignements des autorités de protection des données nationales et européennes. Elle tient compte de la neutralité technologique.

La notion d'« entité publique » a été insérée expressément pour énumérer les entités concernées par les dispositions du titre IV relatif à l'échange d'informations et de données à caractère personnel entre

entités publiques (« *once only* »), d'une part, et du titre V relatif au traitement ultérieur de données à caractère personnel par les entités publiques à des fins autorisées par la loi, d'autre part.

A l'instar des dispositions de l'article 2 du règlement (UE) 2016/679 et de l'article 1er de la directive (UE) 2016/680[1] transposée en droit luxembourgeois par la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, la définition exclut les autorités compétentes en matière pénale ainsi qu'en matière de sécurité nationale de son champ d'application et, de ce fait, du champ d'application des titres IV et V de la loi.

A la lumière des dispositions de l'article 5 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, réglementant le champ de compétence de la CNPD, sont également exclues du champ d'application les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif, lorsqu'elles effectuent un traitement de données à caractère personnel dans l'exercice de leurs fonctions juridictionnelles.

La notion d'« entité publique » est partant volontairement distincte de la notion d'organisme du secteur public visée par les dispositions du règlement (UE) 2022/868. Elle permet de limiter avec précision le champ d'application des échanges d'informations et de données à caractère personnel dans le cadre du principe « *once only* » aux Ministères, y compris leurs services, administrations et aux communes luxembourgeoises. Sont également visés par la notion d'entité publique, les établissements publics luxembourgeois, les groupements d'intérêts économiques ainsi que les personnes morales d'utilité publique, telles que les fondations et associations sans but lucratif, notamment les hôpitaux au sens de la loi modifiée du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière, qui sont listés expressément par règlement grand-ducal aux fins d'application du titre IV et/ou du titre V.

Pour des raisons de sécurité juridique et d'application des dispositions relatives au traitement ultérieur et à la réutilisation des données, la loi précise la notion de « tiers de confiance ».

Titre II – Traitement de données à caractère personnel par les entités publiques nécessaire à l'exécution des missions d'intérêt public ou relevant de l'exercice de l'autorité publique

Ad article 3

L'objectif du présent article est de renforcer la sécurité juridique en matière de traitement de données à caractère personnel par les entités publiques dans le cadre de l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies.

Il reprend en droit national le cas d'ouverture pour le traitement de données à caractère personnel prévu à l'article 6, paragraphe 1er, point e) du règlement (UE) 2016/679, à l'instar du « Bundesdatenschutzgesetz » allemand dont l'article 3 dispose :

> « *Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist* »

Conformément à l'article 6, paragraphe 1er, point e) du règlement (UE) 2016/679, cette disposition autorise les entités publiques à traiter les données à caractère personnel dès lors que leur traitement est nécessaire aux fins de l'exécution de leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies par une disposition de droit de l'Union européenne ou de droit luxembourgeois, par opposition à l'article 6, paragraphe 1er, point c) du même règlement qui concerne l'obligation de traiter certaines données à caractère personnel.

La distinction entre ces deux bases de licéité prévues à l'article 6, paragraphe 1er du règlement (UE) 2016/679 peut paraître fine, mais elle est importante.

---

1 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Ainsi, si l'obligation légale de traiter des données à caractère personnel prévue à l'article 6, paragraphe 1er, point c) du règlement (UE) 2016/679 nécessite un fondement en droit interne ou européen qui définit les finalités du traitement, il suffit, d'après l'article 6, paragraphe 3 du règlement (UE) 2016/679 que le traitement de données à caractère personnel prévu à l'article 6, paragraphe 1er, point e) du règlement (UE) 2016/679 soit nécessaire à « *l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* ». Dans ce second cas de figure, la définition des finalités dans un texte spécifique n'est pas requise.

Comme souligné par la Commission nationale de l'informatique et des libertés française (CNIL), « *comme pour toute autorité publique, la mission d'intérêt public peut donc fonder des traitements de données de nature diverse, dès lors qu'ils sont mis en œuvre aux fins du bon exercice des missions légales qui incombent à ces autorités et dans des conditions qui n'excèdent pas ce qui est nécessaire au regard de cet objectif* ».

Ainsi, le fait pour une administration de pouvoir démontrer qu'elle a reçu dans ses prérogatives des missions spécifiques nécessitant la collecte de certaines données à caractère personnel auprès de personnes concernées pour atteindre les finalités de ces missions suffit pour légitimer la collecte et le traitement de ces données. Cette lecture s'impose également à la lumière du considérant (45) du règlement (UE) 2016/679 qui confirme le caractère facultatif des spécifications pouvant, selon l'article 6, paragraphe 2 du règlement (UE) 2016/679, être introduites en droit interne (« pourrait préciser »).

De ce fait, le principe même que les entités publiques sont en droit de traiter des données à caractère personnel « nécessaires » à l'accomplissement de leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies, et ce sans devoir recourir à une autre base légale spécifique au traitement de données, découle de l'article 6, paragraphe 1er, point e) du règlement (UE) 2016/679.

La Cour de Justice de l'Union européenne a récemment confirmé cette lecture dans l'arrêt C-175/20 « *Valsts ieņēmumu dienests* » du 24 février 2022. Dans le cadre d'une demande de communication de données émanant de l'administration fiscale à l'adresse d'un prestataire de services d'annonces, qui énonçait clairement les finalités, la Cour a décidé :

> « *69. Pourvu que les finalités ainsi énoncées dans ladite demande soient nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investie l'administration fiscale, cette circonstance suffit, ainsi qu'il découle de l'article 6, paragraphe 1, premier alinéa, initio et sous e), du règlement 2016/679, lu conjointement avec l'article 6, paragraphe 3, second alinéa, de ce règlement, pour que lesdits traitements satisfassent également à l'exigence de licéité rappelée au point 66 du présent arrêt.*
>
> *70. À cet égard, il convient de rappeler que la perception de l'impôt et la lutte contre la fraude fiscale doivent être considérées comme étant des missions d'intérêt public, au sens de l'article 6, paragraphe 1, premier alinéa, sous e), du règlement 2016/679 (voir, par analogie, arrêt du 27 septembre 2017, Puškàr, C-73/16, EU :C :2017 :725, point 108).*
>
> *71. Il s'ensuit que, dans un cas où la communication des données à caractère personnel en cause n'est pas directement fondée sur la disposition légale qui en constitue le fondement, mais résulte d'une demande de l'autorité publique compétente, il est nécessaire que cette demande précise quelles sont les finalités spécifiques de cette collecte de données au regard de la mission d'intérêt public ou de l'exercice de l'autorité publique, afin de permettre au destinataire de ladite demande de s'assurer que la transmission des données à caractère personnel en cause est licite et aux juridictions nationales d'opérer un contrôle de la légalité des traitements concernés* ».

Cette lecture de la suffisance de la nécessité du traitement de données pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique est également partagée par nos pays voisins.

Aux Pays-Bas, les restrictions au principe constitutionnel du droit à la vie privée doivent être prévues par la loi (article 10 de la Constitution néerlandaise). Cependant, il est constant en droit néerlandais

que le règlement (UE) 2016/679 réponde aux exigences constitutionnelles et constitue de ce fait une base suffisante permettant une restriction au droit à la vie privée[2].

En Belgique, la pratique décisionnelle va dans le même sens. Ainsi, l'Autorité de protection des données belge estime que l'existence d'une mission d'intérêt public ou d'une autorité publique attribuée à l'entité publique suffit, au sens de l'article 6, paragraphe 1er, point e) du règlement (UE) 2016/679, lu en combinaison avec l'article 6, paragraphe 3 dudit règlement, pour justifier une restriction au principe constitutionnel de la protection de la vie privée.

En d'autres termes, l'Autorité de protection des données belge paraît se limiter à vérifier uniquement si la mission d'intérêt public ou l'autorité publique au sens de l'article 6, paragraphe 1er, point e) du règlement (UE) 2016/679 existe en application du droit interne belge. En revanche, elle ne requiert pas qu'une base légale détaille tous les éléments essentiels du traitement de données à caractère personnel[3].

Le Conseil d'État luxembourgeois paraît retenir une position similaire. Dans cet ordre d'idées, il a précisé dans son avis par rapport au projet de loi qui a donné lieu à la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données :

> « *Le Conseil d'État voudrait ajouter deux observations concernant les implications de l'adoption de la loi sous examen. La première est relative à la pratique actuelle d'insérer dans les lois organiques des différentes administrations ou dans d'autres lois du secteur public des dispositions particulières sur le traitement des données à caractère personnel. Aux termes de l'article 6 du règlement, la licéité du traitement dans le secteur public est vérifiée si le traitement est nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique. Dans cette logique, il ne s'impose pas de donner à chaque traitement de données une base spécifique légale ou réglementaire.* »

---

2 « *Verschillende van deze aspecten hebben een specifieke grondwettelijke garantie in artikel 10, tweede en derde lid, in artikel 11, in artikel 12 en artikel 13. In artikel 10, tweede en derde lid, zijn twee opdrachten aan de wetgever opgenomen. In de eerste plaats dient de wet regels te stellen ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. In de tweede plaats moet de wet regels stellen voor het inzagerecht en voor het recht op verbetering van onjuiste persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG) voorziet materieel grotendeels in de regelgeving waartoe artikel 10, tweede en derde lid, van de Grondwet opdraagt.* », traduction libre : « *Plusieurs de ces aspects font l'objet de garanties constitutionnelles spécifiques dans les articles 10, paragraphes 2 et 3, 11, 12 et 13. L'article 10, paragraphes 2 et 3, contient deux mandats pour le législateur. Premièrement, la loi doit fixer des règles pour protéger la vie privée dans le cadre de l'enregistrement et de la fourniture de données à caractère personnel. Deuxièmement, la loi doit fixer des règles relatives au droit de regard et au droit de rectification des données à caractère personnel inexactes. Le règlement général sur la protection des données (RGPD) prévoit en grande partie la réglementation requise par l'article 10, paragraphes 2 et 3, de la Constitution*. »

3 Autorité de protection des données belge, décision quant au fond no. 149/2022 du 18 octobre 2022, DOS-2021-06293 et DOS-2021-06884 : « *30. Conformément au considérant 41 du RGPD, cette base juridique ou mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la CEDH. Dans l'arrêt Rotaru[3], la CEDH a défini plus précisément la notion de prévisibilité de la base juridique. Cette affaire ayant trait aux systèmes de surveillance de l'appareil sécuritaire d'un état, son contexte diffère de la présente affaire. Dans d'autres affaires, la CEDH a en effet indiqué qu'elle pouvait s'inspirer de ces principes, mais elle estime que ces critères, établis et suivis dans le contexte spécifique de cette affaire concrète, ne sont donc pas applicables en tant que tels à toutes les affaires[4]. […] 37. À cet égard, la Chambre Contentieuse a déjà souligné dans sa décision 124/2021 du 10 novembre 2021 que les missions d'intérêt public ou relevant de l'exercice de l''autorité publique dont sont investis les responsables de traitement ne sont souvent pas basées sur des obligations ou des normes législatives circonscrites avec précision répondant aux exigences mentionnées aux points 29 e.s. Les traitements ont plutôt lieu sur la base d'une autorisation d'agir plus générale, tel que c'est nécessaire pour l'accomplissement de la mission, comme c'est le cas en l'espèce. Il en résulte que**, dans la pratique, la base légale en question ne contient souvent aucune disposition décrivant concrètement les traitements de données nécessaires. Les responsables du traitement qui souhaitent invoquer l'article 6, paragraphe 1, e), du RGPD sur la base d'une telle base légale doivent effectuer eux-mêmes une pondération entre la nécessité du traitement pour la mission d'intérêt public et les intérêts des personnes concernées.** » (mise en évidence ajoutée).

4 Conseil d' État, avis du 30 mars 2018, Projet de loi n° 7184 portant création de la Commission nationale pour la protection des données et la mise en œuvre du 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, portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État et abrogeant la loi du 2 août 2002 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Voir également M. Besch, *Normes et légistique en droit public luxembourgeois*, Larcier, 2019, 469 et s.

Cette lecture conforme aux dispositions de l'article 6, paragraphe 1er, point e) et paragraphe 3 du règlement (UE) 2016/679, telles qu'interprétées par la Cour de Justice européenne (voir *supra*), reste à ce jour admissible aux termes de l'article 31 de la Constitution, en particulier au regard du principe de primauté du droit de l'Union européenne rappelé récemment par la Cour de Justice de l'Union européenne dans une affaire liée à l'interprétation du règlement (UE) 2016/679[4].

Pour renforcer la sécurité juridique et pour expliciter la lecture quasi unanime du fondement de licéité des traitements de données opérés par les entités publiques en lien avec l'exécution des missions d'intérêt public ou avec l'exercice de l'autorité publique leurs conférées par les dispositions applicables, il paraît (et à l'instar des dispositions du « *Bundesdatenschutzgesetz* ») opportun d'adopter explicitement, en droit luxembourgeois, le principe prévu par l'article 6, paragraphes 1er, point e) et 3 du règlement (UE) 2016/679.

Ainsi, le fait pour une entité publique de pouvoir démontrer le respect de la double condition : premièrement qu'elle soit investie d'une mission d'intérêt public ou qui relève de l'exercice de l'autorité publique[5] dont elle est investie et, deuxièmement, que le traitement de données à caractère personnel soit « nécessaire » pour réaliser cette mission, suffit à légitimer la collecte et le traitement des données en question.

A titre illustratif, les missions des centres de recherche publics instaurés par la loi du 3 décembre 2014 ayant pour objet l'organisation des centres de recherche publics sont clairement énoncées en son article 4[6]. Outre les missions générales, des missions spécifiques à chaque centre de recherche sont listées explicitement dans le texte. De ce fait, si les traitements de données à caractère personnel opérés par les centres de recherche publics sont « nécessaires » pour réaliser lesdites missions, cela suffit pour légitimer les traitements de données en question. En revanche, il n'est pas requis qu'une loi nationale spécifique énumère chaque projet de recherche séparément et liste pour chacun d'entre eux les données à collecter, les catégories de personnes concernées, les finalités spécifiques, les responsables du traitement ou encore les durées de conservation nécessaires.

---

4 CJUE, affaire C-33/22, Österreichische Datenschutzbehörde, arrêt du 16 janvier 2024, point 70 : « *En outre, il importe de rappeler que le fait pour un État membre d'invoquer des dispositions de droit national ne saurait porter atteinte à l'unité et à l'efficacité du droit de l'Union. En effet, les effets s'attachant au principe de primauté du droit de l'Union s'imposent à l'ensemble des organes d'un État membre, sans, notamment, que les dispositions internes, y compris d'ordre constitutionnel, puissent y faire obstacle [arrêt du 22 février 2022, RS (Effet des arrêts d'une cour constitutionnelle), C-430/21, EU:C:2022:99, point 51 et jurisprudence citée]* ».

5 Dans ce contexte, il suffit que le fondement juridique conférant une mission d'intérêt public à une entité publique respecte le principe de la hiérarchie de normes. En effet, rien n'empêche notamment que la mission d'intérêt public à exécuter par une commune luxembourgeoise soit prévue par un règlement communal adopté conformément aux dispositions de la loi communale du 13 décembre 1988, tel qu'il est notamment le cas en matière de stationnement payant ou de gestion des déchets.

6 L'article 4 de la loi du 3 décembre 2014 ayant pour objet l'organisation des centres de recherche publics dispose ce qui suit : « *(1) Les centres de recherche publics ont pour missions générales :*

a) de développer et d'entreprendre des activités de recherche fondamentale orientée et de recherche appliquée, support nécessaire aux activités de recherche, de développement et d'innovation;

b) d'opérer le transfert de connaissances et de technologies vers le secteur public et le secteur privé.

(2) Dans l'accomplissement de leurs missions, les centres de recherche publics sont appelés à :

a) stimuler et entreprendre des activités de recherche, de développement et d'innovation en vue de maintenir et de développer leurs compétences scientifiques et technologiques;

b) réaliser au plan national et international des activités de recherche contractuelle et de recherche collaborative avec des organismes, des institutions, des sociétés et des établissements de recherche, de développement et d'innovation ainsi que de la recherche compétitive via des programmes de recherche, de développement et d'innovation nationaux, européens ou internationaux;

c) favoriser la valorisation scientifique, économique et socio-économique de leurs résultats de recherche, de développement et d'innovation et le déploiement de nouvelles activités économiques;

d) réaliser des activités d'études, d'expertises ainsi que de conseil lors de la mise en œuvre de technologies, produits, processus et services nouveaux en se basant sur leur recherche fondamentale orientée et recherche appliquée;

e) contribuer à la formation du personnel de recherche par l'encadrement des doctorants et la participation à des écoles doctorales ainsi qu'à favoriser la mobilité de leur personnel de recherche;

f) contribuer à l'apprentissage et à l'actualisation des connaissances tout au long de la vie dans les domaines qui relèvent de leur compétence;

g) contribuer au développement de la culture scientifique;

h) contribuer par leurs activités de recherche, de développement et d'innovation à la définition, à la mise en œuvre et à l'évaluation des politiques nationales ».

De même, cela couvre également des activités intrinsèquement liées aux missions conférées aux entités publiques, telles que la publication de l'annuaire des entités publiques, l'échange des comptes rendus de réunions par voie de courriels ou la tenue d'un agenda de réunions dans lequel sont inscrits les participants.

Dans ce sens, la Commission nationale de l'informatique et des libertés (CNIL) indique dans son registre des traitements publié sur son site Internet, l'exécution de la mission d'intérêt public (article 6, paragraphe 1er, point e) du règlement (UE) 2016/679) comme fondement de licéité, notamment, pour les traitements de données liés à « *l'envoi par messagerie électronique (emailing) d'informations sur l'actualité ou sur des actions particulières réalisées par la CNIL* » ou pour ceux liés à la production et le partage de la doctrine via le canal d'une plateforme électronique (ce qui implique l'identification des utilisateurs, la gestion des profils utilisateurs, les contributions, les abonnements aux notifications, l'historisation des actions, etc.)[7].

En tout état de cause, il paraît difficilement concevable que le législateur adopte pour chacun des traitements de données à caractère personnel nécessaires au bon fonctionnement et à la réalisation des missions des entités publiques (dont le nombre d'hypothèses est en réalité considérable voire illimité) une loi spécifique au sens formel.

Titre III – Acteurs compétents en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation des données

Ad article 4

L'article 7 du règlement (UE) 2022/868 impose aux États membres la désignation d'un ou de plusieurs organismes compétents.

Dans ce cadre, conformément à l'article 7 paragraphe 2 du règlement (UE) 2022/868, l'État membre peut désigner un « organisme compétent » avec pour mission d'octroyer ou de refuser les accès et les réutilisations de certaines catégories de données protégées détenues par des organismes du secteur public, dont les données à caractère personnel ainsi que les données protégées pour des motifs de confidentialité commerciale (y compris le secret d'affaires, le secret professionnel et le secret d'entreprise), de secret statistique, ou de protection des droits de propriété intellectuelle de tiers.

Pour des raisons de cohérence et d'économie budgétaire, cette option est mise en œuvre par la création d'une Autorité des données centralisée. En effet, il s'avère excessif de recruter un spécialiste disposant des connaissances et de l'expérience pratique afférente auprès de chacune des plus d'une centaine d'entités étatiques ainsi qu'auprès de chacune des plus d'une centaine de communes luxembourgeoises et des autres organismes de droit public relevant du champ d'application du règlement (UE) 2022/868.

De ce fait, il ne reviendrait pas à chaque organisme du secteur public individuellement, mais à l'organisme compétent agissant comme organe central, de veiller au respect des conditions liées à la réutilisation des données.

En tant que structure centrale spécialisée disposant d'une longue expérience dans le conseil en matière de traitement et de réutilisation de données, il apparait indiqué de désigner le Commissariat du gouvernement à la protection des données auprès de l'État comme organisme compétent habilité à octroyer ou refuser les accès et les réutilisations des données au sens dudit règlement européen. Le Commissariat a ainsi pour vocation de mettre à disposition de toutes les entités publiques son expertise juridique dans cette matière complexe à laquelle les administrés sont de plus en plus attentifs au vu des progrès rapides des technologies numériques.

Cette approche assure la cohérence des actions et contribue à une économie d'échelle substantielle aux fins d'une gestion efficace des finances publiques.

Dans un même ordre d'idée, l'Autorité des données aura pour mission d'autoriser ou de refuser le traitement ultérieur de données à caractère personnel par les entités publiques aux conditions établies par la loi.

En parallèle, elle fonctionnera comme organe de réflexion dans les domaines du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation des données. Dans ce contexte,

7 https://www.cnil.fr/sites/cnil/files/2023-07/registre_rgpd_de_la_cnil_juin_2023.pdf

l'Autorité des données sera notamment chargée de formuler des avis et des propositions en la matière au ministre ayant la digitalisation dans ses attributions, de proposer des mesures en la matière ou de conseiller, sur demande, le ministre précité. Elle doit également promouvoir les bonnes pratiques et sensibiliser les acteurs ainsi que le public en la matière, notamment par le biais de séances de formation et d'information du public.

Au vu des missions actuelles du Commissariat du gouvernement à la protection des données auprès de l'État et des nouvelles fonctions de l'Autorité des données, il parait opportun de préciser que le personnel impliqué dans le traitement d'une demande de traitement ultérieur du titre V ou d'accès et de réutilisation des données du titre VI ne doit pas avoir été, ou être, impliqué en amont dans la préparation d'une demande en qualité de délégué à la protection des données. Cette séparation fonctionnelle permet d'éviter d'éventuelles situations de conflits d'intérêts.

A noter qu'une telle séparation fonctionnelle n'est pas novatrice. Elle est régulièrement envisagée dans le cadre de l'organisation d'autres autorités qui se voient confier des missions qui sont susceptibles d'aboutir à d'éventuels conflits d'intérêts. Citons certaines autorités de contrôle, pour lesquelles une séparation fonctionnelle est mise en place entre les pouvoirs d'enquête et de prise de décision afin d'assurer l'indépendance des services habilités à conduire l'enquête ainsi que le caractère impartial de la décision finale. A titre d'exemple, la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données et le règlement d'ordre intérieur de la CNPD prévoient une séparation fonctionnelle entre les pouvoirs d'enquête exercés par le chef d'enquête et les pouvoirs de sanction exercés par la formation restreinte de la CNPD, le chef d'enquête n'étant en tout état de cause pas autorisé à siéger, ni à délibérer lorsque la formation restreinte de la CNPD se prononce sur l'issue de l'enquête.

Par ailleurs, cette solution permettrait également d'allouer efficacement les ressources adéquates à l'exercice de chacune de ces fonctions au sein de l'Autorité des données.

Ad article 5

Conformément à l'article 7 du règlement (UE) 2022/868, les États membres peuvent désigner des organismes du secteur public ayant pour mission d'aider l'organisme du secteur public qui octroie ou refuse l'accès aux fins de la réutilisation des catégories de données (à savoir l'Autorité des données visée à l'article 4 du projet).

Le Centre des technologies de l'information de l'État (Centre) ainsi que le groupement d'intérêt économique Plateforme nationale d'échange de données (LNDS) sont désignés à cette fin.

Les missions du Centre et du LNDS sont prévues aux paragraphes 2 et 3. Elles n'appellent pas d'observations particulières.

Dans un objectif de renforcer la confiance du public, les paragraphes 4 et suivants prévoient des conditions relatives au personnel du Centre et du LNDS, dont notamment l'indépendance fonctionnelle. Le personnel qui assure la réalisation des missions conférées au tiers de confiance doit être nominativement désigné par ce dernier.

L'article sous examen, précise l'obligation de secret que doivent respecter les deux acteurs. Cette disposition énonce le principe d'interdiction de communication d'informations à un tiers permettant la réidentification ou étant susceptible de porter préjudice aux droits à la protection des données, à la propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, le secret professionnel, le secret d'entreprise et le secret statistique. A l'instar de l'article 41 de la loi du 19 juin 2013 relative à l'identification des personnes physiques, ne sont pas visés par cette interdiction les acteurs habilités par ou en vertu de la loi à recevoir communication desdites informations.

Afin de se prémunir de tout risque de conflits d'intérêts, les personnels du Centre et du LNDS ne sauraient exercer une activité qui ne se concilie pas avec leurs missions.

Le paragraphe 6 de l'article sous examen prévoit également l'application de l'article 458 du Code pénal relatif au secret professionnel au personnel. Cette disposition n'est pas prévue de porter préjudice à une éventuelle sous-traitance, en particulier informatique, du CTIE ou du LNDS à des prestataires externes.

A noter, à toutes fins utiles, que le Centre peut charger le LNDS ou d'autres prestataires d'exécuter des tâches en sous-traitance. Dans pareil cas de figure, les dispositions de l'article 28 du règlement (UE) 2016/679 sont applicables dans la mesure où cette sous-traitance implique le traitement de données à caractère personnel pour le compte du Centre.

Ad article 6

Pour renforcer les mesures et garanties appliquées aux processus d'anonymisation et de pseudonymisation des données à caractère personnel et de méthode de contrôle de la divulgation des données à caractère non personnel protégées, il est dans certaines hypothèses nécessaire que les informations permettant la réidentification des acteurs soient gérées de façon à en garantir la confidentialité.

Par sa neutralité, le tiers de confiance constitue le garant essentiel de la non réidentification des personnes concernées dans le cadre du traitement ultérieur ou de la réutilisation des données à caractère personnel visés au titre V et VI de la loi sous examen.

L'article sous examen, instaure l'obligation de secret pour le tiers de confiance. Cette disposition énonce ainsi le principe d'interdiction de communication d'informations permettant la réidentification ou étant susceptibles de porter préjudice aux droits à la protection des données, à la propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique. A l'instar de l'article 41 de la loi du 19 juin 2013 relative à l'identification des personnes physiques, ne sont pas visés par cette interdiction les acteurs habilités par ou en vertu de la loi à recevoir communication desdites informations.

Comme pour le Centre et le LNDS, au vu de l'importance de ses missions, afin de garantir la protection appropriée des données faisant l'objet d'un traitement ultérieur et d'une réutilisation des données ainsi que de renforcer la confiance des personnes concernées, l'article sous examen prévoit des conditions relatives au personnel du tiers de confiance. Ainsi, le personnel qui assure la réalisation des missions conférées au tiers de confiance doit être nominativement désigné par ce dernier.

En outre, pour éviter tout risque de conflit d'intérêt, des restrictions supplémentaires sont prévues pour le personnel telles que l'impossibilité d'exercer une activité qui ne se concilie pas avec les missions du tiers de confiance conférées par la loi, ou l'absence d'intérêt dans le traitement ultérieur ou l'accès et la réutilisation prévus par le projet de loi. L'article sous examen prévoit également l'application de l'article 458 du Code pénal relatif au secret professionnel au personnel du tiers de confiance. A noter que cette disposition n'est pas prévue de porter préjudice à une éventuelle sous-traitance, en particulier informatique, du tiers de confiance à des prestataires externes.

Ad article 7

Conformément à l'article 8 du règlement 2022/868, l'article sous examen instaure un point d'information unique sous l'autorité du ministre ayant la digitalisation dans ses attributions. Il prévoit la possibilité pour le ministre ayant la digitalisation dans ses attributions de sous-traiter les missions du point d'information unique au groupement d'intérêt économique Plateforme nationale d'échange de données (LNDS).

Cette disposition n'appelle pas d'observation particulière.

Ad article 8

L'article 8 instaure le Conseil consultatif de la valorisation des données dans un environnement de confiance (ci-après désigné « Conseil consultatif »), qui a notamment pour mission de régler d'éventuelles difficultés d'application de la loi en rendant des avis à l'Autorité des données, aux entités publiques et aux organismes de droit public dans le cadre du traitement ultérieur de données à caractère personnel et de la réutilisation des données. En complément, le Conseil consultatif a pour mission de fonctionner comme organe de réflexion en la matière.

Un règlement grand-ducal précise la composition, le mode de fonctionnement et les attributions du Conseil consultatif. Le projet de règlement grand-ducal a été rajouté au projet de loi.

Le système ainsi prévu fait le parallèle avec le Conseil national des archives instauré conformément aux dispositions de la loi du 17 août 2018 relative à l'archivage. Il s'inspire également des dispositions de l'article 11 de la loi du 19 juin 2013 relative à l'identification des personnes physiques.

Titre IV – Informations et données à caractère personnel obtenues par les entités publiques auprès d'une autre entité publique

Ad article 9

L'article vise à simplifier voire supprimer certaines démarches administratives pesant lourdement sur les administrés dans le cadre de la présentation d'une demande ou d'une déclaration auprès d'une entité publique.

Il entend faciliter le traitement par les entités publiques des demandes et déclarations présentées par les administrés, d'une part, en obligeant les entités publiques à échanger entre elles toutes informations, données à caractère personnel ou pièces justificatives nécessaires au traitement desdites demandes ou déclarations et, d'autre part, en permettant aux administrés ayant déjà produit des pièces justificatives auprès d'une entité publique de ne pas être tenus de les produire à nouveau. Ainsi, un administré n'aurait plus à présenter par lui-même ces informations et données à caractère personnel, dès lors que l'entité publique auprès de laquelle il présente la demande ou la déclaration est en mesure de les obtenir directement auprès de l'entité publique.

En d'autres termes, l'article érige en obligation légale le traitement de données à caractère personnel nécessaire pour la mise en œuvre du présent titre par les entités publiques. Les échanges de données à caractère personnel sont dès lors fondés sur les dispositions de l'article 6, paragraphe 1er, lettre c) et, pour autant que des catégories de données à caractère personnel sont concernées, de l'article 9, paragraphe 2, lettre g) du règlement (UE) 2016/679.

Par ailleurs, lorsque les informations et données à caractère personnel ne sont pas encore détenues par les entités publiques, l'administré présentant la demande ou produisant la déclaration est tenu de les produire lui-même. Tel est notamment le cas si l'administré est le seul à disposer d'une facture nécessaire pour solliciter une aide financière (ex. acquisition d'un véhicule électrique).

L'article renforce ainsi la communication des informations et des données à caractère personnel entre les entités publiques et donne un cadre législatif à ces échanges dans l'intérêt de l'administré. Ceci contribue à la modernisation de l'action publique et permet d'améliorer la prise de décision efficace au sein des entités publiques. Dans cet esprit, il y a lieu d'encourager les entités publiques à mettre au point des formats interopérables permettant la disponibilité des informations et données à caractère personnel et la mise en œuvre efficace du « *once only* ».

En effet, de nombreux freins à la bonne circulation des informations et des données à caractère personnel entre les entités publiques ont pu être identifiés. Ces freins ont des impacts importants en termes budgétaires, sociologiques et juridiques. Ils entraînent également des conséquences sous-optimales en termes de qualité, d'efficience et de réactivité de l'action publique et peuvent susciter des effets de renoncement à la donnée (notamment par manque de connaissances ou par abandon de l'administré) ou de stratégies de contournement (notamment par la constitution de bases de données équivalentes à celles déjà produites par une autre administration).

L'introduction en droit interne luxembourgeois d'une obligation générale de transmission des informations et des données à caractère personnel entre entités publiques permettra de réduire les coûts administratifs en supprimant le temps passé par les entités publiques à examiner la possibilité juridique de transmettre des données à caractère personnel à une autre entité publique, qui serait chargée de traiter lesdites informations dans l'exercice de ses missions d'intérêt public.

En outre, l'article participe à l'amélioration de la circulation des informations et des données à caractère personnel entre entités publiques. De ce fait, il est de nature à engendrer plusieurs externalités positives, notamment en termes de productivité et de gain de temps. En posant un principe et une obligation générale d'échange de données entre administrations dans le cadre d'une demande ou d'une déclaration présentée par l'administré, l'article en question développe également des effets de réseau entre les entités publiques, ce qui permet un meilleur usage coordonné des données produites par les entités publiques. En conséquence, il contribue à un renforcement de la transparence de l'action publique et à la réalisation de gains de productivité en termes budgétaires et socioéconomiques.

Par ailleurs, l'article mettra fin aux situations parfois irrationnelles où un administré doit produire à plusieurs reprises un même document administratif auprès de différentes entités publiques dans le cadre d'une demande ou d'une déclaration présentée à ces dernières. Pour contrecarrer ce problème, l'article constitue un allégement substantiel de la charge des formalités administratives imposées aux administrés et un moyen efficace dans la lutte contre la fraude en sécurisant la production et la transmission des informations, des données à caractère personnel et des pièces justificatives.

En d'autres mots, le système « *once only* » constitue une vraie mesure de simplification administrative qui repose, pour le traitement des demandes et déclarations des administrés, sur trois caractéristiques essentielles, à savoir :

- la réalisation d'une démarche à l'initiative de l'administré ;
- la limitation des informations et des données à caractère personnel échangées à celles strictement nécessaires à la démarche initiée par l'administré ;

- la possibilité, pour les seules entités publiques agissant dans le cadre de leurs missions légales ou réglementaires, et régulièrement habilitées à connaître ces informations et données, de bénéficier de ces échanges.

Le système proposé constitue dès lors une réforme majeure de nature à simplifier les démarches administratives pour la population. Il permettra également de diminuer les dépenses et favorisera une gestion plus efficace des ressources des entités publiques. En effet, répondre à une autre entité publique selon un cadre prédéfini est vraisemblablement plus simple que de traiter des demandes ou déclarations, y compris les pièces, revêtant différentes formes et provenant de différents canaux de communication (ex. via MyGuichet, par accès au bureau compétent, par téléphone, par courrier, par fax) ou comprenant des erreurs commises notamment par les administrés.

Ainsi, la disposition sous examen contribue directement à une approche proactive des pouvoirs publics et ce dans l'intérêt de tous les administrés, qui font face à une complexité de plus en plus importante du cadre réglementaire, et ce dans le respect des exigences de la protection des données.

En effet, le système d'échange français, sur lequel repose le texte proposé, a été validé par le Conseil d'État français et a été avisé positivement par la Commission nationale de l'informatique et des libertés française (CNIL) comme étant conforme aux exigences prévues par le règlement (UE) 2016/679.

La CNIL note dans ce cadre expressément que la simplification des démarches administratives et l'amélioration des relations entre le public et les administrations constituent des objectifs légitimes. Elle a, en outre, souligné que l'atteinte à la vie privée apparaît faible dans le cadre d'un système d'échanges d'informations et de données à caractère personnel automatique entre entités publiques aux fins de répondre aux demandes et de traiter les déclarations de l'administré. De ce fait, ces échanges ne posent pas de difficultés de principe au niveau de la protection des données à caractère personnel.

Ainsi, la CNIL n'a pas émis d'objection quant à la finalité d'un partage par défaut d'information et de données à caractère personnel entre entités publiques en cas de demande ou de déclaration de l'administré.

Pour éviter d'éventuels abus, le texte indique expressément que les échanges doivent être « nécessaires ». L'ajout de ce terme indique clairement que l'échange d'informations et de données à caractère personnel est une dérogation au principe général de non-recoupement des fichiers administratifs tenus par les entités publiques. A titre d'illustration, si une entité publique en charge d'un dossier a besoin de savoir si une personne est, ou non, imposable, elle ne devra solliciter que cette information, et non une copie de l'ensemble du bulletin d'imposition, qui comporte des informations sensibles telles que les revenus, la situation maritale, les déductions fiscales, etc.

En complément de ces cas de figure où les entités publiques seront au terme de l'article tenues, d'échanger entre elles toutes les informations et données à caractère personnel nécessaires pour traiter une demande ou une déclaration présentée par un administré en application d'une disposition législative ou d'un acte réglementaire, la disposition sous examen constitue également une réforme majeure de nature à simplifier les démarches administratives en ce qu'elle autorise les entités publiques à échanger entre elles les informations et données à caractère personnel nécessaires pour pouvoir informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévu par une disposition légale ou réglementaire. Par ailleurs, elle autorise les entités publiques à échanger des informations et des données à caractère personnel dans la mesure où cet échange est nécessaire pour attribuer éventuellement lesdites prestations ou avantages à l'administré.

Tout comme pour les échanges d'informations et de données nécessaires au traitement des demandes et déclarations présentées par les administrés, la CNIL n'a pas émis d'objection de principe à l'échange d'informations et de données à caractère personnel à des fins d'information de l'administré concernant ses droits ou aux fins de lui octroyer des prestations ou avantages. Ce système s'inscrit dans l'intérêt de tous les administrés, en ce qu'il vise à permettre aux entités publiques de les informer de manière proactive, sans qu'une intervention ou un accord ne soit requis pour initier l'échange de données et d'informations entre entités publiques.

Pour éviter d'éventuels abus, ces échanges sont entourés de garanties appropriées, que ce soit par le biais de la condition de la nécessité (« nécessaire ») ou par les conditions prévues à l'article 11 de la loi.

A l'instar de l'article 4 de la loi du 19 juin 2013 relative à l'identification des personnes physiques, le paragraphe 3 de l'article énonce les finalités du traitement de données à caractère personnel et de l'échange d'informations entre entités publiques. L'échange d'informations et de données à caractère

personnel est dès lors autorisé s'il vise à assurer la mise à disposition d'informations et de données à caractère personnel aux entités publiques pour l'exécution de leurs obligations et de leurs missions d'intérêt public. Il en va de même si l'échange vise à alléger la charge administrative des administrés dans le cadre de leur demande et déclaration ou s'il permet d'éviter aux entités publiques d'organiser elles-mêmes la collecte d'informations et de données à caractère personnel auprès des administrés pour autant que ces informations et données à caractère personnel soient déjà disponibles auprès d'une autre entité publique.

Cette précision des finalités du « *once only* » constitue une garantie supplémentaire pour les droits et libertés des personnes concernées non prévue par les dispositions françaises dont s'inspire le présent titre.

Ad article 10

Cet article prévoit l'obligation pour les administrés de certifier l'exactitude des informations et des données à caractère personnel que l'entité publique chargée de traiter la demande ou déclaration présentée par l'administré a obtenues auprès d'une entité publique. Il constitue le pendant logique de l'obligation prévue à l'article 5, paragraphe 1er, point d) du règlement (UE) 2016/679 qui prévoit expressément que les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour. En l'absence de cette certification, la demande ou déclaration sera incomplète.

Pour couvrir toutes les hypothèses, et à l'instar des dispositions prévues à l'article 21 de la loi du 19 juin 2013 relative à l'identification des personnes physiques, l'article sous examen prévoit expressément que l'exactitude des informations et des données à caractère personnel ne peut pas seulement être certifiée par l'administré, mais également par son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ainsi que par son mandataire spécial.

La mesure proposée constitue une mesure raisonnable et efficace visant à assurer que les informations et les données à caractère personnel qui sont inexactes, soient rectifiées sans tarder.

Par ailleurs, il revient à l'administré de demander la rectification de données à caractère personnel et des informations inexactes auprès de l'entité publique d'où celles-ci proviennent et de communiquer les informations et les données rectifiées à l'entité publique en charge du traitement de la demande ou de la déclaration.

Cette procédure est conforme aux dispositions du règlement (UE) 2016/679 en ce que la rectification de données à caractère personnel doit être sollicitée auprès du responsable du traitement initial qui détient les données et qui est censé les échanger avec l'entité publique qui traite les données à caractère personnel dans le cadre de la demande ou de la déclaration présentée par la personne concernée.

Ad article 11

Le présent article vise à fixer les conditions et modalités applicables à l'échange d'informations et de données à caractère personnel entre les entités publiques.

Le paragraphe 1er de l'article prévoit une interdiction pour les entités publiques de solliciter l'échange d'informations et de données à caractère personnel auprès d'une autre entité publique s'il est manifeste qu'elles ne sont compétentes, au regard de leurs missions légales et réglementaires, ni pour traiter la demande ou la déclaration présentée par l'administré, ni pour l'informer sur son droit au bénéfice éventuel d'une prestation ou d'un avantage voire pour les lui attribuer.

La disposition consacre le principe généralement accepté en matière de protection de données du « besoin d'en connaître » (« *need to know* »), d'après lequel les entités publiques doivent seulement avoir accès aux données à caractère personnel nécessaires pour la réalisation de leurs missions.

Le paragraphe 2 de l'article prévoit une autre garantie appropriée pour les droits et libertés de l'administré en imposant à l'entité publique chargée de traiter la demande ou la déclaration d'informer l'administré du fait que les informations et les données à caractère personnel qu'elle collecte auprès d'une autre entité publique sont nécessaires pour le traitement de la demande ou de la déclaration.

Dans ce contexte, et dans une optique de loyauté et de transparence envers l'administré découlant notamment des dispositions de l'article 5, paragraphe 1er, point a) du règlement (UE) 2016/679, l'entité publique doit faire parvenir à l'administré pour chaque catégorie d'informations et de données à caractère personnel les coordonnées des entités publiques d'où proviennent les informations et données en question.

La même obligation d'information de l'administré s'applique également dans le cas de figure où l'entité publique se procure des informations ou des données à caractère personnel auprès d'autres entités publiques pour informer l'administré sur ses droits ou au bénéfice éventuel d'une prestation ou d'un avantage prévu par des dispositions législatives ou règlementaires ou pour les lui attribuer.

L'information ainsi requise par le texte proposé est aussi une condition *sine qua non* pour l'exercice efficace du droit de rectification prévu à l'article 10, paragraphe 2 du projet de loi.

A l'instar du système avisé favorablement par la CNIL comme étant conforme au règlement (UE) 2016/679, le paragraphe 3 prévoit expressément que le dispositif d'échange d'informations et de données à caractère personnel ne saurait être utilisé pour des finalités incompatibles, en particulier pour la détection systématique des cas de fraudes notamment au moyen de croisements de données et d'informations.

Par ailleurs, en ce qui concerne le cas de figure où les informations et données à caractère personnel sont échangées pour informer les administrés sur leur droit ou bénéfice éventuel d'une prestation ou d'un avantage voire pour leur attribuer ces derniers, l'entité publique procédant auxdits échanges est tenue d'informer l'administré au plus tard au moment de la première communication individuelle sur le fait qu'il a le droit de s'opposer à la poursuite du traitement des données en question. Si l'administré choisit d'exercer son droit d'opposition inconditionnel, l'entité publique qui a obtenu les informations ou données à caractère personnel dans le cadre du « *once only* » est tenue de les détruire sans délai.

Le paragraphe 4 introduit une cause exonératoire de responsabilité dont les entités publiques peuvent se prévaloir lorsqu'il est impossible d'échanger les informations et les données à caractère personnel, notamment parce que les informations et données à caractère personnel ne sont pas disponibles dans un format structuré, couramment utilisé et lisible par machine. L'effet de cette cause exonératoire est double : d'une part, selon la lettre a), les entités publiques ne peuvent alors pas être tenues de procéder à l'échange d'informations et de données à caractère personnel, et d'autre part, selon la lettre b), une obligation est prévue pour les administrés de produire eux-mêmes les informations et les données.

En cas d'impossibilité de procéder à l'échange d'informations et de données à caractère personnel visé par l'article 9, paragraphe 2, les entités publiques sont tenues de dûment motiver en quoi exactement consiste l'impossibilité, en fournissant des explications quant aux circonstances exactes de l'impossibilité, et les mesures nécessaires aux entités publiques pour y remédier. Il revient alors aux entités publiques de remédier dans les meilleurs délais à cette impossibilité afin de rendre possible l'échange des informations et des données à caractère personnel.

Un exemple d'une impossibilité de procéder à l'échange visé serait l'inexistence dans un format électronique des informations et des données à caractère personnel ; notamment parce que celles-ci n'existent que sous format papier. Dans un tel cas, les informations et les données à caractère personnel doivent être digitalisées par les entités publiques afin de permettre sans délai l'échange des informations et données à caractère personnel.

Suivant l'article 12, paragraphe 2, une copie de la motivation de l'impossibilité de procéder à l'échange est transmise au ministre ayant la digitalisation dans ses attributions. Cette information peut également être accédée par les administrés par le biais, notamment, d'une demande d'accès formulée conformément aux dispositions de la loi du 14 septembre 2018 relative à une administration transparente et ouverte. Le Ministère de la Digitalisation, dans sa poursuite continue de la réussite du gouvernement numérique, reste à disposition des entités publiques étant confrontées à une impossibilité de procéder à l'échange nécessaire d'informations et de données à caractère personnel, afin de leur fournir assistance et conseil pour parvenir sans délai audit échange.

En outre, pour que le « *once only* » constitue une mesure efficace de simplification administrative et de modernisation de l'action publique, les entités publiques destinataires des informations et des données à caractère personnel ne peuvent se voir opposer le secret professionnel si elles agissent dans le cadre de leurs missions légales et qu'elles sont habilitées à avoir connaissance des informations ou données en question.

Ad article 12

L'article impose aux entités publiques d'identifier dans les meilleurs délais les informations et les données à caractère personnel qu'elles peuvent obtenir auprès d'une autre entité publique, et ce tant pour le traitement des demandes et déclarations présentées par les administrés que pour l'information

de ces derniers sur leur droit au bénéfice d'une éventuelle prestation ou d'un avantage ou pour pouvoir les leur attribuer.

Sur base de cette analyse, les entités publiques sont tenues de notifier sans délai les échanges d'informations et des données à caractère personnel identifiés aux entités publiques à la source des informations et données. Ces dernières sont tenues en retour de, soit certifier la disponibilité des informations et des données sollicitées (même si cet échange s'avèrera techniquement impossible par la suite au sens de l'article 11, paragraphe 4 de la loi), soit informer les entités publiques demanderesses du fait que les informations et données sollicitées ne sont pas disponibles.

Une copie de l'information relative à la disponibilité des informations et données est transmise au ministre ayant la digitalisation dans ses attributions afin de permettre à ce dernier de cartographier les flux des échanges « *once only* », notamment pour l'identification d'éventuelles sources authentiques.

Ad article 13

Cet article prévoit l'obligation pour les entités publiques concernées de formaliser chaque type d'échange d'informations et de données à caractère personnel visé par l'obligation « *once only* » par le biais d'un protocole contenant tous les éléments obligatoires cités par la disposition sous examen.

Dans un objectif d'« *accountability* », prévu à l'article 5, paragraphe 2 du règlement (UE) 2016/679, et de transparence administrative, les entités publiques sont tenues d'amender le protocole en cas de changement des éléments liés à l'obtention des informations et des données à caractère personnel.

Le protocole ainsi que tout avenant à ce dernier doivent être transmis sans délai à l'Autorité des données pour publication par voie électronique.

Le système du protocole et de sa publication par l'Autorité des données repose sur les dispositions du droit français et des observations formulées par la CNIL en France. Cette dernière a souligné que la diffusion publique de ces informations est un élément important qui contribue à l'équilibre du dispositif « *once only* », puisqu'il permettra aux administrés d'avoir une vision exhaustive des échanges mis en place.

La mise en place d'une infrastructure standardisée de publication des protocoles et d'un pilotage centralisé au niveau de l'Autorité des données permettent en effet de garantir de manière efficace la transparence administrative dans le cadre de la mise en œuvre du principe « *once only* ». Ainsi, les administrés peuvent consulter toutes les informations sur les échanges d'informations et de données à caractère personnel effectués par les entités publiques auprès d'une seule source centralisée.

Pour que cet outil de transparence puisse fonctionner de manière efficace, l'Autorité des données doit être tenue informée de toute modification dans l'application des protocoles en vigueur.

En cas de modification, l'Autorité des données maintient la publication du protocole obsolète durant une période supplémentaire de deux années tout en indiquant dans ladite publication que le protocole n'est plus applicable. Le système sous examen s'inspire du Journal officiel du Grand-Duché de Luxembourg (au Mémorial A, toute loi abrogée reste affichée sur le site internet www.legilux.lu) ou du Registre de commerce et des sociétés (les informations sur une société continuent d'être publiées sur le site internet www.lbr.lu ensemble avec l'indication que la société en question a été radiée).

Ad article 14

Cet article prévoit l'obligation pour l'Autorité des données de tenir un registre de tous les protocoles qui lui ont été transmis par les entités publiques pour publication conformément à l'article 13 de la loi.

En vue d'identifier les sources authentiques d'informations et de données, le ministre ayant la digitalisation dans ses attributions dispose d'un accès direct au dit registre tenu par l'Autorité des données.

Titre V – Traitement ultérieur de données à caractère personnel par les entités publiques

Section I – Dispositions générales

Ad article 15

Cet article crée le fondement juridique, en droit interne, pour les entités publiques, d'un traitement ultérieur de données à caractère personnel pour des finalités autres que celles pour lesquelles les

données ont été initialement collectées, et ce indépendamment de leur compatibilité et de leur base de licéité initiale. A cette fin, l'article énonce limitativement les finalités pour lesquelles le traitement ultérieur de données à caractère personnel par des entités publiques est autorisé.

A noter que le système proposé s'applique sans préjudice de la possibilité pour les entités publiques d'effectuer des traitements ultérieurs de données à caractère personnel sur base de leur compatibilité (articles 5, paragraphe 1er, point b) et 6, paragraphe 4 du règlement (UE) 2016/679) ou de procéder à des traitements ultérieurs de données à caractère personnel sur base d'une disposition spécifique du droit de l'Union ou du droit national applicable, telles que l'article 4, paragraphe 4 de la loi du 3 décembre 2014 ayant pour objet l'organisation des centres de recherche publics ou l'article 423, point 4° du Code de la sécurité sociale.

Au sens du présent titre, le traitement ultérieur de données à caractère personnel par des entités publiques est autorisé s'il est réalisé pour l'une ou plusieurs des finalités énoncées à l'article 15, sous réserve que les conditions énoncées au titre V de la loi soient remplies. Ainsi, l'entité publique est autorisée à effectuer un traitement ultérieur de données à caractère personnel pour des finalités déterminées par le texte, sans devoir réaliser le test de compatibilité des finalités conformément aux critères énoncés à l'article 6, paragraphe 4 du règlement (UE) 2016/679. Ceci couvre tant la mise à disposition des données à caractère personnel et leur partage, que le traitement ultérieur mis en œuvre par les entités publiques.

Le système proposé met dès lors en œuvre la faculté prévue par l'article 6, paragraphe (4) du règlement (UE) 2016/679 de permettre au législateur national de définir les finalités pour lesquelles des traitements de données à caractère sont autorisés, indépendamment de leur compatibilité ou non avec les finalités pour lesquelles les données ont été initialement collectées, sous réserve que cette mesure soit nécessaire et proportionnée dans une société démocratique pour garantir un des objectifs visés à l'article 23, paragraphe 1er du règlement (UE) 2016/679.

Parmi les objectifs visés à l'article 23, paragraphe 1er du règlement (UE) 2016/679 se trouvent les « autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaires, budgétaires et fiscales, de la santé publique et de la sécurité sociale ».

C'est également sur base de cette énumération non limitative des objectifs importants d'intérêt public que le législateur allemand a décidé d'introduire, en droit interne, une liste de finalités pour lesquelles les entités publiques allemandes sont d'office autorisées à procéder à des traitements ultérieurs de données à caractère personnel, dans l'exécution de leurs missions :

« *1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn*

1. *offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,*
2. *Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,*
3. *sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,*
4. *sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,*
5. *sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist, oder*
6. *sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen. […]*»[8].

8 Bundesdatenschutzgesetz (BDSG), § 23 Verarbeitung zu anderen Zwecken durch öffentliche Stellen.

Le législateur finlandais a, lui-aussi, introduit en droit interne, par le biais du « *Act on the Secondary Use of Health and Social Data* », une liste de finalités pour lesquelles un traitement ultérieur de données à caractère personnel est autorisé, indépendamment de la question de savoir si les finalités sont compatibles ou non. Il s'agit des finalités suivantes :

« 1) statistics ;

2) scientific research ;

3) development and innovation activities ;

4) education ;

5) knowledge management ;

6) steering and supervision of social and health care by authorities ; and

7) planning and reporting duty of an authority. »[9]

Notons également que le Comité européen pour la protection des données a explicitement confirmé, dans son avis 08/2017, que l'allégement de la charge administrative sur les personnes physiques ou les organisations, l'efficacité accrue des procédures administratives et l'économie de temps et de ressources, constituent sans nul doute des objectifs d'intérêt public valables.

En conséquence, l'article constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des objectifs visés à l'article 23, paragraphe 1er du règlement (UE) 2016/679.

A l'instar des dispositions du « *Bundesdatenschutzgesetz* »[10] ainsi que, notamment, de l'article 3 paragraphe 6bis de la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme[11], le paragraphe 2 prévoit, dans une optique de sécurité juridique, le fondement de licéité aux termes du règlement (UE) 2016/679 pour le traitement ultérieur, y compris le partage et la mise à disposition de données à caractère personnel, par les entités publiques conformément au titre V de la loi.

A noter que le considérant (159) du règlement (UE) 2016/679 précise expressément que le « *traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété* ***au sens large*** *et* ***couvrir, par exemple****, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé. Il devrait, en outre, tenir compte de l'objectif de l'Union mentionné à l'article 179, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, consistant à réaliser un espace européen de la recherche. Par « fins de recherche scientifique », il convient également d'entendre les études menées dans l'intérêt public dans le domaine de la santé publique* » (mise en évidence ajoutée).

De ce fait, le traitement de données à caractère personnel effectué par les entités publiques pour les finalités énoncées à l'article 15 est licite en application de l'article 9, paragraphe 2, point j), sinon le point g) du règlement (UE) 2016/679, en particulier compte tenu du fait que la loi prévoit expressément des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Ad article 16

Cet article reprend le principe général de la minimisation des données prévue à l'article 5, paragraphe 1er, point c) du règlement (UE) 2016/679 tel que spécifié par les dispositions de l'article 89, paragraphe 1er du même règlement.

La rédaction des paragraphes 1er à 3 de l'article 16 est inspirée des articles 186 et suivants de la loi belge du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Il prévoit explicitement que les entités publiques doivent à chaque fois procéder à un traitement ultérieur qui ne permet pas l'identification des personnes concernées si cela s'avère possible. Seulement lorsque le traitement des données anonymisées ne permet pas d'atteindre la finalité poursuivie, les entités publiques sont autorisées à traiter ultérieurement des données sous format pseudonymisé. Dans

---

9 Act on the Secondary Use of Health and Social Data, Section 2.

10 Bundesdatenschutzgesetz (BDSG), § 23 Verarbeitung zu anderen Zwecken durch öffentliche Stellen.

11 « *Le traitement de données à caractère personnel sur base de la présente loi aux fins de la prévention du blanchiment et du financement du terrorisme est considéré comme une question d'intérêt public au titre du règlement (UE) 2016/679* ».

ce même ordre d'idées, un traitement des données en clair est seulement permis dans les limites du strict nécessaire, à savoir à condition que les entités publiques, en leur qualité de responsables du traitement, prouvent que les finalités du traitement n'ont pas pu être atteintes en traitant des données anonymisées ou des données à caractère personnel pseudonymisées.

Pour réduire au minimum le risque de réidentification des personnes concernées, l'article prévoit, à l'instar des dispositions du règlement relatif à l'espace européen des données de santé, une obligation pour les entités publiques qui détiennent les données à caractère personnel d'identifier les informations protégées pour des motifs de protection des données à caractère personnel.

Le paragraphe 5 traite plus spécifiquement des risques de réidentification. L'état de la technique et les procédés d'anonymisation sont évolutifs, tout comme les données disponibles (publiquement ou pas) qui rendraient les personnes concernées identifiables (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 règlement) variera avec le temps.

La disposition en question instaure une obligation de confidentialité pour les entités publiques qui procèdent au traitement ultérieur de données à caractère personnel. De ce fait, elle interdit la divulgation de toute information qui pourrait compromettre les droits et intérêts des individus, que les entités publiques auraient pu acquérir dans le cadre du traitement ultérieur de données à caractère personnel, et ce malgré les garanties mises en place conformément à la loi. Dans ce contexte, le texte interdit également aux entités publiques d'effectuer un traitement ultérieur de données à caractère personnel visant à rétablir l'identité des personnes concernées.

En tout état de cause, les entités publiques sont tenues, en outre, de mettre en place des mesures techniques et opérationnelles pour empêcher toute réidentification.

Section II – Traitement ultérieur de données à caractère personnel par la même entité publique

Ad article 17

Une entité publique est autorisée à traiter ultérieurement les données à caractère personnel qu'elle détient, qu'elles proviennent directement de la personne concernée ou d'autres sources. Ceci couvre aussi les cas de figure où les entités publiques, comme notamment l'Observatoire national de la santé, l'Inspection générale de la sécurité sociale, ou encore le Service de Coordination de la Recherche et de l'Innovation pédagogiques et technologiques, traitent ultérieurement des données qu'elles ont initialement collectées auprès d'autres entités publiques dans le cadre de leurs missions.

Le traitement ultérieur par une même entité est seulement autorisé pour les finalités limitativement énoncées à l'article 15 et ceci sous réserve des conditions d'anonymisation et de pseudonymisation prévues à l'article 16 de la loi.

Comme énoncé plus haut dans le commentaire des articles, le fait que la loi énonce limitativement des finalités pour lesquelles le traitement ultérieur de données à caractère personnel est d'office autorisé n'exclut nullement que les entités publiques traitent ultérieurement des données à caractère personnel si les finalités ultérieures sont compatibles conformément aux articles 5, paragraphe 1er, point b) et 6, paragraphe 4 du règlement (UE) 2016/679.

En dérogation au système général instauré par le paragraphe 1er, des conditions plus strictes sont prévues pour le traitement ultérieur des catégories particulières de données à caractère personnel visées aux articles 9 et 10 du règlement (UE) 2016/679. Ces catégories des données peuvent seulement être traitées ultérieurement par la même entité si elles ont préalablement été anonymisées ou pseudonymisées. Pour ce faire, l'entité publique peut (mais ne doit pas) recourir au service du Centre. En revanche, le traitement desdites catégories de données à caractère personnel en clair est formellement interdit par la loi.

Section III – Traitement ultérieur de données à caractère personnel par une autre entité publique ou par plusieurs entités publiques

Ad article 18

Cet article prévoit des conditions strictes pour le traitement ultérieur de données à caractère personnel détenues par une entité publique, indépendamment de leur source initiale, par une autre entité publique ou par plusieurs entités publiques.

Les traitements ultérieurs de données à caractère personnel ainsi visés peuvent seulement être mis en œuvre pour les finalités énoncées à l'article 15, sous réserve de respecter les conditions cumulatives limitativement énumérées au paragraphe 1er.

Ainsi, il est requis que l'entité publique détenant les données à caractère personnel donne son accord au traitement ultérieur des données à caractère personnel. Dans ce contexte, il échet de noter que seul l'accord de l'entité publique qui détient les données à caractère personnel est requis, sans que cette dernière soit obligée de solliciter l'accord des entités publiques auprès desquelles les données ont initialement été collectées.

L'entité publique peut marquer son accord de principe au traitement ultérieur, y compris le partage et la mise à disposition des données, en signalant que les données sont disponibles à des fins de traitement ultérieur par le biais de leur inscription sur la liste des ressources consultable tenue par le point d'information unique. Dans l'hypothèse où les données ne figurent pas sur cette liste, les entités publiques ont la possibilité de marquer leur accord spécifique au traitement ultérieur de données à caractère personnel en contresignant la demande que l'entité publique effectuant le traitement ultérieur prévoit d'introduire auprès de l'Autorité des données.

Cela étant dit, l'article sous examen ne crée pas d'obligation pour les entités publiques de partager des données à caractère personnel avec d'autres entités publiques en vue d'un traitement ultérieur conformément aux dispositions du titre V.

En pratique, l'entité publique souhaitant traiter ultérieurement les données à caractère personnel se concertera avec les entités publiques détenant les données en amont de l'introduction auprès de l'Autorité des données de la demande de traitement ultérieur conformément au titre VII de la loi.

Pour ce faire, les entités publiques souhaitant traiter ultérieurement les données à caractère personnel ont la faculté de recourir aux services proposés par le LNDS, qui dans ce cas de figure est obligé de les assister, que ce soit au niveau de la préparation de la demande et des pièces à joindre à celle-ci, ou au niveau de la préparation des démarches auprès des organismes du secteur public en vue d'obtenir leur accord à l'accès et la réutilisation des données que ces derniers détiennent. Rien n'empêche cependant que l'entité publique souhaitant traiter ultérieurement les données à caractère personnel recoure aux services offerts par d'autres acteurs, tels que le Centre qui peut dispenser des conseils dans le cadre des missions qui lui sont assignées par la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État, pour préparer la demande d'accès et de réutilisation. Cela étant dit, le texte n'impose pas d'obligation au Centre de fournir cette assistance.

Dans une optique de mise en balance des intérêts poursuivis par les entités publiques et ceux de la personne concernée, l'article prévoit que le traitement ultérieur ne doit pas porter une atteinte disproportionnée aux droits et libertés des individus au regard des finalités poursuivies. L'analyse de proportionnalité doit être documentée dans le cadre de la demande et des pièces justificatives qui doivent y être jointes. Le libellé de cette condition s'inspire étroitement des dispositions de l'article 17, paragraphe 4 de la loi du 17 août 2018 relative à l'archivage.

La troisième condition énoncée par l'article sous examen s'inscrit dans l'esprit de la mise en œuvre des garanties appropriées généralement acceptées en matière de protection des données. Elle s'inspire notamment des dispositions des articles 5, paragraphe 1er, point c), 24, 25 et 89 du règlement (UE) 2016/679.

Ainsi, les données à caractère personnel peuvent être traitées ultérieurement, soit sous réserve d'être préalablement anonymisées, soit lorsque le traitement de données anonymisées ne permet pas d'atteindre la finalité poursuivie, pour autant qu'elles aient été pseudonymisées, et à condition que l'Autorité des données délivre une autorisation préalable et que le traitement ultérieur soit effectué dans l'environnement de traitement sécurisé prévu à l'article 36.

Le paragraphe 2 ouvre la possibilité aux entités publiques demanderesses qui se voient refuser le partage de données à caractère personnel par une autre entité publique de saisir le Conseil consultatif pour avis. La procédure prévue à l'article sous examen est identique à celle prévue par les dispositions de l'article 17 de la loi du 17 août 2018 relative à l'archivage.

L'avis du Conseil consultatif ne lie pas l'entité publique détenant les données à caractère personnel. Cette dernière restera libre dans sa prise de décision. Elle est seulement appelée à reconsidérer sa position et à émettre sa décision finale par écrit dans un délai de trois semaines. L'absence de décision finale dans le délai imparti vaut refus définitif de partage de la part de l'entité publique en question.

En cas d'accord au traitement ultérieur de données à caractère personnel, l'entité publique détentrice des données est tenue de contresigner la demande conformément aux dispositions de la loi.

TITRE VI – Accès et réutilisation des données détenues par des organismes du secteur public par des réutilisateurs de données

Section I – Dispositions générales

Observations générales :

Le titre VI concerne spécifiquement la mise en œuvre, en droit national, du chapitre II du règlement (UE) 2022/868 concernant la réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public.

L'objectif du règlement (UE) 2022/868 est d'accroître la confiance dans le partage des données en établissant des mécanismes appropriés de garanties pour les personnes et les organismes du secteur public détenant les données et ce, en levant les obstacles notamment techniques à la réutilisation des données (voir considérant (5) du règlement (UE) 2022/868).

Le titre VI se distingue des traitements couverts par le titre V en ce qu'il traite de la réutilisation des données au sens du règlement (UE) 2022/868, la réutilisation étant définie par ledit règlement européen comme étant une utilisation de données par des personnes physiques ou morales, à l'exception de l'échange de données entre des organismes du secteur public aux seules fins de l'exercice de leurs missions de service public.

Le titre VI prévoit les catégories de données concernées disponibles à l'accès et à la réutilisation (articles 19 et 21) ainsi qu'un régime d'autorisation et de réutilisation de ces données (article 20 et articles 22 à 24).

Ad article 19

Conformément aux dispositions du règlement (UE) 2022/868, l'article précise les catégories de données susceptibles d'être accédées et réutilisées aux termes du titre VI de la loi.

Le paragraphe 2 énonce expressément que les entités publiques ne sont pas en droit d'invoquer les dispositions du titre VI pour solliciter l'accès et la réutilisation des données. En revanche, les entités publiques, en tant qu'organismes du secteur public, sont visées par les dispositions du titre VI pour ce qui concerne la mise à disposition des données aux réutilisateurs de données.

Ad article 20

Conformément aux dispositions du règlement (UE) 2022/868, l'article liste limitativement les finalités pour lesquelles l'accès et la réutilisation aux données visés au titre VI de la loi sont autorisés, sous réserve des conditions applicables.

A la lumière des dispositions du règlement (UE) 2022/868, la réutilisation des données sous le régime dudit règlement inclut l'utilisation de données détenues par des organismes du secteur public, et ce tant à des fins commerciales, qu'à des fins non commerciales autres que l'objectif initial de la mission de service public pour lequel les données ont été produites.

Ad article 21

Cet article précise la forme que les données prévues à l'article 19, paragraphe 1er doivent avoir lorsqu'elles sont rendues accessibles à des fins de réutilisation au sens du titre VI.

Lorsqu'il s'agit de données à caractère personnel, l'accès et la réutilisation ne peuvent concerner que des données à caractère personnel préalablement anonymisées. Par dérogation à ce principe général, il peut être fait usage de données à caractère personnel préalablement pseudonymisées, à condition de démontrer que la réutilisation de données anonymisées ne permet pas d'atteindre les finalités poursuivies.

A l'instar des dispositions du règlement européen relatif à l'espace européen des données de santé, l'article impose aux organismes du secteur public qui détiennent les données à caractère personnel et les données à caractère non personnel d'identifier les données protégées pour les motifs visés à l'article 19 de la loi.

Par ailleurs, conformément aux exigences de la réglementation européenne, en particulier les dispositions du règlement (UE) 2022/868, le texte prévoit une obligation de confidentialité à laquelle le réutilisateur des données est tenu lorsqu'il prend connaissance, malgré les garanties mises en place, d'informations compromettant les droits et libertés de tiers.

Dans ce même ordre d'idées, la disposition interdit au réutilisateur de données de rétablir l'identité de toute personne concernée à laquelle se rapportent les données. Il est également tenu de mettre en place des mesures techniques et opérationnelles appropriées. Celles-ci doivent être actualisées en tenant compte de l'état de la technique.

Le système proposé s'applique sans préjudice des obligations prévues aux articles 33 et 34 du règlement (UE) 2016/679 auxquelles les réutilisateurs de données sont tenus en leur qualité de responsable du traitement. Il en va de même des obligations incombant aux réutilisateurs de données conformément à l'article 5, paragraphe 5 du règlement (UE) 2022/868.

Section II – Conditions applicables à la réutilisation de données à caractère personnel

Ad article 22

Cet article prévoit les conditions cumulatives dans lesquelles les accès et la réutilisation de données à caractère personnel par les réutilisateurs de données sont autorisés conformément aux dispositions du titre VI de la loi.

Ainsi, il faut que le réutilisateur de données veille à ce que l'accès et la réutilisation s'inscrivent exclusivement dans une ou plusieurs des finalités limitativement énoncées par la loi. En signant la demande et en soumettant cette dernière conformément aux dispositions des titres VI et VII, il s'engage à les respecter.

Encore est-il requis que l'accès et la réutilisation des données ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée. L'analyse de proportionnalité doit être documentée dans le cadre de la demande et des pièces justificatives qui doivent y être jointes. Le libellé de cette condition, visant à encadrer la réutilisation des données de manière non discriminatoire, transparente, proportionnée et objectivement justifiée conformément au règlement (UE) 2022/868, s'inspire étroitement des dispositions de l'article 17, paragraphe 4 de la loi du 17 août 2018 relative à l'archivage.

De plus, l'accès et la réutilisation des données à caractère personnel présupposent qu'un accord a été trouvé entre les réutilisateurs de données et tous les organismes du secteur public détenant les données et que ces derniers marquent leur accord à l'accès aux fins de la réutilisation des données. Dans ce contexte, il échet de noter que seul l'accord de l'organisme du secteur public qui détient les données est requis. En d'autres termes, il n'est pas nécessaire de solliciter l'accord de tous les autres acteurs auprès desquelles l'organisme du secteur public a initialement collecté les données.

L'accord par les organismes du secteur public qui détiennent les données peut être exprimé par ces derniers en inscrivant les données disponibles sur la liste des ressources consultable, qui est tenue par le point d'information unique conformément à l'article 8, paragraphe 2 du règlement (UE) 2022/868.

Dans l'hypothèse où les données ne figurent pas sur cette liste, les organismes du secteur public qui détiennent les données à caractère personnel ont la possibilité de marquer leur accord spécifique à la mise à disposition des données à caractère personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en contresignant la demande que le réutilisateur des données prévoit d'introduire auprès de l'Autorité des données. Le réutilisateur de données sera dès lors tenu de procéder à une concertation avec tous les organismes du secteur public détenant les données en amont de l'introduction auprès de l'Autorité des données de la demande d'accès et de réutilisation des données conformément au titre VII de la loi.

Pour ce faire, les réutilisateurs de données ont la faculté de recourir aux services proposés par le LNDS, qui dans ce cas de figure est obligé d'assister le réutilisateur, que ce soit au niveau de la préparation de la demande et des pièces à joindre à celle-ci, ou au niveau de la préparation des démarches auprès des organismes du secteur public en vue d'obtenir leur accord à l'accès et à la réutilisation des données que ces derniers détiennent. Rien n'empêche que le réutilisateur recoure aux services offerts par d'autres acteurs, tel que le Centre, pour préparer la demande d'accès et de réutilisation. Cela étant dit, le texte n'impose pas d'obligation au Centre de fournir cette assistance.

Dans ce cas de figure, l'accord des organismes du secteur public détenant les données se manifeste par leur contresignature de la demande à introduire auprès de l'Autorité des données. En l'absence de la contresignature de la demande par toutes les parties en question, la demande d'accès et de réutilisation de données à caractère personnel est déclarée irrecevable par l'Autorité des données conformément aux dispositions de l'article 29, paragraphe 4.

Cela étant, le réutilisateur de données, confronté à un refus d'un ou de plusieurs organismes du secteur public détenant les données (notamment au motif d'une atteinte disproportionnée aux droits et libertés de la personne concernée ou parce que la demande ne s'inscrit pas dans une des finalités prévues par la loi), a la faculté de saisir le Conseil consultatif pour avis. Comme évoqué plus haut (commentaire ad article 18), la procédure prévue à l'article sous examen est identique à celle prévue par les dispositions de l'article 17 de la loi du 17 août 2018 relative à l'archivage.

Ainsi, l'avis du Conseil consultatif n'est pas contraignant, mais invite les organismes du secteur public détenant les données à revoir leur position et, le cas échéant, à rendre une décision finale favorable à la réutilisation.

Le Conseil consultatif dispose d'un délai de trois semaines pour rendre son avis. Une fois l'avis rendu, l'organisme du secteur public détenant les données sollicitées dispose de trois semaines pour prendre une décision finale. Cette décision d'autorisation ou de refus doit être actée par écrit. A noter que le défaut de réponse formelle par l'organisme du secteur public détenant les données équivaudra à un refus.

En cas d'accord, l'organisme du secteur public détenant les données à caractère personnel contresigne la demande d'accès et de réutilisation visée à l'article 28, sous peine d'irrecevabilité.

En complément des conditions énoncées ci-avant, l'article sous examen soumet l'accès et la réutilisation des données à caractère personnel à la condition que les données soient anonymisées ou pseudonymisées préalablement à leur accès et à leur réutilisation. A noter également que les dispositions de l'article 35 relatives aux mesures appropriées trouvent application.

Enfin, et sous réserve du respect des conditions susvisées, l'article conditionne l'accès et la réutilisation des données à caractère personnel au fait que l'accès et la réutilisation des données se fassent dans l'environnement de traitement sécurisé visé à l'article 36.

A l'instar des dispositions du « *Bundesdatenschutzgesetz* »[12] ainsi que, notamment, de l'article 3(6bis) de la loi relative à la lutte contre le blanchiment et contre le financement du terrorisme[13], le paragraphe 2 prévoit, dans une optique de sécurité juridique, le fondement de licéité aux termes du règlement (UE) 2016/679 pour le traitement ultérieur, y compris le partage et la mise à disposition de données à caractère personnel, par les organismes du secteur public conformément au titre VI. Dans ce cadre, il est renvoyé aux explications reprises sous le commentaire de l'article 15 *supra*.

Le considérant (159) du règlement (UE) 2016/679 précise expressément que le « *traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété* ***au sens large*** *et* ***couvrir, par exemple****, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé. Il devrait, en outre, tenir compte de l'objectif de l'Union mentionné à l'article 179, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, consistant à réaliser un espace européen de la recherche. Par « fins de recherche scientifique », il convient également d'entendre les études menées dans l'intérêt public dans le domaine de la santé publique* » (mise en évidence ajoutée).

De ce fait, le traitement de données à caractère personnel effectué par les réutilisateurs de données conformément au titre VI pour les finalités énoncées à l'article 20 devrait être licite en application de l'article 9, paragraphe 2, points g) ou j) du règlement (UE) 2016/679, en particulier compte tenu du fait que la loi prévoit expressément des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

---

12 Bundesdatenschutzgesetz (BDSG), § 23 Verarbeitung zu anderen Zwecken durch öffentliche Stellen.

13 « *Le traitement de données à caractère personnel sur base de la présente loi aux fins de la prévention du blanchiment et du financement du terrorisme est considéré comme une question d'intérêt public au titre du règlement (UE) 2016/679* ».

Section III – Conditions applicables à la réutilisation de données à caractère non personnel

Ad article 23

L'article 23 de la loi sous examen constitue le pendant de l'article 22. La différence avec l'article 22 réside dans son champ d'application qui est celui de l'accès et de la réutilisation des données à caractère non personnel détenues par les organismes du secteur public.

Ainsi, les conditions sont fort semblables à celles de l'article 22, tout en étant adaptées aux spécificités liées à la nature des informations et des données à caractère non personnel.

Il n'appelle pas d'observations particulières autres que celles formulées dans le cadre de l'article 22 *supra*.

Section IV – Conditions applicables à la réutilisation d'ensembles contenant des données à caractère personnel et des données à caractère non personnel

Ad article 24

L'article 24 vise les cas de figure où un accès et une réutilisation portent sur un ensemble de données inextricablement liées comprenant à la fois des données à caractère personnel ainsi que des données à caractère non personnel. Tel est notamment le cas lorsqu'un accès et une réutilisation portent sur des informations protégées pour un ou plusieurs motifs visés à l'article 19, paragraphe 1er, points 1° à 3°, combinées avec les coordonnées des personnes concernées (constituant des données à caractère personnel au sens du règlement (UE) 2016/679) auxquelles se rapportent les informations en question.

Dans ces cas de figure, les conditions applicables aux données à caractère personnel et celles applicables aux données à caractère non personnel s'appliquent cumulativement.

Titre VII – Modalités applicables au traitement ultérieur de données à caractère personnel par les entités publiques et à l'accès et la réutilisation des données par des réutilisateurs de données

Section I – Dispositions générales

Ad article 25

Cet article précise que les dispositions du titre VII couvrent tant les cas de figure visés au titre V (traitement ultérieur de données à caractère personnel par les entités publiques) que ceux du titre VI du projet de loi sous examen (accès et réutilisation de données détenues par des organismes du secteur public), qui sont soumis à autorisation de l'Autorité des données. De ce fait, l'article rend inapplicables les dispositions du titre VII, y compris de l'obligation de la mise en place d'un plan de confidentialité et d'un recours à l'environnement de traitement sécurisé, au traitement ultérieur de données à caractère personnel par la même entité publique conformément à l'article 17 de la loi.

Le présent titre, qui s'inscrit dans l'esprit de la mise en œuvre des garanties appropriées généralement acceptées en matière de protection des données, est soumise à une analyse d'impact relative à la protection des données générale dans le cadre de l'adoption de la loi conformément à l'article 35, paragraphe (10) du règlement (UE) 2016/679.

L'analyse d'impact révèle que les nombreuses mesures prévues par la loi constituent des garanties transversales fortes permettant d'éviter d'atteintes disproportionnées aux droits et libertés des personnes concernées par rapport aux finalités de traitement ultérieur et de réutilisation autorisées par la loi. Les principales mesures et garanties peuvent être résumées comme suit :

GARANTIES *MESURES*	Transparence	Responsabilisation	Sécurité juridique	Minimisation	*Privacy by design*	*Privacy by default*	Proportionnalité	Nécessité	Accès restreint	Non-réidentification	Qualité des données
Détermination par le législateur des responsables du traitement et des sous-traitants.	x	x	x								
Détermination limitative par la loi des finalités autorisées.	x		x				x				
Détermination par la loi des bases de licéité.	x		x				x				
Accord préalable de l'entité publique détentrice.				x		x	x	x	x	x	x
Autorisation préalable de l'Autorité de données en cas de données non-anonymes sur base d'une analyse extensive concrète des conditions du traitement ultérieur et de la réutilisation.	x			x	x	x	x	x		x	x
Exigence d'une documentation détaillée relative au traitement ultérieur à charge des entités publiques utilisatrices/relative au réutilisation des données à charge des réutilisateurs.	x	x			x	x	x	x			
Anonymisation / pseudonymisation préalable aux actes de traitement effectués dans le cadre du traitement ultérieur et de la réutilsation, ainsi que d'agrégation en cas de réutilisation.				x	x	x	x	x	x	x	
Actes de pseudonymisation sous la responsabilité de l'Autorité des données, du Centre et, le cas échéant, du tiers de confiance.				x	x	x		x	x	x	x
Exigence d'un plan de confidentialité à mettre en place par les entités publiques utilisatrices et les réutilisateurs décrivant le processus d'anonymisation ou de pseudonymisation et d'agéragation des données.	x	x		x	x	x				x	x
Validation du plan de confidentialité par le Centre ou un tiers de confiance mandaté par le Centre.				x	x	x			x	x	x
Réalisation du traitement ultérieur (sur des données non anonymes) et de la réutilisation dans un environnement de traitement sécurisé.					x	x			x	x	x
Définition d'exigences légales strictes concernant le fonctionnement de l'environnement sécurisé.	x				x				x	x	x
Indépendance des acteurs et de leur personnel.					x	x			x	x	
Obligation de confidentialité et au secret professionnel (art. 458 du code pénal) des acteurs désignés pour intervenir dans le cadre de la mise en place du processus d'anonymisation ou de pseudonymisation des données à caractère personnel.		x							x	x	

GARANTIES / *MESURES*	Transparence	Responsabilisation	Sécurité juridique	Minimisation	*Privacy by design*	*Privacy by default*	Proportionnalité	Nécessité	Accès restreint	Non-réidentification	Qualité des données
Obligation à charge de l'Autorité des données, du Centre et du tiers de confiance de désigner le personnel en charge des missions prévues le texte.	x	x							x	x	
Interdiction de réidentification des personnes concernées.										x	

La mise en œuvre des mesures et garantie prévues par la loi est dès lors de nature à limiter de manière satisfaisante le risque de perte de confidentialité (i.e. accès illégitime aux données), d'intégrité (i.e. modification non désirée des données) et de perte de disponibilité (i.e. vol et destruction de données).

Ainsi, les entités publiques effectuant un traitement ultérieur de données à caractère personnel au sens du titre V ainsi que les réutilisateurs de données visés au titre VI, soumis aux formalités du titre VII, peuvent se limiter lors de la réalisation de leur propre analyse d'impact aux seuls éléments spécifiques du traitement ultérieur ou de la réutilisation qu'ils envisagent, à savoir en particulier aux éléments visés respectivement aux articles 27 et 28.

Section II – Demande de traitement ultérieur ou d'accès et de réutilisation des données

Ad article 26

L'article sous examen pose l'exigence que les demandes à adresser à l'Autorité des données revêtent une forme écrite. La formulation prévue est techniquement neutre. Ainsi, les demandes sont présentées exclusivement sous format électronique et peuvent être signées électroniquement.

Les demandes doivent être formulées avec un degré de précision suffisant pour que l'Autorité des données soit en mesure de prendre une décision éclairée et ce en connaissance de tous les éléments entourant le traitement ultérieur ou l'accès et la réutilisation des données.

Aux termes du paragraphe 2, toute modification substantielle de la demande ou de ses annexes nécessite le dépôt d'une nouvelle demande dans les formes et conditions prévues à l'article 29 du projet de loi. Tel est notamment le cas si le réutilisateur de données sollicite :

– un élargissement du contexte du traitement de données envisagé, que ce soit au niveau des organismes du secteur public détenant les données, qu'au niveau des destinataires des données ;
– une modification des conditions d'anonymisation, de pseudonymisation, d'agrégation ou de toute autre méthode de contrôle de la divulgation des données visées à l'article 21 ;
– une modification des catégories de données, notamment compte tenu d'une introduction souhaitée de données dans l'environnement de traitement sécurisé, ou de personnes concernées ;
– une modification des finalités de l'accès et de la réutilisation.

Ad article 27

Cet article énonce limitativement les informations et éléments que la demande de traitement ultérieur de données à caractère personnel doit contenir.

Il énonce également de manière expresse les documents qui doivent être annexés à la demande, à savoir l'analyse d'impact relative à la protection des données à caractère personnel visée par les dispositions du règlement (UE) 2016/679 ainsi que la notice d'information à l'adresse des personnes concernées, de même que le plan de confidentialité signé par les acteurs impliqués par ledit traitement.

La responsabilité de veiller à l'exactitude des informations contenues dans la demande et les pièces jointes repose exclusivement sur les entités publiques qui soumettent la demande à l'Autorité des données. Cette dernière ne saurait être tenue responsable d'éventuels manquements par le demandeur ou d'éventuelles non-conformités des documents, tels que l'analyse d'impact relative à la protection des données visée par l'article 35 du règlement (UE) 2016/679 ou l'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679, versés par le demandeur. Il en va de même pour le plan de confidentialité soumis à l'Autorité des données dans le cadre de la demande.

Dans ce sens, le paragraphe 3 prévoit expressément que les entités publiques effectuant le traitement ultérieur de données à caractère personnel certifient l'exactitude des informations contenues dans la demande et les pièces jointes, ainsi que le fait que le plan de confidentialité tient compte de tous les éléments de la demande. Ils s'engagent, en outre, formellement à respecter les termes de l'autorisation de l'Autorité des données et du plan de confidentialité.

Toute fourniture, lors de l'introduction de la demande, d'informations sciemment inexactes ou en violation avec les dispositions de l'article 27 entraînent l'application de sanctions pénales (article 38).

Ad article 28

Cet article prévoit de manière explicite les informations à présenter par les réutilisateurs de données dans le cadre d'une demande d'accès et de réutilisation visée au titre VI du projet de texte.

Tout comme pour les demandes couvrant les cas de figure visés au titre V, l'article énonce de manière limitative les documents à joindre par le réutilisateur de données à sa demande d'accès et de réutilisation.

La responsabilité de veiller à l'exactitude des informations contenues dans la demande et les pièces jointes repose exclusivement sur les réutilisateurs de données qui soumettent la demande à l'Autorité des données. Cette dernière ne saurait être tenue responsable pour d'éventuels manquements par le demandeur ou pour d'éventuelles non-conformités des documents, tels que l'analyse d'impact relative à la protection des données visée par l'article 35 du règlement (UE) 2016/679 ou l'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679, versés par le demandeur. Il en va de même pour le plan de confidentialité soumis à l'Autorité des données dans le cadre de la demande.

Dans ce sens, le paragraphe 5 prévoit expressément que les réutilisateurs de données certifient l'exactitude des informations contenues dans la demande et les pièces jointes ainsi que le fait que le plan de confidentialité tient compte de tous les éléments de la demande. Ils s'engagent, en outre, formellement à respecter les termes de l'autorisation de l'Autorité des données et du plan de confidentialité. Ceci s'applique sans préjudice des dispositions du règlement (UE) 2022/868, notamment de l'article 5, paragraphe 10 dudit règlement.

Toute fourniture, lors de l'introduction de la demande, d'informations sciemment inexactes ou en violation avec les dispositions de l'article 28 entraîne l'application de sanctions pénales (article 38).

Section III – Instruction de la demande par l'Autorité des données

Ad article 29

Cet article précise que les demandes de traitements ultérieurs de données à caractère personnel conformément au titre V ainsi que les demandes de réutilisation de données conformément au titre VI doivent être déposées auprès de l'Autorité des données et prévoit la procédure de dépôt.

Il prévoit également des dispositions spécifiques visant le cas où le demandeur sollicite une modification limitée à la durée (prévue aux articles 27, paragraphe 1er, point 7° ou 28, paragraphe 1er, point 10°) couverte par l'autorisation initiale de l'Autorité des données.

La procédure de modification ponctuelle de la durée est inspirée du régime mis en œuvre par l'autorité finlandaise « *FinData* » (« *Social and health data permit authority* ») dans le contexte de la législation sur la réutilisation des données de santé et de la sécurité sociale sous le régime du « *Act on the Secondary Use of Health and Social Data* ».

Pour éviter la suppression irrémédiable des données liées à un projet autorisé, ces dernières sont conservées dans un système d'archivage intermédiaire à accès restreint pendant le délai d'instruction

de la demande de modification ponctuelle, lorsque le temps pris pour instruire la demande excède la durée couverte par l'autorisation initiale de l'Autorité des données.

Pour éviter toute fraude ou traitement illicite d'informations dans le système d'archivage intermédiaire, le Centre, en tant que gestionnaire de l'environnement de traitement sécurisé, doit au moins mettre en œuvre les garanties appropriées prévues par la disposition sous examen.

Dans un souci de simplification administrative, le paragraphe 5 prévoit une procédure spécifique lorsque l'Autorité des données demande des renseignements complémentaires au demandeur. L'objectif est d'éviter que le demandeur ne doive recommencer l'entière procédure prévue au titre VII en raison d'un élément mineur qui fait défaut ou devrait être clarifié. Si le demandeur ne répond pas dans un délai d'un mois, sa demande est rejetée d'office.

Cela étant dit, la procédure spécifique du paragraphe 5 est sans préjudice des cas de figure où l'Autorité des données est appelée à déclarer irrecevable les demandes qui ne comprennent pas tous les éléments énoncés aux articles 27 ou 28.

Ad article 30

Cet article prévoit que l'Autorité des données fixe, pour chaque demande de traitement ultérieur des données ou d'accès et de réutilisation des données, une redevance afin couvrir les frais administratifs occasionnés par le traitement de la demande et par la mise à disposition des données dans l'environnement de traitement sécurisé.

La procédure applicable à la perception de la redevance est fixée par règlement grand-ducal.

Ad article 31

Cet article prévoit les cas dans lesquels l'Autorité des données délivre l'autorisation conformément aux titres V à VII de la loi sous examen.

Le système proposé s'inscrit dans la mise en œuvre des garanties appropriées conformément à l'article 89, paragraphe 1er du règlement (UE) 2016/679 et dans la mise en œuvre des dispositions du règlement (UE) 2022/868.

Ainsi, l'Autorité des données autorise toute demande qui respecte les conditions énoncées à l'article sous examen, après s'être assurée, sur base d'un examen quant au fond, de l'absence d'atteinte disproportionnée aux droits et libertés d'autrui au regard des finalités poursuivies.

A noter que le demandeur qui se voit accorder une autorisation de l'Autorité des données est tenu de respecter les conditions émises.

Les décisions d'autorisation ou de refus de l'Autorité des données doivent être motivées. Elles comportent comme pièces jointes, la demande qui lui a été présentée ainsi que, le cas échéant, l'avis du Conseil consultatif.

Le paragraphe 4 prévoit les conditions dans lesquelles une modification substantielle du traitement ultérieur de données à caractère personnel visé au titre V ou de l'accès et de la réutilisation des données visés au titre VI couverts par une autorisation de l'Autorité des données peut être sollicitée par le demandeur initial. Dans l'hypothèse où l'entité publique effectuant le traitement ultérieur de données à caractère personnel couvert par l'autorisation initiale de l'Autorité des données sollicite une modification substantielle de celui-ci, elle est tenue d'introduire une nouvelle demande et de recommencer la procédure prévue au titre VII de la loi. Constituent notamment une modification substantielle du traitement ultérieur autorisé :

– un élargissement du contexte du traitement de données envisagé, que ce soit au niveau des organismes du secteur public détenant les données, qu'au niveau des destinataires des données ;
– une modification des conditions d'anonymisation ou de pseudonymisation des données à caractère personnel ;
– une modification des catégories de données ou de personnes concernées ;
– une modification des finalités de l'accès et de la réutilisation.

A noter que la procédure est identique pour les cas où la modification substantielle porte sur l'accès et la réutilisation des données visés au titre VI.

En dérogation à cette procédure, le paragraphe 5 instaure une procédure spécifique pour les cas où la modification sollicitée porte exclusivement sur les éléments visés à l'article 27, paragraphe 1er,

point 7° ou à l'article 28, paragraphe 1er, point 10° autorisés par l'Autorité des données. Dans ces cas de figure, l'Autorité des données est appelée à statuer par voie de procédure accélérée conformément aux dispositions de l'article 29, paragraphe 3.

A l'instar des dispositions du règlement européen relatif à l'espace européen des données de santé, le texte impose aux entités publiques et aux organismes du secteur public de mettre les données à caractère personnel et les données à caractère non personnel visées par l'autorisation de l'Autorité des données à disposition de celle-ci en vue de la mise en œuvre des mesures d'anonymisation, de pseudonymisation et d'agréagtion ainsi que de leur mise à disposition de l'environnement de traitement sécurisé.

Par ailleurs, l'article prévoit que les entités publiques traitant ultérieurement les données à caractère personnel et les réutilisateurs de données doivent traiter les données uniquement conformément aux termes de l'autorisation de l'Autorité des données.

Ad article 32

Conformément aux dispositions du règlement (UE) 2022/868, l'Autorité des données a le droit de vérifier le processus, les moyens et tout résultat du traitement ultérieur de données à caractère personnel et des accès et réutilisations de données faits conformément aux dispositions du projet de loi, afin de préserver l'intégrité de la protection des données ainsi que des autres droits éventuellement applicables, tels que la propriété intellectuelle ou la confidentialité commerciale.

Pour autant, le Centre reste le garant de l'efficacité de l'anonymisation et de la pseudonymisation des données à caractère personnel ainsi que de la modification, de l'agrégation, de la suppression et du contrôle de la divulgation des données, conformément aux exigences de la loi sous examen et du règlement (UE) 2022/868.

Dans l'hypothèse où l'Autorité des données constate que les résultats contiennent des informations qui seraient susceptibles de porter atteinte aux droits et intérêts de tiers, elle a le droit d'interdire l'utilisation desdits résultats. Sa décision d'interdiction doit être transparente et compréhensible pour les réutilisateurs de données.

Les dispositions de l'article 32 s'entendent sans préjudice des prérogatives de la Commission nationale pour la protection des données d'interdire les traitements de données à caractère personnel opérés en contravention aux conditions reprises dans l'autorisation émise par l'Autorité des données, conformément au règlement (UE) 2016/679, lu ensemble avec la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Section IV – Publicité par l'Autorité des données

Ad article 33

L'article 33 met en œuvre les exigences prévues, en particulier à l'article 5, paragraphe 1er du règlement (UE) 2022/868.

Il n'appelle pas d'observations particulières.

Ad article 34

L'Autorité des données tient un registre des traitements ultérieurs de données à caractère personnel autorisés conformément au titre V, ainsi que des accès et réutilisations des données autorisés conformément au titre VI. Le registre est accessible publiquement. Ce registre contient pour chaque autorisation accordée, une copie de la décision adoptée ainsi que, si applicable, l'avis du Conseil consultatif et la notice d'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679 à communiquer par le demandeur.

Dans un objectif de transparence, la publication des éléments d'information à destination des personnes concernées visée au paragraphe 2 vaut information des personnes concernées au sens des articles 12 à 14 du règlement (UE) 2016/679.

Le système central d'information des personnes concernées constitue une avancée substantielle par rapport au *status quo*, qui se caractérise par une diversité de canaux de communication indirects d'informations (notamment sur les différents sites internet) à l'adresse des personnes concernées sur les

traitements de données à caractère personnel, conformément à l'article 14, paragraphe 5 du règlement (UE) 2016/679.

La responsabilité de veiller à l'exactitude des éléments contenus dans la notice d'information soumis à l'Autorité des données revient exclusivement aux entités publiques effectuant le traitement ultérieur des données à caractère personnel et aux réutilisateurs de données. L'Autorité des données ne saurait être tenue responsable d'éventuels manquements par le demandeur ou d'éventuelles non-conformités de l'information à destination des personnes concernées au regard des dispositions du règlement (UE) 2016/679.

Section V – Mesures appropriées et mise à disposition des données dans un environnement de traitement sécurisé

Ad article 35

Cet article impose la mise en œuvre de mesures d'anonymisation et/ou de pseudonymisation des données à caractère personnel et/ou de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données préalablement aux traitements ultérieurs de données à caractère personnel et aux réutilisations de données. Ces mesures doivent être effectives et efficaces pour éviter toute réidentification des personnes concernées ainsi que toute atteinte aux droits de tiers, telles que la confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise, le secret statistique et de propriété intellectuelle.

Pour garantir la confidentialité des données, le paragraphe 1er instaure le principe de l'anonymisation, de la pseudonymisation et de l'agrégation des données à la source, et ce afin que nul autre que l'entité publique ou l'organisme du secteur public desquelles proviennent les données n'ait accès aux données en clair.

Le recours à de telles mesures appropriées à la source s'inscrit dans une optique de mise en œuvre de garanties appropriées pour les droits et libertés de la personne concernée conformément à l'article 89, paragraphe 1er du règlement (UE) 2016/679. Il permet également d'assurer le respect des exigences instaurées par le règlement (UE) 2022/868.

Le paragraphe 2 énonce la procédure applicable et prévoit que les méthodes et modalités des mesures d'anonymisation, de pseudonymisation et d'agrégation des données doivent être choisies et mises en œuvre sur base d'une évaluation spécifique à la demande.

L'évaluation des mesures spécifiques à mettre en œuvre est initiée par l'acteur qui souhaite introduire une demande d'autorisation à l'Autorité des données conformément à l'article 29, à savoir, dans les cas visés au titre V, par les entités publiques effectuant le traitement ultérieur de données à caractère personnel et, dans les cas visés au titre VI, par les réutilisateurs de données.

Cette analyse doit être consignée dans un plan de confidentialité.

Le Centre, ou le tiers de confiance mandaté par le Centre, fort de son expertise en la matière, doit valider le projet de plan de confidentialité qui lui est soumis. Afin de lui permettre d'évaluer les besoins spécifiques d'anonymisation et de pseudonymisation des données à caractère personnel et/ou les besoins spécifiques liés à la modification, l'agrégation, la suppression et au traitement selon toute autre méthode de contrôle de la divulgation des données, le demandeur doit, de sa propre initiative et sur sollicitation, fournir au Centre, ou au tiers de confiance mandaté par le Centre, toute information pertinente liée au traitement ultérieur de données à caractère personnel ou à l'accès et la réutilisation de données.

Rien n'empêche que le LNDS soit sollicité par le demandeur pour lui fournir une assistance dans le cadre de la préparation et de l'amendement du plan de confidentialité. Cette assistance peut prendre la forme de propositions sur la meilleure manière d'anonymiser et de pseudonymiser les données à caractère personnel et d'agréger les données. Cela étant dit, lorsque le demandeur a recours aux services offerts par le LNDS pour préparer le plan de confidentialité et la demande, l'obligation de fourniture de renseignements s'applique également en cas de demande du LNDS.

Le plan de confidentialité est amendé jusqu'à validation finale et signature par tous les acteurs concernés. Il contient une description détaillée des mesures appropriées à mettre en œuvre et précise les obligations respectives des acteurs. Par ailleurs, il attribue clairement et de manière univoque les responsabilités respectives dans la mise en œuvre desdites mesures. Sans préjudice des obligations d'anonymisation, de pseudonymisation et d'agrégation à la source, ceci pourrait notamment impliquer

que le Centre soit chargé de contrôler que les jeux de données anonymisés, pseudonymisés et/ou agrégés à la source ne permettent pas, notamment, la réidentification des personnes concernées après leur traitement et combinaison conformément au paragraphe 4.

En signant le plan de confidentialité, le Centre, ou le tiers de confiance mandaté par le Centre, certifie que les mesures prévues au paragraphe 1er consignées dans le plan de confidentialité sont effectives et efficaces pour éviter toute réidentification des personnes concernées ainsi que toute atteinte aux droits de tiers, tels que la confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise, le secret statistique et de propriété intellectuelle, de sorte que ces exigences techniques ne font plus l'objet d'une vérification par l'Autorité des données.

Compte tenu du fait que le Centre doit certifier la faisabilité de la mise en œuvre des mesures énoncées dans le plan de confidentialité et de la mise à disposition des données dans l'environnement de traitement sécurisé, le Centre doit être impliqué au cours de l'élaboration du plan de confidentialité. L'objectif est de s'assurer, en amont, de la faisabilité du projet et d'œuvrer, dès le départ, vers un plan de confidentialité viable et réalisable. L'attestation de faisabilité du Centre doit être jointe à la demande visée aux articles 27 et 28 de la loi.

Le paragraphe 4 a trait aux actions à prendre par le Centre, ou par le tiers de confiance mandaté par ce dernier.

Sans préjudice de l'obligation de procéder à l'anonymisation, de la pseudonymisation et de l'agrégation à la source, la combinaison et le traitement des données doit se faire exclusivement sous le contrôle du Centre. Ceci permet d'éviter des fuites de données détenues par les organismes du secteur public ainsi que des risques de réidentification potentiels. Ainsi, il est formellement exclu que les données détenues par les acteurs publics sortent de leur environnement sécurisé en vue d'une combinaison éventuelle, notamment par des entités privées avec leurs propres données, car ceci augmente potentiellement le risque de réidentification. Cette restriction constitue dès lors un garde-fou important pour le respect des droits et libertés individuels. Elle permet également d'éviter que des données soient mises à disposition dans l'environnement de traitement sécurisé en l'absence d'autorisation de l'Autorité des données.

Ad article 36

Conformément au règlement (UE) 2022/868, il est instauré un environnement de traitement sécurisé. Il est mis à disposition par l'Autorité des données et géré par le Centre.

L'environnement de traitement sécurisé constitue une garantie essentielle en ce qu'il permet de ne pas transmettre directement les données sollicitées aux réutilisateurs et de conserver le contrôle sur ces dernières notamment en sélectionnant quelles opérations de traitement peuvent y être réalisées (notamment l'affichage, le stockage, la suppression, l'exportation) et en encadrant strictement l'extraction des données/résultats (ex. interdiction d'extraction de données non anonymisées). Il constitue ainsi une garantie appropriée pour les droits et libertés de la personne concernée conformément à l'article 89, paragraphe 1er du règlement (UE) 2016/679.

Ainsi, le réutilisateur de données travaillant dans l'environnement de traitement sécurisé devrait pouvoir réutiliser les données uniquement aux fins et de la manière présentées dans la demande et telles que prévues dans l'autorisation. Le réutilisateur de données ne devrait pas pouvoir reproduire les données, de plus les données devraient y être mises à disposition uniquement dans le cadre d'une demande autorisée de manière cloisonnée. Le système proposé s'inscrit dans le même ordre d'idées que la « *Luxembourg Microdata Platform on Labour and Social Protection* » développée par l'Inspection générale de la sécurité sociale (IGSS).

L'article prévoit également les exigences que l'environnement de traitement sécurisé doit remplir, à savoir notamment la journalisation des accès, les conditions d'authentification des réutilisateurs de données ainsi que le fait que les accès doivent se limiter aux seules données sur lesquelles portent l'autorisation de l'Autorité des données.

Afin de conserver le contrôle de l'environnement de traitement sécurisé et des données qui y sont mises à disposition, cet environnement de traitement sécurisé ne doit pas permettre au réutilisateur de données d'y ajouter des données ou de les combiner avec les données provenant des organismes du secteur public sans avoir obtenu l'autorisation de l'Autorité des données.

Dans le même objectif, il n'est pas permis d'introduire dans l'environnement de traitement sécurisé des solutions technologiques, sauf dans les conditions établies par la loi.

Le paragraphe 4 vise des réutilisations transfrontalières de données. Le système proposé permet au Centre, sous réserve de l'autorisation de l'Autorité des données, de créer un environnement de traitement sécurisé commun entre organismes compétents de l'Union européenne désignés conformément à l'article 7 du règlement (UE) 2022/868 et de combiner les données sollicitées dans un tel contexte.

Ad article 37

A l'instar des dispositions du règlement européen relatif à l'espace européen des données de santé, l'article précise les rôles et responsabilités des parties impliqués dans le traitement ultérieur des données à caractère personnel et dans la réutilisation des données. Il instaure une chaine de responsabilité du traitement de données. En ce faisant, l'article clarifie que les acteurs qu'il vise dans ses paragraphes 1 à 3 n'agissent pas comme responsables conjoints du traitement, mais chacun de manière successive pour les opérations de traitement de données à caractère qu'il opère conformément à la loi. De ce fait, il assure la cohérence avec les dispositions de la réglementation sectorielle, notamment celles prévues par le règlement européen relatif à l'espace européen des données de santé.

Ainsi, les entités publiques et les organismes du secteur public détenant les données ont la qualité de responsable du traitement pour la mise à disposition des données à caractère personnel sollicitées.

L'Autorité des données, à son tour, la qualité de responsable du traitement pour le traitement de données à caractère personnel réalisé dans le cadre de l'accomplissement de ses missions conformément à la présente loi, ceci sans préjudice de la possibilité de sous-traiter des tâches à d'autres acteurs. Partant, notamment dans les cas visés aux articles 35 et 36, le Centre agit comme sous-traitant de l'Autorité des données. Le Centre peut sous-traiter ultérieurement les tâches et missions lui attribuées conformément à la loi. Dans ce contexte, la loi régit les relations de sous-traitance entre l'Autorité des données et le Centre au sens de l'article 28 du règlement (UE) 2016/679, de sorte qu'un encadrement conventionnel desdites relations ne s'impose plus.

Les entités publiques qui traitent ultérieurement les données à caractère personnel et les réutilisateurs de données ont, à leur tour, la qualité de responsable du traitement pour les traitements de données à caractère personnel dans l'environnement de traitement sécurisé.

Section VI – Recours

Ad article 38

Les décisions adoptées par l'Autorité des données conformément aux dispositions du titre VII sont des actes administratifs. Si ces actes font grief, ils peuvent être portés devant les juridictions administratives.

Le recours sera un recours devant le Tribunal administratif qui statue comme juge du fond. Les règles de procédure et de délais applicables sont celles qui régissent ces juridictions.

Les dispositions retenues sont reprises de l'article 55 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

TITRE VIII – Gouvernance en matière de services d'intermédiation de données et d'altruisme des données

Section I – Services d'intermédiation de données

Ad article 39

Conformément à l'article 13 du règlement (UE) 2022/868, la Commission nationale pour la protection des données est désignée autorité compétente pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données.

Cet article n'appelle pas d'observations particulières.

Ad article 40

L'article précise que la CNPD dispose des pouvoirs de contrôle tels que prévus à l'article 14 du règlement (UE) 2022/868.

Cette disposition n'appelle pas d'observations particulières.

Ad article 41

L'article précise qu'un règlement interne de la Commission nationale pour la protection des données définit la procédure en matière de notification pour les services d'intermédiation de données, conformément à l'article 11 du règlement (UE) 2022/868.

Cette disposition n'appelle pas d'observations particulières.

Ad article 42

L'article précise que la Commission nationale pour la protection des données peut, conformément à l'article 11, paragraphe 11, du règlement (UE) 2022/868, imposer des redevances proportionnées et objectives pour la notification des services d'intermédiation. Les modalités de paiement des redevances sont déterminées par règlement de la Commission nationale pour la protection des données.

Ad article 43

Dans le cadre d'une violation de l'obligation de notification incombant aux prestataires de services d'intermédiation de données en vertu de l'article 11 du règlement (UE) 2022/868 ou des conditions liées à la fourniture de services d'intermédiation de données en vertu de l'article 12 du règlement (UE) 2022/868, la CNPD peut, par voie de décision, imposer des amendes administratives. L'article prévoit une fourchette pour la détermination des amendes. Par ailleurs, il prévoit la possibilité pour la Commission nationale pour la protection des données d'infliger des astreintes.

Section II – Altruisme des données

Ad article 44

A l'instar des dispositions de l'article 23 du règlement (UE) 2022/868, la Commission nationale est l'autorité compétente responsable du registre public national des organisations altruistes en matière de données reconnues.

Par ailleurs, l'article impose à la Commission nationale pour la protection des données la tenue et la mise à jour du registre public national des organisations altruistes en matière de données reconnues.

Ad article 45

L'article prévoit que la Commission nationale pour la protection des données dispose des pouvoirs de contrôle prévus à l'article 24 du règlement (UE) 2022/868.

Cette disposition n'appelle pas d'observations particulières.

Section III – Recours

Ad article 46

Les décisions adoptées par la Commission nationale pour la protection des données conformément aux sections I et II du titre VIII sont des actes administratifs. Si ces actes font grief, ils peuvent être portés devant les juridictions administratives.

Le recours sera un recours devant le Tribunal administratif qui statue comme juge du fond. Les règles de procédure et de délais applicables sont celles qui régissent ces juridictions.

TITRE IX – Dispositions finales

Ad article 47

L'article définit l'intitulé de citation de la loi.

Cette disposition n'appelle pas d'observations particulières.

*

FICHE FINANCIERE

(Article 79 de la loi modifiée du 8 juin 1999 sur le Budget,
la Comptabilité et la Trésorerie de l'État)

Le projet de loi faisant objet engendre aussi bien un impact financier qu'un besoin de recrutement en effectifs.

Le projet de loi relatif à la valorisation des données dans un environnement de confiance met, notamment, en œuvre le règlement (UE) 2022/868 sur la gouvernance des données (« data governance act »), applicable depuis le 24 septembre 2023 qui prévoit le cadre réglementaire pour la réutilisation, par des acteurs du secteur privé, des données détenues par les organismes du secteur public.

Le règlement (UE) 2022/868 impose aux États membres de prévoir les conditions applicables à la réutilisation des données et d'assortir ces réutilisations d'un contrôle rigoureux des règles de protection desdites données, et ce par le biais d'une autorisation préalable de réutilisation.

Dans cette optique, le projet de loi sous rubrique prévoit, en particulier, les rôles et responsabilités des différents organismes compétents, la procédure applicable à l'octroi des autorisations de réutilisation des données ainsi que les conditions applicables à la réutilisation des données.

A noter que le projet de loi sous rubrique instaure également :

- le principe du « once only », selon lequel une personne fournit une seule fois des données aux autorités publiques, sans avoir à le faire à plusieurs reprises. Cette mesure de simplification administrative, qui constitue une priorité du Gouvernement, fera économiser beaucoup de temps, de ressources et d'argent à tous les acteurs concernés, qu'il s'agisse des citoyens et des entreprises ou de l'administration publique. Dans une optique de cohérence et de transparence administrative, le Commissariat sera impliqué dans la mise en œuvre des formalités administratives (ex. tenue des protocoles d'échange de données entre entités publiques dans le cadre du « once only » et leur publication).
- le principe selon lequel les traitements de données opérés par les entités publiques en lien avec l'exécution des missions d'intérêt public leurs conférées par les dispositions applicables sont licites, sans qu'il soit nécessaire de disposer d'une loi spécifique qui précise toutes les modalités du traitement de données à caractère personnel.

Le Centre des technologies de l'information de l'État, dénommé ci-après par le terme « CTIE » est désignée organisme compétent au sens de l'article 7, paragraphe 1er, du règlement (UE) 2022/868 pour aider l'Autorité des données dans l'exercice de ses missions conformément aux dispositions de la présente loi. Le CTIE aura notamment pour mission de gérer l'environnement de traitement sécurisé prévu à l'article 36, qui est mis à disposition des réutilisateurs de données, et de fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles. En outre le CTIE assurera de la mise en œuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou à de modification, d'agrégation, de suppression et de traitement des informations et données selon toute autre méthode de contrôle de la divulgation des données conformément au plan de confidentialité, préalablement à la mise à disposition des données dans l'environnement de traitement sécurisé.

Un rôle crucial reviendra au Commissariat du gouvernement à la protection des données auprès de l'État (« Commissariat »). Pour des raisons d'économie budgétaire, de gestion efficace des finances publiques et de cohérence procédurale, le Commissariat est désigné comme organisme compétent pour octroyer ou refuser l'accès à des fins de réutilisation des données détenues par les organismes du secteur public. En tant que structure spécialisée expérimentée dans le conseil en matière de réutilisation de données, il agira comme « Autorité des données » centralisée compétente conformément à l'article 7 du règlement (UE) 2022/868 pour octroyer et pour refuser l'accès aux données détenues par les organismes du secteur public aux fins de leur réutilisation par toute partie intéressée.

Par ailleurs, il interviendra comme entité centralisée, compétente pour autoriser les traitements de données à caractère personnel par les entités publiques et pour gérer les protocoles d'échange de données entre entités publiques dans le cadre du « *once only* ».

Le ministère de la Digitalisation assurera l'instauration d'un point d'information unique conformément à l'article 8 du règlement (UE) 2022/868. Ce point d'information unique a pour mission de recevoir les demandes d'accès et de réutilisation de données visées, de les transmettre à l'Autorité des

données et d'assurer les échanges et les démarches. En outre, il a la charge de la mise à disposition d'un catalogue des ressources consultables contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

Impact financier

Le projet de loi n'engendre a priori pas un budget supplémentaire auprès du ministère de la Digitalisation et du CTIE, comme les coûts pour remplir leurs missions décrites sont inclus dans les limites budgétaires prévues dans le budget pluriannuel du ministère et du CTIE.

Les coûts pour la mise en place d'une plateforme back-office pour la gestion des demandes d'accès et des autorisations, sont estimés à 750.000 EUR est sont également inclus dans les limites budgétaires prévues dans le budget pluriannuel du CTIE.

Le groupement d'intérêt économique PNED G.I.E. – Plateforme nationale d'échange de données, désigné ci-après par le terme « LNDS », est désigné organisme compétent au sens de l'article 7, paragraphe 1er, du règlement (UE) 2022/868. Les tâches lui conférées par le ministère, le CTIE ou le Commissariat sont réalisées dans les limites budgétaires du G.I.E.

Conformément à l'article 30 du projet de loi, pour chaque demande d'accès, l'autorité des données perçoit une redevance qui se compose :

a) d'un forfait fixe pour couvrir la charge administrative du traitement de la demande ;

b) des coûts réels facturés par les sous-traitants du ministère, du CTIE ou du Commissariat dans le cadre de la validation du plan de confidentialité et de l'anonymisation/pseudonymisation des données ;

c) des coûts du CTIE pour la mise à disposition des données dans un environnement de traitement sécurisé ;

A titre indicatif :

- Les coûts forfaitaires sous a) pourrait être fixés à environ 500 EUR par demande déposée.
- Les coûts sous b) dépendent de la complexité du dossier et des moyens et méthodes techniques mises en œuvre par le plan de confidentialité.
- Les coûts sous c) sont actuellement estimés à de 125 euros HTVA par jour pour la mise à disposition d'un environnement de traitement sécurité standard (1 GPU vCore + 5GB RAM, 6 CPU vCore + 32GB RAM, 256GB BS, 1TB OS).

Cependant la préparation des nouvelles missions prévues d'être attribuées au Commissariat en tant qu'« Autorité des données » conformément aux règlement (UE) 2022/868 et au projet de loi régissant la réutilisation des données à caractère personnel par les entités publiques et le « once only » au sein du secteur public constitue une tâche nouvelle non prévue dans le cadre de la préparation initiale du budget 2024 (déposées au courant du mois d'avril 2023) ainsi que dans le cadre de la planification pluriannuelle 2025-2027.

Toutefois, ces missions requièrent prévisiblement l'investissement de larges parties du budget du Commissariat pour l'année 2024.

En effet, la réalisation des travaux d'analyse préparatoires ainsi requise vise à établir dans une première phase (surtout 2025), en particulier :

- l'optimisation des processus de travail, afin de réduire le temps de traitement des demandes (de par la loi a priori 2 mois) ;
- la prise de décisions administratives par l'Autorité des données, en particulier la préparation de modèles de décisions (irrecevabilités, demandes de renseignements complémentaires, refus, autorisations, etc.) ;
- la définition des modalités d'échanges entre organismes compétents au sens de la règlementation susmentionnée ainsi que leur perfectionnement et mise en œuvre.

Dans une deuxième phase (2026 et suivants), le budget pour frais d'experts et d'études sollicité de 375.000 EUR par année est nécessaire pour permettre au Commissariat d'assurer la mise en œuvre des nouvelles tâches prévues de lui être attribuées par la réglementation susvisée (sans négliger pour autant ces missions actuelles), et ce en particulier dans le contexte.

En outre, il est nécessaire d'augmenter le budget relatif aux frais de bureau à 12.000 EUR et le budget relatif aux Indemnités pour services de tiers, honoraires d'experts, frais de formation, frais de maintenance, frais de publicité, de sensibilisation et d'information, acquisition de machines de bureau, dépenses diverses à 80.000 EUR (tendance croissante pour les années 2026 à 2028), et ce proportionnellement aux recrutements envisagés pour les années 2025 à 2028.

Le tableau ci-après illustre les budgets supplémentaires précités

	Libellé	*2024*	*2025*	*2026*	*2027*	*2028*
		Budget voté	*Proposition budgétaire*	*Prévision*	*Prévision*	*Prévision*
12.041	Frais de bureau	6	12 (6)	18 (6)	20 (6)	22
12.121	Frais d'experts et d'études.	275	375 (89)	375 (89)	375 (89)	375
12.346	Indemnités pour services de tiers, honoraires d'experts, frais de formation, frais de maintenance, frais de publicité, de sensibilisation et d'information, acquisition de machines de bureau, dépenses diverses.	60	80 (62)	85 (63)	90 (64)	90

Unité : Milliers d'euros ; Les chiffres en () sont celles indiquées dans le budget pluriannuel 2024

Partant des budgets indiqués dans le plan pluriannuel du budget 2024, le projet de loi engendre une enveloppe budgétaire supplémentaire de **310.000 EUR pour l'année 2025 et les années à suivre**.

Le renforcement en personnel devra être considéré dans le cadre de la procédure CER pour les budgets 2025 et 2026.

Contribution à une simplification administrative

En tant que structure spécialisée centrale disposant d'une longue expérience dans le conseil en matière de traitement et de réutilisation de données, le Commissariat prend le rôle de facilitateur de la réutilisation des données détenues par les organismes du droit public. En effet, les réutilisateurs – acteurs de la recherche publique ainsi que des acteurs économiques – sauraient s'adresser à une seule autorité pour toutes les démarches.

Dans cet ordre d'idées, le système proposée (inspiré du système finlandais ayant fait ses preuves) contribue à l'activité économique de la place luxembourgeoise. Il favorise également un environnement propice pour la recherche scientifique.

Par ailleurs, l'Autorité des données pourrait intervenir comme pivot central dans la mise en œuvre des réglementations futures, tel que le règlement sur le « *European Health Data Space* ». Ces textes prévoient également l'autorisation des réutilisations de données par un acteur spécialisé.

Ainsi, le fait d'instaurer une Autorité des données dans le cadre du règlement (UE) 2022/868 pourrait permettre d'éviter l'insécurité juridique et le recoupement de compétences entre différents acteurs dans le cadre de la mise en œuvre des réglementations sectorielles visant la réutilisation des données.

*

CHECK DURABILITÉ - NOHALTEGKEETSCHECK

La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

Ministre responsable :	La Ministre de la Digitalisation
Projet de loi ou amendement :	Projet de loi 1) relatif à la valorisation des données dans un environnement de confiance ; 2) relatif à la mise en œuvre du principe « once only » ; 3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ; 4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Le check durabilité est un outil d'évaluation des actes législatifs par rapport à leur impact sur le developpement durable. Son objectif est de donner l'occasion d'introduire des aspects relatifs au développement durable à un stade préparatoire des projets de loi. Tout en faisant avancer ce thème transversal qu'est le developpement durable, il permet aussi d'assurer une plus grande cohérence politique et une meilleure qualité des textes législatifs.

1. Est-ce que le projet de loi sous rubrique a un impact sur le champ d'action (1-10) du 3ème Plan national pour un Développement durable ?
   En cas de réponse négative, expliquez-en succinctement les raisons.
   En cas de réponse positive sous 1., quels seront les effets positifs et / ou négatifs éventuels de cet impact?

2. Quelles catégories de personnes seront touchées par cet impact ?

3. Quelles mesures sont envisagées afin de pouvoir atténuer les effets négatifs et comment pourront être renforcés les aspects positifs de cet impact ?

Afin de faciliter cet exercice, l'instrument du contrôle de la durabilité est accompagné par des points d'orientation – **auxquels il n'est pas besoin de réagir ou répondre mais qui servent uniquement d'orientation** - , ainsi que par une documentation sur les dix champs d'actions précités.

1. Assurer une inclusion sociale et une éducation pour tous. Poins d'orientation Documentation ☐ Oui ☒ Non

2. Assurer les conditions d'une population en bonne santé. Poins d'orientation Documentation ☐ Oui ☒ Non

3. Promouvoir une consommation et une production durables. Poins d'orientation / Documentation ☐Oui ☒Non

4. Diversifier et assurer une économie inclusive et porteuse d'avenir. Poins d'orientation / Documentation ☒Oui ☐Non

Le présent projet de loi, en visant à valoriser les données du secteur public dans un environnement de confiance, contribue à la croissance économique et l'innovation en définissant les conditions afin que les applications et la valeur de l'information des données du secteur public puissent être multipliées, tout en garantissant le respect des droits de tiers.

D'une part, la mise en oeuvre du principe once only renforce la transparence du secteur public et en instaurant ce principe selon lequel une personne fournit une seule fois des données aux entités publiques, au lieu de devoir le faire à plusieurs reprises, rendra plus rapides et plus efficaces les procédures pour les citoyens, les entreprises et les entités publiques. Le système « once only » constitue ainsi une vraie mesure de simplification administrative qui permettra de diminuer les dépenses et favorisera une gestion plus efficace des ressources des entités publiques.

D'autre part, en définissant les conditions régissant le traitement ultérieur des données du secteur public au sein-même du secteur public, ainsi que les conditions régissant la réutilisation des données de secteur public sujettes aux droits de tiers, en complément du régime juridique régissant l'Open Data, le présent projet de loi contribue à faciliter la valorisation et l'exploitation des données du secteur public, une vaste ressource de données qui peuvent contribuer à de multiples innovations, y inclus la recherche et le développement de nouveaux services et politiques publics, de nouvelles connaissances, et de nouveaux produits et services, dont l'ensemble de l'économie pourra bénéficier et stimulant ainsi la société de l'information.

5. Planifier et coordonner l'utilisation du territoire. Poins d'orientation / Documentation ☐Oui ☒Non

6. Assurer une mobilité durable. Poins d'orientation / Documentation ☐Oui ☒Non

7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles. Poins d'orientation / Documentation ☐Oui ☒Non

8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable. Poins d'orientation / Documentation ☐Oui ☒Non

9. Contribuer, sur le plan global, à l'éradication de la pauvreté et à la cohérence des politiques pour le développement durable.	Poins d'orientation Documentation	☐ Oui	☒ Non

10. Garantir des finances durables.

Poins d'orientation
Documentation

☐ Oui ☒ Non

Cette partie du formulaire est facultative - Veuillez cocher la case correspondante

En outre, et dans une optique d'enrichir davantage l'analyse apportée par le contrôle de la durabilité, il est proposé de recourir, de manière facultative, à une évaluation de l'impact des mesures sur base d'indicateurs retenus dans le PNDD. Ces indicateurs sont suivis par le STATEC.

Continuer avec l'évaluation ? ☐ Oui ☒ Non

(1) Dans le tableau, choisissez l'évaluation : **non applicable**, ou de 1 = **pas du tout probable** à 5 = **très possible**

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
1		Contribue à la réduction du taux de risque de pauvreté ou d'exclusion sociale	Taux de risque de pauvreté ou d'exclusion sociale	% de la population
1		Contribue à la réduction du nombre de personnes vivant dans des ménages à très faible intensité de travail	Personnes vivant dans des ménages à très faible intensité de travail	milliers
1		Contribue à la réduction de la différence entre taux de risque de pauvreté avant et après transferts sociaux	Différence entre taux de risque de pauvreté avant et après transferts sociaux	pp
1		Contribue à l'augmentation du taux de certification nationale	Taux de certification nationale	%
1		Contribue à l'apprentissage tout au long de la vie en % de la population de 25 à 64 ans	Apprentissage tout au long de la vie en % de la population de 25 à 64 ans	%
1		Contribue à l'augmentation de la représentation du sexe sous-représenté dans les organes de prises de décision	Représentation du sexe sous-représenté dans les organes de prises de décision	%
1		Contribue à l'augmentation de la proportion des sièges détenus par les femmes au sein du parlement national	Proportion des sièges détenus par les femmes au sein du parlement national	%
1		Contribue à l'amélioration de la répartition des charges de travail domestique dans le sens d'une égalité des genres	Temps consacré au travail domestique non payé et activités bénévoles	hh:mm

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
1		Contribue à suivre l'impact du coût du logement afin de circonscrire le risque d'exclusion sociale	Indice des prix réels du logement	Indice 2015=100
2		Contribue à la réduction du taux de personnes en surpoids ou obèses	Taux de personnes en surpoids ou obèses	% de la population
2		Contribue à la réduction du nombre de nouveaux cas d'infection au HIV	Nombre de nouveaux cas d'infection au HIV	Nb de personnes
2		Contribue à la réduction de l'incidence de l'hépatite B pour 100 000 habitants	Incidence de l'hépatite B pour 100 000 habitants	Nb de cas pour 100 000 habitants
2		Contribue à la réduction du nombre de décès prématurés liés aux maladies chroniques pour 100 000 habitants	Nombre de décès prématurés liés aux maladies chroniques pour 100 000 habitants	Nb de décès pour 100 000 habitants
2		Contribue à la réduction du nombre de suicides pour 100 000 habitants	Nombre de suicides pour 100 000 habitant	Nb de suicides pour 100 000 habitants
2		Contribue à la réduction du nombre de décès liés à la consommation de psychotropes	Nombre de décès liés à la consommation de psychotropes	Nb de décès
2		Contribue à la réduction du taux de mortalité lié aux accidents de la route pour 100 000 habitants	Taux de mortalité lié aux accidents de la route pour 100 000 habitants	Nb de décès pour 100 000 habitants
2		Contribue à la réduction de la proportion de fumeurs	Proportion de fumeurs	% de la population
2		Contribue à la réduction du taux de natalité chez les adolescentes pour 1 000 adolescentes	Taux de natalité chez les adolescentes pour 1 000 adolescentes	Nb de naissance pour 1000 adolescentes
2		Contribue à la réduction du nombre d'accidents du travail	Nombre d'accidents du travail (non mortel + mortel)	Nb d'accidents
3		Contribue à l'augmentation de la part de la surface agricole utile en agriculture biologique	Part de la surface agricole utile en agriculture biologique	% de la SAU
3		Contribue à l'augmentation de la productivité de l'agriculture par heure travaillée	Productivité de l'agriculture par heure travaillée	Indice 2010=100
3		Contribue à la réduction d'exposition de la population urbaine à la pollution de l'air par les particules fines	Exposition de la population urbaine à la pollution de l'air par les particules fines	Microgrammes par m^3
3		Contribue à la réduction de production de déchets par habitant	Production de déchets par habitant	kg/hab
3		Contribue à l'augmentation du taux de recyclage des déchets municipaux	Taux de recyclage des déchets municipaux	%
3		Contribue à l'augmentation du taux de recyclage des déchets d'équipements électriques et électroniques	Taux de recyclage des déchets d'équipements électriques et électroniques	%

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
3		Contribue à la réduction de la production de déchets dangereux	Production de déchets dangereux	tonnes
3		Contribue à l'augmentation de la production de biens et services environnementaux	Production de biens et services environnementaux	millions EUR
3		Contribue à l'augmentation de l'intensité de la consommation intérieure de matière	Intensité de la consommation intérieure de matière	tonnes / millions EUR
4		Contribue à la réduction des jeunes sans emploi et ne participant ni à l'éducation ni à la formation (NEET)	Jeunes sans emploi et ne participant ni à l'éducation ni à la formation (NEET)	% de jeunes
4		Contribue à l'augmentation du pourcentage des intentions entreprenariales	Pourcentage des intentions entreprenariales	%
4		Contribue à la réduction des écarts de salaires hommes-femmes	Ecarts de salaires hommes-femmes	%
4		Contribue à l'augmentation du taux d'emploi	Taux d'emploi	% de la population
4		Contribue à la création d'emplois stables	Proportion de salariés ayant des contrats temporaires	% de l'emploi total
4		Contribue à la réduction de l'emploi à temps partiel involontaire	Emploi à temps partiel involontaire	% de l'emploi total
4		Contribue à la réduction des salariés ayant de longues heures involontaires	Salariés ayant de longues heures involontaires	% de l'emploi total
4		Contribue à la réduction du taux de chomage	Taux de chomage	% de la population active
4		Contribue à la réduction du taux de chomage longue durée	Taux de chomage longue durée	% de la population active
4		Contribue à l'augmentation du taux de croissance du PIB réel (moyenne sur 3 ans)	Taux de croissance du PIB réel (moyenne sur 3 ans)	%
4		Contribue à l'augmentation de la productivité globale des facteurs	Productivité globale des facteurs	Indice 2010=100
4		Contribue à l'augmentation de la productivité réelle du travail par heures travaillées (taux de croissance moyen sur 3 ans)	Productivité réelle du travail par heures travaillées (taux de croissance moyen sur 3 ans)	%
4		Contribue à l'augmentation de la productivité des ressources	Productivité des ressources	Indice 2000=100
4		Contribue à l'augmentation de la valeur ajoutée dans l'industrie manufacturière	Valeur ajoutée dans l'industrie manufacturière, en proportion de la valeur ajoutée totale des branches	% de la VA totale

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
4		Contribue à l'augmentation de l'emploi dans l'industrie manufacturière	Emploi dans l'industrie manufacturière, en proportion de l'emploi total	% de l'emploi
4		Contribue à la réduction des émissions de CO2 de l'industrie manufacturière	Émissions de CO2 de l'industrie manufacturière par unité de valeur ajoutée	% de la VA totale
4		Contribue à l'augmentation des dépenses intérieures brutes de R&D	Niveau des dépenses intérieures brute de R&D	% du PIB
4		Contribue à l'augmentation du nombre de chercheurs	Nombre de chercheurs pour 1000 actifs	nb pour 1000 actifs
5		Contribue à la réduction du nombre de personnes confrontées à la délinquance, à la violence ou au vandalisme dans leur quartier, en proportion de la population totale	Nombre de personnes confrontées à la délinquance, à la violence ou au vandalisme dans leur quartier, en proportion de la population totale	%
5		Contribue à la réduction du pourcentage du territoire transformé en zones artificialisées	Zones artificialisées	% du territoire
5		Contribue à l'augmentation des dépenses totales de protection environnementale	Dépenses totales de protection environnementale	millions EUR
6		Contribue à l'augmentation de l'utilisation des transports publics	Utilisation des transports publics	% des voyageurs
7		Contribue à la fertilité des sols sans nuire à la qualité des eaux de surface et/ou les eaux souterraines, de provoquer l'eutrophisation des eaux et de dégrader les écosystèmes terrestres et/ou aquatiques (unité: kg d'azote par ha SAU)?	Bilan des substances nutritives d'azote	kg d'azote par ha SAU
7		Contribue à la fertilité des sols sans nuire à la qualité des eaux de surface et/ou les eaux souterraines, de provoquer l'eutrophisation des eaux et de dégrader les écosystèmes terrestres et/ou aquatiques (unité: kg de phosphore par ha SAU)	Bilan des substances nutritives phosphorées	kg de phosphore par ha SAU
7		Contribue à une consommation durable d'une eau de robinet de qualité potable	Part des dépenses en eau dans le total des dépenses des ménages	%
7		Contribue à l'augmentation du pourcentage des masses d'eau de surface naturelles ayant atteint un état écologique "satisfaisant" et des masses d'eau souterraine ayant atteint un bon état chimique	Pourcentage des masses d'eau de surface naturelles ayant atteint un état écologique "satisfaisant" et des masses d'eau souterraine ayant atteint un bon état chimique	%
7		Contribue à l'augmentation de l'efficacité de l'usage de l'eau	Efficacité de l'usage de l'eau	m3/millions EUR
7		Contribuer à une protection des masses d'eau de surfaces et les masses d'eau souterraine par des prélèvements durables et une utilisation plus efficiente de l'eau	Indice de stress hydriques	%
7		Contribue à la préservation et/ou l'augmentation de la part de zones agricoles et forestières	Part des zones agricoles et forestières	% du territoire

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
7		Contribue à l'augmentation de la part du territoire designée comme zone protégée pour la biodiversité	Part du territoire désignée comme zone protégée pour la biodiversité	% du territoire
7		Contribue à la protection des oiseaux inscrits sur la liste rouge des espèces menacées	Nombre d'espèces sur la liste rouge des oiseaux	Nb d'espèces
7		Contribue à la lutte contre les espèces exotiques invasives inscrites sur la liste noire	Nombre de taxons sur la liste noire des plantes vasculaires	Nb de taxons
7		Contribue à la favorabilité de l'état de conservation des habitats	Etat de conservation des habitats	% favorables
8		Contribue à la réduction de l'intensité énergétique	Intensité énergétique	TJ/millions EUR
8		Contribue à la réduction de la consommation finale d'énergie	Consommation finale d'énergie	GWh
8		Contribue à l'augmentation de la part des énergies renouvelables dans la consommation finale d'énergie	Part des énergies renouvelables dans la consommation finale d'énergie	%
8		Contribue à la réduction de la part des dépenses énergétiques dans le total des dépenses des ménages	Part des dépenses énergétiques dans le total des dépenses des ménages	%
8		Contribue à la réduction du total des émissions de gaz à effet de serre	Total des émissions de gaz à effet de serre	millions tonnes CO2
8		Contribue à la réduction des émissions de gaz à effet de serre hors SEGE	Emissions de gaz à effet de serre hors SEGE	millions tonnes CO2
8		Contribue à la réduction de l'intensité des émissions de gaz à effet de serre	Intensité des émissions de gaz à effet de serre	kg CO2 / EUR
9		Contribue à l'augmentation de l'aide au développement - Education	Aide au développement - Education	millions EUR
9		Contribue à l'augmentation de l'aide au développement - Agriculture	Aide au développement - Agriculture	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide au développement - Santé de base	Aide au développement - Santé de base	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de la part des étudiants des pays en développement qui étudient au Luxembourg	Part des étudiants des pays en développement qui étudient au Luxembourg	%
9		Contribue à l'augmentation du montant des bourses d'étude	Montant des bourses d'étude	millions EUR
9		Contribue à l'augmentation de l'aide au développement - Eau et assainissement	Aide au développement - Eau et assainissement	millions EUR (prix constant 2016)

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
9		Contribue à l'augmentation de l'aide au développement - Energie	Aide au développement - Energie	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide au développement - Lois et règlements commerciaux	Aide au développement - Lois et règlements commerciaux	millions EUR (prix constant 2016)
9		Contribue à l'augmentation du montant des dépenses sociales expimé en ratio du PIB	Montant des dépenses sociales exprimé en ratio du PIB	% du PIB
9		Contribue à l'augmentation de l'aide publique nette au développement, montant alloué aux pays les moins avancés (absolu)	Aide publique nette au développement, montant alloué aux pays les moins avancés	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide publique nette au développement, montant alloué aux pays les moins avancés (en proportion du montant total d'aide au développement)	Aide publique nette au développement, montant alloué aux pays les moins avancés, en proportion du montant total d'aide au développement	%
9		Contribue à l'augmentation de l'aide au développement - Prévention et préparation aux catastrophes	Aide au développement - Prévention et préparation aux catastrophes	millions EUR (prix constant 2016)
9		Contribue à l'engagement international de 100 Mrds USD pour dépenses reliées au climat	Contribution à l'engagement international de 100 Mrds USD pour dépenses reliées au climat	millions EUR
9		Contribue à l'augmentation de l'aide au développement avec marqueur biodiversité	Aide au développement avec marqueur biodiversité	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide publique nette au développement, montant total, en proportion du revenu national brut	Aide publique nette au développement, montant total, en proportion du revenu national brut	% du RNB
9		Contribue à l'augmentation de l'aide au développement - coopération technique	Aide au développement – coopération technique	millions EUR (prix constant 2016)
9		Contribue à la réduction de la dette publique en proportion du Produit Intérieur Brut	Dette publique en proportion du Produit Intérieur Brut	% du Pib
9		Contribue à l'augmentation du montant investi dans des projets de soutien à l'enseignement supérieur	Montant investi dans des projets de soutien à l'enseignement supérieur	millions EUR (prix constant 2016)
9		Contribue à l'augmentation de l'aide publique au développement - renforcement de la société civile dans les pays partenaires	Aide publique au développement - renforcement de la société civile dans les pays partenaires	millions EUR (prix constant 2016)
10		Contribue à l'action climatique dans les pays en développement et à la protection du climat au niveau global	Contribution des CDM à la réduction des émissions de gaz à effet de serre	millions EUR
10		Contribue à l'augmentation de l'alimentation du fonds climat énergie	Fonds climat énergie	millions EUR
10		Contribue à l'augmentation de la part des taxes environnementales dans le total des taxes nationales	Part des taxes environnementales dans le total des taxes nationales	% du revenu fiscal

FICHE D'ÉVALUATION D'IMPACT
MESURES LÉGISLATIVES, RÉGLEMENTAIRES ET AUTRES

Coordonnées du projet

Intitulé du projet :	Projet de loi 1) relatif à la valorisation des données dans un environnement de confiance ; 2) relatif à la mise en œuvre du principe « once only » ; 3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ; 4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
Ministère initiateur :	Ministère de la Digitalisation
Auteur(s) :	Maximilien Spielmann Annelies Vandendriessche
Téléphone :	247-72018; 247-72126
Courriel :	maximilien.spielmann@cgpd.lu; annelies.vandendriessche@digital.etat.lu
Objectif(s) du projet :	Le présent projet de loi vise à (1) instaurer le principe "once only" selon lequel une personne fournit une seule fois des données aux entités publiques; (2) compléter la mise en application du règlement (UE) 2022/868 sur la gouvernance des données régissant la réutilisation des données du secteur public sujettes à des droits de tiers par les dispositions nationales qui s'imposent, désignant des organismes compétents, la procédure à suivre pour l'octroi des autorisations d'accès et de réutilisation des données, et les conditions applicables à l'accès et à la réutilisation des données; (3) compléter la mise en application du règlement (UE) 2016/679 en spécifiant les finalités pour lesquelles le traitement ultérieur de données à caractère personnel par les entités publiques est autorisé, sous réserve du respect des conditions prévues par le projet de loi, et ce nonobstant leur compatibilité avec les finalités initiales du traitement de données à caractère personnel, et (4) explicitant le fondement de licéité des traitements de données opérés par les entités publiques en lien avec l'exécution des missions d'intérêt public ou relevant de l'exercice de l'autorité publique leurs conférées par les dispositions applicables.

Autre(s) Ministère(s) / Organisme(s) / Commune(s) impliqué(e)(s)	Commissariat du Gouvernement à la Protection des données auprès de l'État
Date :	22/05/2024

Mieux légiférer

1 Partie(s) prenante(s) (organismes divers, citoyens,...) consultée(s) : ☒ Oui ☐ Non

Si oui, laquelle / lesquelles : Les différents ministères et les autres entités visées, notamment le Ministère de l'Économie, le Service des médias, de la connectivité et de la politique numérique (SMC), le Ministère de la Santé et de la Sécurité sociale, l'Inspection générale de la sécurité sociale, le Ministère de la Recherche et de l'Enseignement supérieur, le Centre des technologies de l'Information de l'État et le Luxembourg National Data Service (LNDS).

Remarques / Observations : Le projet de loi a été élaboré en concertation avec les acteurs susmentionnés.

2 Destinataires du projet :

- Entreprises / Professions libérales : ☒ Oui ☐ Non
- Citoyens : ☒ Oui ☐ Non
- Administrations : ☒ Oui ☐ Non

3 Le principe « Think small first » est-il respecté ? (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?) ☒ Oui ☐ Non ☐ N.a. [1]

Remarques / Observations : Le projet de loi a été rédigé dans une optique de simplification administrative et d'accélération de procédures, notamment dans le cadre du traitement ultérieur de données à caractère personnel par la même entité publique ou dans les cas d'un traitement ultérieur de données anonymisées par les entités publiques. Par ailleurs, pour les cas visés par le règlement (UE) 2022/868, le texte prévoit la possibilité d'une mise à disposition des données moyennant une redevance réduite ou à titre gratuit, notamment pour les PME, les jeunes pousses, les organisations de la société civile et les établissements d'enseignement.

[1] N.a. : non applicable.

4 Le projet est-il lisible et compréhensible pour le destinataire ? ☒ Oui ☐ Non

Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? ☒ Oui ☐ Non

Remarques / Observations : Conformément au règlement (UE) 2022/868 et au projet de loi, l'Autorité des données promeut les bonnes pratiques à travers les entités publiques, en matière de traitement ultérieur de données à caractère personnel, et à travers les organismes de droit public en matière d'accès et de réutilisation de données. Elle a également pour mission de sensibiliser les entités publiques, les organismes de droit public et le public en matière de traitement ultérieur de données à caractère personnel et en matière d'accès et de réutilisation de données.

Dans ce cadre, elle publiera des lignes directrices, qu'elle tiendra à jour de façon régulière.

5 Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? ☒ Oui ☐ Non

Remarques / Observations :

Dans un objectif de rendre plus rapides et plus efficaces les procédures pour les citoyens, les entreprises et les entités publiques, le projet de loi instaure le principe du « once only », selon lequel une personne fournit une seule fois des données aux entités publiques, au lieu de devoir le faire à plusieurs reprises. Le système « once only » constitue ainsi une vraie mesure de simplification administrative qui permettra de diminuer les dépenses et favorisera une gestion plus efficace des ressources des entités publiques.

Le règlement (UE) 2022/868 prévoit un système d'octroi ou de refus d'accès aux fins de la réutilisation des catégories de données visés à l'article 3, paragraphe 1 dudit règlement. Pour des raisons de simplification administrative et de cohérence, le projet de loi instaure une procédure d'autorisation centralisée auprès de l'Autorité des données. Afin d'éviter des contradictions ainsi qu'une complexification procédurale, les traitements ultérieurs de données à caractère personnel au sein du secteur public sont soumis à la même procédure d'autorisation. Ainsi, le projet de loi instaure une procédure uniforme pour la mise en application du règlement (UE) 2022/686 et les traitements ultérieurs de données à caractère personnel par les entités publiques.

6 Le projet contient-il une charge administrative [2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) ☐ Oui ☒ Non

Si oui, quel est le coût administratif [3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

[2] Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en œuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

[3] Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple : taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

7 a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? ☒ Oui ☐ Non ☐ N.a.

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

Le projet de loi instaure le principe du "once only" au sein du secteur public. Il favorise également le traitement ultérieur des données à caractère personnel par les entités publiques.

De ce fait, l'objectif principal de la loi est de favoriser l'échange de données interadministratif (national ou international) plutôt que de demander l'information au destinataire.

b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel [4] ? ☒ Oui ☐ Non ☐ N.a.

Si oui, de quelle(s)

Le projet de loi met en oeuvre le règlement (UE) 2022/868 relatif à la

donnée(s) et/ou administration(s) s'agit-il ?	réutilisation de données protégées détenues par les organismes du secteur public. Par ailleurs, le projet de loi prévoit, conformément au règlement (UE) 2016/679, un cadre spécifique au traitement ultérieur de données à caractère personnel par les entités publiques. Il instaure également le principe du "once only" au sein du secteur public.

[4] Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

8 Le projet prévoit-il :

- une autorisation tacite en cas de non réponse de l'administration ?	☐ Oui	☒ Non	☐ N.a.
- des délais de réponse à respecter par l'administration ?	☒ Oui	☐ Non	☐ N.a.
- le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ?	☐ Oui	☒ Non	☐ N.a.

9 Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? ☒ Oui ☐ Non ☐ N.a.

Si oui, laquelle :	La procédure d'introduction de demande prévue par le projet de loi est uniformisée pour les traitements ultérieurs de données à caractère personnel au sein des entités publiques et pour les demandes d'accès et de réutilisation des données sujettes à des droits de tiers au sens du Règlement (UE) 2022/868. La procédure prévue prend également dûment en compte les besoins de la proposition de règlement (UE) relatif à l'espace européen des données de santé.

10 En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? ☐ Oui ☐ Non ☒ N.a.

Sinon, pourquoi ?	

11 Le projet contribue-t-il en général à une :

a) simplification administrative, et/ou à une	☒ Oui	☐ Non
b) amélioration de la qualité réglementaire ?	☒ Oui	☐ Non

Remarques / Observations :	Dans un objectif de rendre plus rapides et plus efficaces les procédures pour les citoyens, les entreprises et les entités publiques, le projet de loi instaure le principe du « once only », selon lequel une personne fournit une seule fois des données aux entités publiques au lieu de devoir le faire à plusieurs reprises. Le système « once only » constitue ainsi une vraie mesure de simplification administrative qui permettra de diminuer les dépenses et favorisera une gestion efficace des ressources publiques. Dans la même logique, il explicite le fondement de licéité des traitements de données à caractère personnel opérés par les entités publiques en lien avec l'exécution des missions d'intérêt public leurs conférées par les dispositions applicables. En outre, le projet de loi met en oeuvre le règlement (UE) 2022/868 relatif à la réutilisation de données protégées détenues par les organismes du secteur public. Dans une optique de gestion efficiente des données par les entités publiques dans le respect de la protection des données, le projet de loi vise

	également à faciliter la mise en œuvre de traitements ultérieurs de données au sein du secteur public, en spécifiant les conditions qui y sont applicables. Afin d'éviter des contradictions ainsi qu'une complexification procédurale, les traitements ultérieurs de données à caractère personnel au sein du secteur public sont soumis à la même procédure d'autorisation que les réutilisations de données visées par le règlement (UE) 2022/686.			
12	Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ?	☐ Oui	☐ Non	☒ N.a.
13	Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office)	☒ Oui	☐ Non	
	Si oui, quel est le délai pour disposer du nouveau système ?	Le système informatique doit être opérationnel au jour de l'entrée en vigueur de la loi.		
14	Y a-t-il un besoin en formation du personnel de l'administration concernée ?	☒ Oui	☐ Non	☐ N.a.
	Si oui, lequel ?	Le personnel de l'Autorité des données doit entretenir ses connaissances spécialisées relatives à la réutilisation des données détenues par les organismes du secteur public. A noter que cette formation du personnel du Commissariat du gouvernement à la protection des données auprès de l'Etat constitue la suite logique de l'entrentien des connaissances spécialisées en matière de protection des données conformément au règlement (UE) 2026/679.		
	Remarques / Observations :			

Egalité des chances

15 Le projet est-il :

- principalement centré sur l'égalité des femmes et des hommes ? ☐ Oui ☒ Non
- positif en matière d'égalité des femmes et des hommes ? ☐ Oui ☒ Non

Si oui, expliquez de quelle manière :

- neutre en matière d'égalité des femmes et des hommes ? ☒ Oui ☐ Non

Si oui, expliquez pourquoi :

- négatif en matière d'égalité des femmes et des hommes ? ☐ Oui ☒ Non

Si oui, expliquez de quelle manière :

16 Y a-t-il un impact financier différent sur les femmes et les hommes ? ☐ Oui ☐ Non ☒ N.a.

Si oui, expliquez de quelle manière :

Directive « services »

17 Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation [5] ? ☐ Oui ☐ Non ☒ N.a.

Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march___int__rieur/Services/index.html

[5] Article 15 paragraphe 2 de la directive « services » (cf. Note explicative, p.10-11)

18 Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers [6] ? ☐ Oui ☐ Non ☒ N.a.

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march___int__rieur/Services/index.html

[6] Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p.10-11)

Impression: CTIE – Division Imprimés et Fournitures de bureau

20250514_Avis

Nº 8395[1]

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AVIS DE LA CHAMBRE DES FONCTIONNAIRES ET EMPLOYES PUBLICS

(21.10.2024)

Par deux dépêches du 12 juin 2024, Madame la Ministre de la Digitalisation a demandé l'avis de la Chambre des fonctionnaires et employés publics sur les projets de loi et de règlement grand-ducal spécifiés à l'intitulé.

Le projet de loi introduit plusieurs mesures dans le domaine de la gestion des données à caractère personnel par les entités publiques conformément aux règlements (UE) 2016/679 et 2022/868, à savoir, entre autres, la fixation des conditions et modalités de traitement, de réutilisation et de traitement ultérieur des données dans le cadre de l'exécution d'une mission d'intérêt public ainsi que la définition des autorités et acteurs publics compétents intervenant dans ce cadre et de leurs attributions.

Le texte introduit par ailleurs dans ce contexte le principe « *once only* », selon lequel les administrés transmettent leurs données une seule fois à une autorité dans le cadre d'une démarche administrative, sans devoir fournir ces mêmes données de nouveau pour chaque nouvelle démarche par après, que ce soit auprès de la même autorité ou auprès d'une autre autorité.

Le projet de règlement grand-ducal détermine la composition et le fonctionnement du Conseil consultatif de la valorisation des données dans un environnement de confiance, organe qui aura pour mission de conseiller le Commissariat du gouvernement à la protection des données auprès de l'État et d'émettre des avis sur les questions en relation avec le traitement et la réutilisation des données à caractère personnel dans le cadre de la future loi y relative.

La Chambre des fonctionnaires et employés publics constate que le texte du projet de loi est particulièrement technique et indigeste. Si elle comprend que le domaine y couvert nécessite des règles spécifiques, elle met en garde contre une surrégulation au détriment des administrations et des administrés. Ce dernier phénomène est malheureusement à la mode depuis des années, y compris en matière de protection des données. Sous le prétexte de devoir agir dans l'intérêt général, la sécurité publique, la lutte contre le terrorisme ou la criminalité financière, la transparence et la protection des données,

les administrations et les particuliers sont noyés au quotidien sous des règles et procédures lourdes, ennuyeuses et inutiles (formulaires, déclarations et demandes à remplir, obligation de donner en permanence lors d'échanges quelconques de données l'accord ou le désaccord pour le traitement de celles-ci, etc.), qui pourraient parfaitement être évitées, mais qui sont malheureusement imposées de plus en plus souvent par les bureaucrates de l'Union européenne.

Il est d'ailleurs paradoxal que l'objectif affiché à l'exposé des motifs joint au projet de loi est de faire « *économiser beaucoup de temps, de ressources et d'argent à tous les acteurs concernés, qu'il s'agisse des citoyens et des entreprises ou de l'administration publique* », tandis que ledit projet introduit une panoplie de nouvelles règles et procédures complexes à mettre en œuvre, qui nécessitent un investissement considérable en temps, ressources et argent auprès des entités publiques.

Les administrations seront submergées d'obligations en vertu du texte projeté et de la réglementation européenne y liée, de telle sorte que même les spécialistes en la matière risquent de se perdre dans ce labyrinthe législatif.

Selon la dernière phrase de l'exposé des motifs accompagnant le projet de loi, « *toutes les propositions* (prévues par le projet) *ont été élaborées en concertation étroite avec les acteurs concernés* ».

Cette affirmation prête à confusion. En effet, les mesures prévues par le projet de loi ont une envergure énorme, touchant toutes les administrations, les communes, les établissements publics, etc. La Chambre doute que les mesures projetées aient été élaborées de concert avec toutes les entités qui seront concernées par celles-ci. La fiche d'évaluation d'impact annexé au projet de loi ne mentionne d'ailleurs qu'une demi-douzaine d'organismes qui ont été consultés en amont. Au vu des maintes dispositions sur la protection des données à caractère personnel que comprend le dossier sous examen, la Chambre s'étonne que la Commission nationale pour la protection des données ne figure pas parmi les organismes consultés.

Si la Chambre ne nie pas que l'application du principe « *once only* » est certainement une bonne chose pour les administrés en faisant économiser à ceux-ci beaucoup de temps, ce qu'elle approuve, elle craint néanmoins que cette application ne mène pas du tout à une simplification administrative pour les entités publiques, contrairement à ce qu'énonce l'exposé des motifs joint au projet de loi, selon lequel le système « *once only* » constitue « *une vraie mesure de simplification administrative* ».

Les mesures projetées ne doivent pas conduire à un ralentissement des procédures. Si, à travers les procédures prévues, les entités publiques prenaient plus de temps à obtenir les données nécessaires pour le traitement d'un dossier auprès d'une autre entité qu'auprès de l'administré, au détriment de ce dernier, l'application obligatoire du principe « *once only* » telle que prévue par le projet de loi sous avis ne ferait aucun sens. Or, au vu des règles complexes projetées et de l'obligation du système « *once only* », il est à craindre que le traitement de nombreux dossiers soit bloqué, du moins dans un premier temps.

En effet, à l'heure actuelle, les infrastructures et les procédures auprès des maintes entités publiques visées par le texte ne sont pas prêtes pour appliquer tout de suite le principe en question selon les mécanismes envisagés. L'échange de données devra fonctionner sans lourdeurs administratives. La Chambre doute cependant que tel soit le cas, d'autant plus que le système d'échange projeté devra être mis en œuvre non seulement auprès des administrations de l'État, mais aussi auprès des communes et des établissements publics notamment, entités qui sont organisées et qui fonctionnement toutes de manière totalement différente.

Le projet de loi ne prévoit d'ailleurs ni de délai ni de période transitoire pour la mise en conformité de leurs infrastructures et procédures par les entités publiques et pour la préparation de l'application obligatoire du principe « *once only* », ce qui crée une situation d'insécurité juridique.

Pour l'échange des données entre diverses entités publiques concernant une demande leur soumise par un administré, celles-ci doivent à chaque fois, « *pour chaque type d'échange d'informations et de données à caractère personnel* », élaborer et signer un protocole spécifique. En cas de changement d'un élément lié à l'échange en question, un nouveau document doit être signé. Le projet de loi sous avis comporte plein d'obligations dans ce sens. La Chambre se demande en quoi toutes ces procédures sont en phase avec la simplification administrative.

S'y ajoute que des procédures – qui ne sont pas encore définies – doivent être mises en place pour informer constamment les administrés sur l'état d'avancement de leurs dossiers et pour les avertir, voire requérir leur accord, sur la réutilisation de leurs données. Ces démarches, sans doute nécessaires

entre autres dans un souci de transparence et pour éviter des abus, utilisent des ressources et créent des charges de travail supplémentaires pour les entités publiques.

D'après l'exposé des motifs joint au projet de loi, le système « *once only* » favorisera une gestion plus efficace des ressources des entités publiques. La Chambre fait remarquer que l'application dudit système ne doit pas avoir un impact négatif sur le personnel des administrations. Le dossier omet de préciser comment le gouvernement entend concrètement faire face aux charges supplémentaires des administrations à travers le recrutement de personnel.

Concernant les administrés, ceux-ci seront aussi soumis à des procédures complémentaires, puisqu'ils devront certainement signer lors de leur première démarche administrative une paperasserie, incompréhensible pour le commun des mortels, par laquelle ils donnent leur accord pour le traitement de leurs données à caractère personnel.

Dans ce contexte, la Chambre relève en outre qu'il ne faut pas oublier à assurer l'accompagnement des personnes ayant des difficultés à se familiariser avec le monde numérique. La possibilité de recourir à des échanges traditionnels et non digitaux doit être conservée.

Selon le projet de loi, le recours au système « *once only* » est une obligation pour les entités publiques y visées. Si cette obligation fait du sens pour les procédures liées entre elles dans le cadre d'un dossier unique (comme par exemple dans les domaines de la construction et du logement, où différentes entités publiques interviennent dans un même dossier pour émettre certaines autorisations), tel n'est pas le cas de l'avis de la Chambre pour les démarches administratives qui n'ont aucun lien entre elles. Il faudra veiller à ne pas rendre excessivement compliquées les démarches administratives, tant pour les administrés que pour les administrations.

Le projet de loi prévoit par ailleurs la possibilité de transmettre à des personnes tierces les données à caractère personnel des administrés détenues par les entités publiques, ceci sans l'accord des administrés concernés. La Chambre relève que les administrés doivent en tout cas être informés sur la transmission de leurs données et avoir les moyens de s'y opposer dans la mesure où cela est possible.

De l'avis de la Chambre, la mise en place du principe « *once only* » mènera au final à une simplification des démarches pour les administrés, mais elle renforcera au contraire la charge administrative pour le personnel de l'ensemble des administrations et services publics, étatiques et communaux, au vu des nombreuses procédures et règles nouvelles qui seront introduites et de la responsabilité supplémentaire qui en découle. Du point de vue de la protection des intérêts de ses ressortissants, la Chambre est donc plutôt hésitante face au système projeté.

Pour le reste, la Chambre des fonctionnaires et employés publics s'abstient d'examiner plus en détail les dispositions techniques prévues par les deux textes lui soumis pour avis et elle ne peut y marquer son accord que sous la réserve expresse des observations qui précèdent.

Ainsi délibéré en séance plénière le 21 octobre 2024.

Le Directeur, — *Le Président,*

G. TRAUFFLER — R. WOLFF

Impression: CTIE – Division Imprimés et Fournitures de bureau

20250514_Avis_2

N° 8395[2]

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AVIS DE LA CHAMBRE DES SALARIES

(23.10.2024)

Par lettres du 12 juin 2024, Madame Stéphanie Obertin, ministre de la Digitalisation a soumis le projet de loi et le projet de règlement grand-ducal sous rubrique à l'avis de la Chambre des salariés (CSL).

1. Le présent projet a pour objet de compléter le règlement (UE) 2022/868 sur la gouvernance des données (Data Governance Act,ci-après aussi AGD) qui a pour objectif d'instaurer la confiance entre les citoyens et les acteurs impliqués dans l'accès et la réutilisation des données, en particulier en concevant des mécanismes appropriés permettant le respect des droits individuels dans le contexte de l'accès et de la réutilisation des données à caractère personnel et à caractère non personnel détenues par les organismes du secteur public.

2. Le règlement (UE) 2022/868 est applicable depuis le 24 septembre 2023 et il détermine la majorité des dispositions de fond.

Résumé du règlement (UE) 2022/868[1]

Il vise à rendre davantage de données disponibles pour la réutilisation et à faciliter le partage des données dans des domaines tels que la santé, l'environnement, l'énergie, l'agriculture, la mobilité, la finance, l'industrie manufacturière, l'administration publique et les compétences, au profit des citoyens et des entreprises, en créant des emplois et en stimulant l'innovation.

Le règlement européen énonce :

– *les **conditions de réutilisation de certaines données protégées** détenues par des organismes du secteur public ;*

1 Source : https://eur-lex.europa.eu/FR/legal-content/summary/european-data-governance.html

– *des **règles** pour les entreprises fournissant des services d'intermédiation de données ;*
– ***un cadre pour l'altruisme en matière de données** (le partage des données de manière volontaire et sans contrepartie) ;*
– ***un cadre pour le Comité européen de l'innovation dans le domaine des données (EDIB)** ; et*
– *des mesures permettant le **flux sécurisé de données à caractère non personnel** en dehors de l'UE.*

Réutilisation de certaines catégories de données publiques

Les organismes du secteur public détiennent de grandes quantités de données protégées par les droits de tiers (tels que les secrets commerciaux, les données personnelles ou la propriété intellectuelle) qui ne peuvent pas être utilisées en tant que données ouvertes, mais qui pourraient être réutilisées en vertu de règles européennes ou nationales spécifiques. Lorsqu'une telle réutilisation est autorisée, les organismes du secteur public devront respecter les conditions de réutilisation fixées par l'AGD. Les conditions de réutilisation doivent être non discriminatoires, transparentes, proportionnées, justifiées et rendues publiques.

Transfert de données vers des pays tiers

Un réutilisateur ayant l'intention de transférer des données protégées et à caractère non personnel vers un pays tiers devra se conformer aux règles spécifiques de l'AGD.

Redevances

Les redevances de réutilisation que les Etats membres peuvent fixer, doivent être transparentes, proportionnées, non discriminatoires et objectivement justifiées. Les organismes du secteur public qui accordent des permis de réutilisation peuvent appliquer des frais réduits ou nuls, par exemple pour les petites et moyennes entreprises, les jeunes entreprises, les organisations de la société civile et les établissements d'enseignement.

Point d'information unique

Pour garantir que les données puissent être trouvées («trouvabilité»), les États membres de l'UE devront veiller à ce que toutes les informations pertinentes sur les conditions de réutilisation et sur les redevances soient disponibles et facilement accessibles via un point d'information unique. La Commission européenne rassemblera à son tour ces informations sur data.europa.eu.

Services d'intermédiation de données

L'AGD réglemente en outre les fournisseurs de services d'intermédiation de données, qui sont des tiers neutres qui mettent en relation les personnes et les entreprises qui détiennent des données avec d'autres qui souhaitent les utiliser. Les exigences relatives à ces services visent à garantir que ces intermédiaires de données fonctionneront comme des organisateurs dignes de confiance du partage des données. Afin de renforcer la confiance dans le partage des données, cette approche établit un modèle basé sur la neutralité et la transparence des intermédiaires de données tout en donnant aux personnes et aux entreprises le contrôle de leurs données.

Les entités souhaitant fournir des services d'intermédiation de données doivent :

– *respecter des exigences strictes pour garantir la neutralité et éviter les conflits d'intérêts ;*
– *être structurellement séparées de tout autre service à valeur ajoutée fourni ;*
– *avoir des conditions tarifaires indépendantes du fait que le détenteur de données * ou l'utilisateur de données* potentiel utilise d'autres services; et*
– *s'enregistrer auprès d'une autorité compétente.*

Altruisme en matière de données

Il y a altruisme en matière de données lorsque des personnes et des entreprises donnent leur consentement ou leur autorisation pour mettre à disposition les données qu'elles génèrent en vue de leur utilisation dans l'intérêt public, volontairement et sans contrepartie. Ces données ont un énorme potentiel pour faire avancer la recherche et développer de meilleurs produits et services, notamment dans les domaines de la santé, de l'action climatique et de la mobilité. Les États membres peuvent développer des politiques nationales pour encourager l'altruisme en matière de données,

et une entité engagée dans l'altruisme en matière de données peut demander à être enregistrée comme «organisation altruiste en matière de données reconnue dans l'Union». La Commission tiendra un registre de ces organisations au niveau de l'UE.

Comité européen de l'innovation dans le domaine des données

La Commission mettra en place l'EDIB, qui sera composé de représentants :

- *des autorités nationales désignées dans le cadre de l'AGD ;*
- *du Comité européen de la protection des données;*
- *du Contrôleur européen de la protection des données;*
- *de l'Agence de l'Union européenne pour la cybersécurité;*
- *du Représentant de l'UE pour les PME; et*
- *d'autres secteurs et organismes spécifiques disposant d'une expertise particulière.*

Les tâches de l'EDIB consistent notamment à conseiller et à assister la Commission dans les domaines suivants :

- *le développement d'une pratique cohérente dans le traitement des demandes de réutilisation des données ;*
- *l'amélioration de l'interopérabilité des données et des services de partage de données ;*
- *le développement d'une pratique cohérente des autorités compétentes dans la mise en vigueur des exigences applicables aux prestataires de services d'intermédiation de données*.*

Flux de données internationaux

Les données à caractère non personnel pouvant avoir une valeur économique considérable, l'AGD introduit des garanties pour protéger ces données contre tout accès illicite par les autorités des pays tiers.

3. Au niveau national les conditions applicables à l'accès et à la réutilisation des données détenues par les organismes du secteur public doivent être précisées.

Ces conditions doivent être non discriminatoires, transparentes, proportionnées et objectivement justifiées en ce qui concerne les catégories de données et les finalités de la réutilisation, ainsi que la nature des données pour lesquelles la réutilisation est autorisée.

Le présent projet de loi, qui doit ainsi se lire conjointement avec le règlement (UE) 2022/868, complète par conséquent ce cadre européen par les dispositions nationales qui s'imposent, en particulier concernant :

- la désignation des organismes compétents,
- la procédure à suivre pour l'octroi des autorisations d'accès et de réutilisation des données, et
- les conditions applicables à l'accès et à la réutilisation des données.

4. Le **Commissariat du gouvernement à la protection des données auprès de l'État** est désigné comme **« Autorité des données »** centralisée conformément au règlement (UE) 2022/868.

Il sera l'organisme compétent pour octroyer ou refuser les accès et les réutilisations des données détenues par les organismes du secteur public.

L'Autorité des données doit collaborer étroitement avec le Centre des technologies de l'information de l'État, dénommé ci-après par le terme « Centre », le tiers de confiance mandaté par le Centre et le groupement d'intérêt économique PNED G.I.E. – Plateforme nationale d'échange de données, désigné ci-après par le terme « LNDS ».

Elle doit fonctionner comme organe de réflexion et d'impulsion dans le domaine du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation de données et de formuler des avis et des propositions en la matière au ministre ayant la digitalisation dans ses attributions.

5. Le **Centre des technologies de l'information de l'État et le « Luxembourg National Data Service »** sont désignés organismes compétents conformément au règlement (UE) 2022/868 pour aider l'Autorité des données dans l'exercice des missions d'octroyer et de refuser les accès et les réutilisations. En outre, ils ont pour mission de mettre en œuvre les mesures imposées par le règlement (UE) 2022/868 et la loi.

Le Centre a ainsi notamment pour missions :

– de mettre à disposition un environnement de traitement sécurisé tel p.ex. restreindre le nombre de personnes pouvant accéder aux données, tenir un registre des accès etc.
– de fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles ;
– de s'assurer de la mise en œuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou à de modification, d'agrégation, de suppression et de traitement des informations et données.

Le **LNDS** a notamment pour missions :

– d'aider les organismes du secteur public à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données ;
– de fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur.

Le Centre et le LNDS veillent notamment à ce que leur personnel soit fonctionnellement indépendant des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données. Ils doivent désigner leur personnel sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel. Ils doivent aussi veiller à ce que ce personnel n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui leurs sont conférés par la future loi. Il est interdit au personnel du Centre et du LNDS chargé de l'exécution des missions qui leurs sont conférées par la future loi d'avoir un intérêt quelconque, par lui-même ou par personne interposée, et sous quelque forme juridique que ce soit, dans une entité publique, dans un organisme du secteur public détenant les données ou dans un réutilisateur de données.

6. Pour éviter d'éventuels conflits d'intérêts et pour maintenir la confiance des citoyens dans une gestion prudente de leurs données par les acteurs publics, la loi prévoit la possibilité pour le Centre des technologies de l'information de l'État de recourir aux services d'un **tiers de confiance** qui doit être une **entité fonctionnellement indépendante des entités publiques, des organismes du secteur public détenant les données et du réutilisateur de données.**

Le tiers de confiance a notamment pour missions

– d'effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données ;
– de collaborer étroitement avec l'Autorité des données, le Centre et le LNDS.

Le tiers de confiance doit disposer de ressources humaines et techniques suffisantes et de l'expertise adéquate pour s'acquitter efficacement des missions dont il est chargé.

Il ne doit divulguer aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données, ou susceptible de porter préjudice aux droits à la protection des données, à la propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique.

Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation.

Son personnel doit être désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement.

Ce personnel ne doit pas être chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données. Et ce personnel ne doit exercer aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui lui sont conférés.

Il est interdit au personnel du tiers de confiance chargé de l'exécution des missions conférées à ce dernier par la future loi d'avoir un intérêt quelconque, par lui-même ou par personne interposée, et sous quelque forme juridique que ce soit, dans une entité publique, dans un organisme du secteur public détenant les données ou dans un réutilisateur de données.

7. En complément du règlement (UE) 2022/868, et afin de faciliter la mise en œuvre de traitements ultérieurs de données dans le secteur public, le projet de loi énonce les **finalités pour lesquelles le traitement ultérieur de données à caractère personnel est autorisé** et précise que les traitements de données opérés par les **entités publiques en lien avec l'exécution des missions d'intérêt public** ou relevant de l'exercice de l'autorité publique leurs conférées sont fondés sur **l'article 6, paragraphes 1, point e) et 3 du règlement (UE) 2016/679.**

Ainsi les entités publiques sont habilitées à traiter les données à caractère personnel nécessaires aux fins relevant de l'exécution de leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies par une disposition de droit de l'Union européenne ou de droit national applicable.

Selon le projet de loi, est une **« entité publique »** : un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal.

La CSL regrette que le règlement grand-ducal ne soit pas encore disponible afin de pouvoir être analysé en même temps que le projet de loi.

8. Sous l'autorité du ministre ayant la digitalisation dans ses attributions est instauré un **point d'information unique** conformément à l'article 8 du règlement (UE) 2022/868.

Le point d'information unique a pour missions :

– de recevoir les demandes d'accès et de réutilisation de données, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et d'assurer les échanges et les démarches nécessaires;
– de rendre disponibles au public toutes les informations pertinentes concernant la mise à disposition des données par les entités publiques (en application des articles 5 et 6 du règlement (UE) 2022/868) ainsi que toute autre information dont la publication est sollicitée par l'Autorité des données ;
– de mettre à disposition par voie électronique une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

9. Il est en outre institué, sous l'autorité du ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions, un **Conseil consultatif de la valorisation des données dans un environnement de confiance, appelé le « Conseil consultatif** ».

Il a pour mission :

– de fonctionner comme organe consultatif de l'Autorité des données ;
– de soumettre un avis motivé dans les cas où ce dernier est sollicité ;
– de se prononcer sur toute question en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données qui lui est soumise par le ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions ;
– de promouvoir l'accès et la réutilisation des données.

Le Conseil consultatif est composé de représentants issus des ministères et administrations de l'État. Un règlement grand-ducal précise la composition et le mode de fonctionnement du Conseil consultatif.

10. Dans un objectif de rendre plus rapides et plus efficaces les procédures pour les citoyens et les entreprises, le projet de loi instaure également le **principe du « once only »**, qui constitue une priorité du Gouvernement, et selon lequel **une personne fournit une seule fois des données aux autorités, au lieu de devoir le faire à plusieurs reprises.**

Le système proposé a pour but de faire économiser du temps, des ressources et de l'argent à tous les acteurs concernés, qu'il s'agisse des citoyens, des entreprises ou de l'administration publique.

Le système « once only » constitue ainsi selon les auteurs du projet, une vraie mesure de simplification administrative qui permettra de diminuer les dépenses et favorisera une gestion plus efficace des ressources des entités publiques.

Ce principe du « once only » impliquera qu'un administré présentant une demande ou produisant une déclaration à une entité publique ne peut être tenu de produire des informations ou des données à caractère personnel que celle-ci détient déjà ou qu'elle peut obtenir auprès d'une autre entité publique.

Les entités publiques échangent entre elles toutes les informations ou les données à caractère personnel nécessaires pour traiter une demande présentée par l'administré ou une déclaration présentée par celui-ci en application d'une disposition législative ou réglementaire. Elles échangent aussi entre elles les informations ou les données à caractère personnel nécessaires pour pouvoir informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévu par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

Lorsque les informations ou données à caractère personnel nécessaires pour traiter la demande présentée par l'administré ou la déclaration présentée par celui-ci doivent être obtenues auprès d'une autre entité publique, l'administré certifie l'exactitude des informations et des données à caractère personnel ainsi obtenues.

Dans les cas où les informations et les données à caractère personnel s'avèrent inexactes, l'administré est tenu de demander leur rectification auprès de l'entité publique d'où elles proviennent et de communiquer les informations et les données à caractère personnel rectifiées à l'entité publique en charge du traitement de la demande ou de la déclaration présentée par l'administré.

L'entité publique ne sollicite pas l'échange d'informations et de données à caractère personnel auprès d'une autre entité publique s'il est manifeste qu'elle n'est pas compétente pour traiter la demande de l'administré.

L'entité publique chargée de traiter la demande ou la déclaration fait connaître à l'administré les informations ou les données à caractère personnel nécessaires au traitement de la demande ou de la déclaration qu'elle se procure auprès d'autres entités publiques. L'information contient, pour chaque catégorie d'informations et de données à caractère personnel, les coordonnées des entités publiques d'où proviennent les informations et les données à caractère personnel.

Les informations et les données à caractère personnel collectées et échangées ne peuvent être utilisées ultérieurement à des fins de détection systématique d'une fraude. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à procéder auxdites détections et ce pour les détections sur lesquelles porte cette habilitation.

C'est au plus tard au moment de la première communication individuelle avec l'administré, que celui-ci est avisé de son droit de s'opposer à la poursuite du traitement des données à caractère personnel. En cas d'opposition exprimée par l'administré de poursuivre le traitement, les informations et les données à caractère personnel obtenues à la suite de cet échange sont détruites sans délai.

Les entités publiques destinataires des informations et des données à caractère personnel ne peuvent se voir opposer le secret professionnel dès lors qu'elles sont, dans le cadre de leurs missions légales, habilitées à avoir connaissance des informations ou des données à caractère personnel ainsi échangées.

Le projet de loi prévoit qu'un règlement grand-ducal détermine les informations ou données à caractère personnel, qui en raison de leur nature, ne peuvent faire l'objet de ces échanges entre entités publiques.

La CSL constate et regrette que ce projet de règlement grand-ducal fait malheureusement encore défaut.

Les entités publiques sont tenues d'identifier, dans les meilleurs délais, les informations et données à caractère personnel qu'elles peuvent obtenir auprès d'une autre entité publique :

– dans le cadre du traitement effectué dans l'exercice de leurs missions des demandes et déclarations présentées par un administré ;

– pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

Les entités publiques notifient, sans délai, les échanges d'informations et de données à caractère personnel identifiées conformément au paragraphe précédent aux entités publiques auprès desquelles les informations et données à caractère personnel pourraient être obtenues.

Dans un délai d'un mois à partir de la notification visée à l'alinéa qui précède, les entités publiques notifiées :

– certifient la disponibilité des informations et des données à caractère personnel à l'entité publique demanderesse et confirment que l'échange d'informations et de données à caractère personnel n'est pas impossible
– ou informent l'entité publique demanderesse du fait qu'elles ne détiennent pas les informations et les données à caractère personnel sollicitées ou que l'échange d'informations et de données à caractère personnel est impossible.

Une copie de l'information visée ci-avant est transmise au ministre ayant la digitalisation dans ses attributions.

11. Chaque type d'échange d'informations et de données à caractère personnel est formalisé dans un **protocole signé entre les entités publiques concernées préalablement à l'échange des informations et des données à caractère personnel**.

Le protocole contient, au moins, les éléments suivants :

1° 1° les coordonnées des entités publiques d'où proviennent les informations et les données à caractère personnel et des entités publiques destinataires des informations et les données à caractère personnel ;

2° 2° une description détaillée du contexte du traitement des informations et des données à caractère personnel ainsi que les motifs pour lesquels les informations et les données à caractère personnel sont nécessaires pour le respect des obligations ;

3° 3° une description détaillée des catégories d'informations et de données à caractère personnel visées par l'échange à l'entité publique destinataire ;

4° 4° une description détaillée des catégories de personnes concernées ;

5° 5° une description détaillée des finalités du traitement ;

6° 6° le cas échéant, l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers et les pays tiers à destination desquels des transferts de données à caractère personnel sont envisagés ainsi que l'existence ou l'absence de garanties appropriées conformément au chapitre V du règlement (UE) 2016/679 ;

7° 7° les motifs pour lesquels les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies.

Tout changement des éléments liés à l'obtention des informations et des données à caractère personnel auprès d'une entité publique doit être formalisé par avenant du protocole.

Le protocole ainsi que tout avenant sont transmis sans délai à l'Autorité des données qui les publie par voie électronique pour une durée de 2 ans. Les entités publiques informent sans délai l'Autorité des données lorsqu'un protocole n'est plus applicable.

12. L'Autorité des données tient un **registre de tous les protocoles** qui lui sont transmis pour publication.

13. Le **traitement ultérieur de données à caractère personnel** par des entités publiques est autorisé si le traitement des données à caractère personnel est effectué exclusivement pour une ou plusieurs des finalités suivantes :

– **l'analyse statistique ;**
– **les activités d'éducation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;**
– **la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;**

– **l'évaluation et la planification des politiques envisagées ou planifiées par le Gouvernement et approuvées par décision du Gouvernement en conseil, ou en ce qui concerne les communes, envisagées ou planifiées par le Conseil communal ;**
– **lorsque la mise en œuvre d'un accord international requiert la communication d'informations ou lorsque le traitement ultérieur des données à caractère personnel permet de répondre aux demandes d'informations officielles provenant de gouvernements étrangers ou d'organisations internationales approuvées par décision du Gouvernement en conseil ;**
– **les activités de développement, d'évaluation, de démonstration, de sécurité et d'innovation de dispositifs ou de services ;**
– **la formation, le test et l'évaluation d'algorithmes, y compris dans les dispositifs, les systèmes d'intelligence artificielle et les applications numériques.**

Le traitement ultérieur des données à caractère personnel, y compris leur partage et leur mise à disposition, par les entités publiques doit en outre être licite au sens de l'article 6, paragraphe 1er, lettre e) (mission d'intérêt public) et, si applicable, de l'article 9 (données sensibles), paragraphe 2, lettre g) (mission d'intérêt public) ou j) (santé publique) du règlement (UE) 2016/679.

14. Les données à caractère personnel détenues par des entités publiques doivent être **anonymisées préalablement à leur traitement ultérieur** aux fins énoncées ci-avant.

Lorsque le traitement de données anonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel doivent être **pseudonymisées préalablement à leur traitement ultérieur.**

Et lorsque le traitement ultérieur de données à caractère personnel pseudonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel peuvent être traitées ultérieurement de manière nonpseudonymisées dans les limites du strict nécessaire.

15. Le **point d'information unique met à disposition par voie électronique une liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles en vue de leur traitement ultérieur**, avec des informations pertinentes décrivant les données à caractère personnel disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur traitement ultérieur.

16. L'**accès et la réutilisation, par un réutilisateur, des données détenues par des organismes du secteur public, vise,** conformément au règlement (UE) 2022/868, les **données qui sont protégées pour des motifs :**

1° de confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise ;

2° de secret statistique ;

3° de protection des droits de propriété intellectuelle de tiers ; ou

4° de protection des données à caractère personnel.

L'accès et la réutilisation des données par des réutilisateurs sont autorisés si l'accès et la réutilisation des données est effectué exclusivement pour une ou plusieurs des **finalités suivantes** :

– **l'analyse statistique ;**
– **les activités d'éducation, de formation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;**
– **la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;**
– **le développement, l'évaluation, la démonstration, la sécurité et l'innovation de technologies ;**
– **le développement, l'évaluation, la démonstration, la sécurité et l'innovation de produits ;**
– **l'évaluation des politiques publiques luxembourgeoises ou européennes**

17. Le projet de loi précise également les conditions endéans lesquelles la réutilisation est possible. Ainsi les données à caractère personnel détenues par des organismes du secteur public doivent notamment être **anonymisées, sinon pseudonymisées,** préalablement à l'accès et à la réutilisation par le réutilisateur de données.

18. La réutilisation de données nécessite en outre l'**accord de l'Autorité des données**.

Les demandes de traitement ultérieur de données à caractère personnel ainsi que les demandes d'accès et de réutilisation à présenter à l'Autorité des données doivent être formulées de façon précise et revêtir une **forme écrite**. Le projet de loi précise les informations qui doivent être fournies par le demandeur dans sa demande.

L'Autorité des données statue ensuite dans un délai de 2 mois à compter du dépôt de la demande.

19. L'Autorité des données tient un **registre public des traitements ultérieurs de données à caractère personnel et des accès et réutilisations de données autorisées**.

20. En ce qui concerne les **services d'intermédiation de données** (Chapitre III du règlement (UE) 2022/868), la **Commission nationale pour la protection des données (CNPD)** est l'autorité compétente pour effectuer les tâches liées à la procédure de notification, telle que visée à l'article 13 du règlement (UE) 2022/868. Un règlement interne de la CNPD définira la procédure en matière de notification pour les services d'intermédiation de données.

La CNPD pourra imposer des **redevances proportionnées et objectives** pour la notification des services d'intermédiation. Un règlement de la CNPD déterminera le montant et les modalités de paiement de ces redevances.

Dans le cadre d'une violation de l'obligation de notification incombant aux prestataires de services d'intermédiation de données ou des conditions liées à la fourniture de services d'intermédiation de données, la CNPD peut, par voie de décision, imposer des amendes administratives à hauteur de 500 à 100.000 euros aux prestataires de services d'intermédiation de données.

La CNPD pourra aussi infliger au prestataire de services d'intermédiation de données des astreintes jusqu'à concurrence de 250 euros par jour de retard à compter de la date qu'elle fixe dans sa décision, pour le contraindre à communiquer toute information demandée par la CNPD ou à respecter une demande de cessation prononcée.

21. La CNPD est en outre l'autorité responsable du **registre public national des organisations altruistes en matière de données** reconnues, tel que visé à l'article 23 du règlement (UE) 2022/868.

22. Un **projet de règlement grand-ducal** complète le projet de loi. Il prévoit la composition, le mode de fonctionnement et les attributions du Conseil consultatif de la valorisation des données dans un environnement de confiance et il précise les règles relatives au calcul et à la perception des redevances lesquelles ne doivent pas dépasser le montant des coûts réels liés au mécanisme de réutilisation des données.

*

23. **La CSL marque son accord au présent projet de loi et de règlement grand-ducal.**

Luxembourg, le 23 octobre 2024

Pour la Chambre des salariés,

Le Directeur,
Sylvain HOFFMANN

La Présidente,
Nora BACK

Impression: CTIE – Division Imprimés et Fournitures de bureau

20250514_Avis_4

N° 8395[3]

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AVIS DE L'ORDRE DES ARCHITECTES ET DES INGENIEURS-CONSEILS

(28.10.2024)

SOMMAIRE

*

1. CONSIDERATIONS GENERALES

L'OAI accueille favorablement le projet visant à accroître la capacité des services de l'Etat à utiliser les données numériques existantes et futures dans un objectif d'optimisation de leurs missions, ce dans l'assurance d'une parfaite protection des données individuelles sources.

Historiquement, le moteur initial réglementaire trouve son fondement dans le règlement (UE) 2022/868 sur la gouvernance des données applicable à partir du 24/09/2023. Ce règlement se trouve être d'application directe mais néanmoins, pour le chapitre des conditions applicables à l'accès et à la réutilisation des données détenues par les organismes du secteur public, des précisions doivent être apportées au niveau national, ce qu'ambitionne de faire le présent projet de loi sous analyse. Notamment, le projet détaille les dispositions relatives à la désignation des organismes compétents, la procédure à suivre pour l'octroi des autorisations d'accès et de réutilisation des données ainsi que les conditions applicables à l'accès et à la réutilisation des données.

En outre, le projet de loi prévoit des dispositions spécifiques visant la mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), notamment en énonçant les finalités pour lesquelles le traitement ultérieur des données à caractère personnel est autorisé.

Différents acteurs compétents en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation sont prévus par le projet de loi dont les missions sont globalement résumées de la manière suivante :

- l'Autorité des données, dont les responsabilités sont assumées par le Commissariat du Gouvernement à la protection des données, en tant qu'organe de réflexion et de catalyse dans le domaine du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation de données respectivement, en tant que conseil en la matière près le ministre ayant la digitalisation dans ses attributions, en tant que promoteur et force de sensibilisation auprès des entités publiques et organismes de droit public dans les bonnes pratiques,
- le Centre des technologies de l'information de l'Etat et le « *Luxembourg National Data Service* » en tant qu'assistants techniques à l'Autorité des données,
- le tiers de confiance en tant qu'exécutant des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données,
- le point d'information unique en tant qu'organe-pivot recevant les demandes d'accès et de réutilisation pour la transmission à l'Autorité des données, en tant qu'office de publication d'informations, en tant que gestionnaire d'une liste des ressources consultable donnant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données,
- le Conseil consultatif de la valorisation des données dans un environnement de confiance, composé de représentants issus des ministères et administrations de l'Etat, en tant qu'organe consultatif de l'Autorité des données.

D'autre part, complétant la dynamique de valorisation des données dans un environnement fiable, le projet met en avant le principe « once only » (fourniture une seule et unique fois des données aux autorités) en insufflant un cadre procédural optimisé qui permettra de rendre plus rapides et plus efficaces les démarches réalisées par les citoyens et les entreprises.

Cette mesure rentre en plein avec le vœu de l'OAI de favoriser le plus possible **une véritable simplification administrative, se traduisant par une digitalisation intelligente des procédures, pour dématérialiser et accélérer leur instruction** afin d'obtenir notamment les autorisations plus rapidement, de manière plus fluide et traçable, et pour les projets requérant de multiples autorisations, par la création d'un « guichet unique » disposant de compétences transversa les pour traiter à la fois avec les administrations étatiques et communales.

Enfin, nous tenons à rappeler la position de l'OAI quant à l'élaboration d'un paquet complet – regroupant lois et règlements grand-ducaux d'exécution – afin d'éviter des phases d'incertitude qui favorisent la judiciarisation du secteur.

*

2. METHODOLOGIE

Le présent avis a été établi notamment suite à l'analyse par le Conseil de l'Ordre et par le groupe de travail OAI « Diagnostic des incohérences au niveau des lois / RGD et des problèmes structurels dans les procédures ».

*

3. AVIS SUR LE PROJET DE LOI N°8395 RELATIF A LA VALORISATION DES DONNEES DANS UN ENVIRONNEMENT DE CONFIANCE

L'intérêt majeur concernant l'OAI est l'application „once only" dans les marchés publics.

A ce sujet l'OAI rappelle la lourdeur de la gestion administrative des participations à des marchés publics.

Pour chaque soumission, chaque pouvoir adjudicateur (et parfois le même pouvoir adjudicateur pour diverses soumissions pourtant rapprochées dans le temps !) exige du soumissionnaire (en principe uniquement celui susceptible d'être déclaré adjudicataire) les pièces justificatives requises dans le cadre du contrôle de l'absence de cause d'exclusion, en particulier :

1. Certificat d'inscription au registre professionnel
2. Certificat d'inscription au registre de commerce
3. L'(les) autorisation(s) d'établissement valables pour chaque membre du groupement
4. Extrait du casier judiciaire
5. Les pièces attestant la situation fiscale et parafiscale du candidat (attestation établie par le Centre d'informatique, d'affiliation et de perception des cotisations commun aux institutions de sécurité sociale, et l'Administration des contributions directes).

L'OAI escompte donc que la loi en projet conduira à l'application concrète du principe « once only ».

Le principe de la collecte unique de données doit être un des moyens essentiels de simplifier les différentes procédures et formulaires publiques obligatoires pour les soumissionnaires (coffre-fort électronique).

L'OAI préconise que la mise en œuvre de cette réforme fasse l'objet de mesures d'accompagnement sur le terrain. Il s'agira d'informer et de former les agents publics étatiques et communaux afin de mettre concrètement en application une politique de gestion administrative conforme au principe « once only ».

Pour rappel, en matière de marchés publics le document unique de marché dit DUME (applicable pour les marchés européens, Livres II et III) est un instrument qui a été créé dans le cadre du plan d'action européen e-Government UE 2016-2020, conformément au principe « once only » et devait contribuer à réduire la charge administrative et à faciliter la participation des opérateurs économiques aux soumissions.

Or, en pratique, en dépit des dispositions de la loi modifiée du 8 avril 2018 sur les marchés publics, cette simplification administrative n'est pas toujours respectée par les pouvoirs adjudicateurs qui réclament souvent, pour tout candidat, la remise du DUME ET la remise des documents administratifs (les certificats évoqués ci-avant) qui doivent figurer à l'appui de chaque nouvelle soumission.

L'OAI indique par conséquent qu'il faudra veiller à ce que le principe « once only » trouve une traduction concrète et une application généralisée par les entités publiques concernées.

*

4. CONCLUSION

L'OAI est en mesure de marquer son accord sur le présent projet de loi sous réserve de la prise en compte de ses remarques.

Luxembourg, le 28 octobre 2024

Pour l'Ordre des Architectes et des Ingénieurs-Conseils

Michelle FRIEDERICI	Patrick NOSBUSCH	Pierre HURT
Présidente	*Vice-Président*	*Directeur*

Impression: CTIE – Division Imprimés et Fournitures de bureau

20250515_Avis_2

N° 8395[4]

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(20.12.2024)

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (ci-après la « loi du 1er août 2018 »), la Commission nationale pour la protection des données (ci-après la « Commission nationale » ou la « CNPD ») « *conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ».

Par ailleurs, l'article 36.4 du RGPD dispose que « *[l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement* ».

2. Par courrier du 12 juin 2024, Madame la Ministre de la Digitalisation a invité la Commission nationale à aviser le projet de loi n°8395 relatif à 1° la valorisation des données dans un environnement de confiance ; 2° la mise en œuvre du principe « once only » ; 3° la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ; 4° la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces

données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « projet de loi »).

3. Le présent projet de loi vise à introduire en droit luxembourgeois des précisions quant aux traitements de données à caractère personnel effectués par des entités publiques dans le cadre de l'exécution de leurs missions d'intérêts public (Titre II), ainsi qu'au traitement ultérieur de données à caractère personnel mis en œuvre par lesdites entités publiques (Titre V). De même, le projet de loi vise à instaurer en droit national l'échange d'informations et de données à caractère personnel entre entités publiques, c'est-à-dire le principe du « once only » (Titre IV).

4. La CNPD constate que le projet de loi vise parallèlement à mettre en œuvre certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (ci-après le « règlement 2022/868 »). Plus précisément, le Titre VI du projet de loi encadre l'accès et la réutilisation de données détenues par des organismes du secteur public par des réutilisateurs de données[1], tandis que le Titre VIII contient des précisions relatives à la gouvernance des services d'intermédiation de données et d'altruisme de données[2].

*

I. REMARQUES LIMINAIRES

5. A titre préliminaire, la Commission nationale regrette qu'au sein du projet de loi des dispositions purement nationales, comme par exemple l'introduction en droit luxembourgeois du principe du « once only », soient mélangées à des dispositions visant à implémenter le règlement 2022/868, alors que cela rend difficile la compréhension et la lisibilité du projet de loi. Ce d'autant plus que le législateur a fait le choix de rendre applicable des dispositions issues de la mise en œuvre dudit règlement 2022/868 à des dispositions nationales.

Elle constate notamment que les modalités concernant un traitement ultérieur des données à caractère personnel par les entités publiques du Grand-duché, d'une part, et celles applicables à l'accès et à la réutilisation de données conformément au chapitre II du règlement 2022/868, d'autre part, sont regroupées sous un même titre du projet de loi.[3] Ce regroupement au sein d'un même titre crée a priori l'impression qu'il s'agit de modalités en commun pour le traitement ultérieur, ainsi que pour la réutilisation de données. Néanmoins, en analysant en détail ledit titre, la Commission nationale remarque que certaines dispositions y contenues sont identiques pour les deux procédures, alors que d'autres sont divergentes, ce qui rend la lecture du projet de loi particulièrement compliquée. Par exemple, les exigences de forme de la demande d'autorisation ou son instruction par l'Autorité des données[4] sont pareilles pour les deux modalités,[5] alors que les dispositions sur le contenu de ladite demande ou la procédure d'autorisation par l'Autorité des données diffèrent d'une procédure à l'autre.[6]

6. La CNPD est dès lors d'avis qu'il n'est pas aisé pour une entité publique qui souhaite demander une autorisation pour un traitement ultérieur de données à caractère personnel, voire pour un réutilisateur désirant formuler une demande d'accès et de réutilisation de données, de comprendre les différentes procédures et les démarches à accomplir. Cela vaut d'autant plus, pour les personnes concernées dont les données à caractère personnel sont susceptibles d'être traitées dans ce contexte. En effet, il est très difficile de saisir quelles conditions et garanties sont à respecter par les entités publiques ou les réutilisateurs de leurs données.

---

1 Voir Chapitre II du règlement 2022/868.

2 Voir Chapitres III et IV du règlement 2022/868.

3 Voir le TITRE VII du projet de loi intitulé « *Modalités applicables au traitement ultérieur des données à caractère personnel par les entités publiques et à l'accès et à la réutilisation de données par des réutilisateurs de données.* »

4 Voir commentaires de la CNPD sous le point « II.B Sur l'Autorité des données ».

5 Voir articles 26 et 29 du projet de loi.

6 Voir articles 27, 28 et 31 du projet de loi.

Elle se demande même dans ce contexte si, pour plus de clarté et de compréhension, il ne serait pas plus approprié de scinder le projet de loi en deux pour distinguer entre les dispositions purement nationales[7] et celles qui visent à implémenter le règlement 2022/868[8].

*

II. SUR LES ACTEURS COMPETENTS EN MATIERE DE TRAITEMENT ULTERIEUR DE DONNEES A CARACTERE PERSONNEL ET D'ACCES ET DE REUTILISATION DE DONNEES

A. Sur les entités publiques et les organismes du secteur public

7. La Commission nationale note que l'article 2, paragraphe (2) du projet de loi définit de manière très large la notion d'« entité publique » en englobant une multitude de différents acteurs, et plus précisément « *un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal […]* ». Par ailleurs, il ressort du commentaire des articles que lesdites personnes morales d'utilité publique visent aussi « *les fondations et associations sans but lucratif, notamment les hôpitaux au sens de la loi modifiée du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière, qui sont listés expressément par règlement grand-ducal aux fins d'application du titre IV et/ou du titre V.* »

8. La Commission nationale note tout d'abord que, d'après le commentaire des articles, la définition d'« entité publique » est « *volontairement distincte de la notion d'organisme du secteur public visée par les dispositions du règlement (UE) 2022/868.* » En effet, conformément à l'article 3, paragraphe (1) du règlement 2022/868, le chapitre II sur la réutilisation[9] s'applique uniquement aux données détenues par les organismes du secteur public, tandis que l'article 3, paragraphe (2) dudit règlement exclut expressément les données détenues par les entreprises publiques. En ce qui concerne le terme « entité publique » utilisé par le projet de loi sous avis, celui-ci n'est pas mentionné du tout dans ce règlement.

9. La CNPD conclut dès lors sur base de ce qui précède que les « entités publiques » sont uniquement concernées par les dispositions purement nationales, c'est-à-dire les titres II, IV et V du projet de loi relatifs au traitement nécessaire à l'exécution d'une mission d'intérêt public, au principe du « once only », ainsi qu'au traitement ultérieur de données à caractère personnel, tandis que les « organismes du secteur public » sont seulement visés par le titre VI sur la réutilisation des données qu'ils détiennent en implémentation du règlement 2022/868.

Néanmoins, en comparant la définition de l'« organisme du secteur public » contenue à l'article 2, point 17) du règlement 2022/868[10] à celle précitée de l'« entité publique », la Commission nationale a des difficultés à saisir en quoi consiste concrètement la différence entre les deux notions. En d'autres termes, elle se demande quelles entités seraient uniquement visées par l'une des deux notions, voire lesquelles seraient même englobées par les deux.

10. Ensuite, elle voudrait contredire les affirmations des auteurs du projet de loi selon lesquelles la définition de l'entité publique « *permet de limiter avec précision le champ d'application des échanges d'informations et de données à caractère personnel dans le cadre du principe « once only » aux Ministères, y compris leurs services, administrations et aux communes luxembourgeoises* », alors que le titre IV sur le « once only » vise aussi les établissements publics, les groupements d'intérêt économique, ainsi que les personnes morales d'utilité publique, y inclus les fondations et associations sans

---

7 V. point 3 du présent avis.

8 V. point 4 du présent avis.

9 Intitulé intégral du Chapitre II du règlement 2022/868 : „Réutilisation de certaines données détenues par des organismes du secteur public. »

10 « *l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public* ».

but lucratif et les hôpitaux. Elle se réfère dans ce contexte notamment au recueil listant les établissements publics au Luxembourg[11] qui contient un nombre élevé d'acteurs venant de différents secteurs, dont la CNPD, et qui tomberaient donc dans la définition d'« entité publique », comme par exemple la Banque et Caisse d'Epargne de l'Etat (Spuerkees), la Banque centrale du Luxembourg (BCL), les Centres de recherche LIH, LIST et LISER,[12] différentes chambres professionnelles,[13] le Corps grand-ducal d'incendie et de secours (CGDIS) ou encore !'Entreprise des postes et télécommunications (POST Luxembourg).

La Commission nationale se permet dès lors d'exprimer déjà à ce stade ses inquiétudes sur l'ampleur potentielle du projet de loi, compte tenu des acteurs qui pourraient être susceptibles d'appliquer ses dispositions.

11. Finalement, il y a lieu de constater que la définition de l'entité publique exclut du champ d'application du projet de loi les autorités compétentes en matière pénale et sécurité nationale[14], ainsi que les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif, lorsqu'elles effectuent un traitement de données à caractère personnel dans l'exercice de leurs fonctions juridictionnelles.[15]

Cependant, il convient de souligner que lesdites autorités compétentes définies par l'article 2, point 7° de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, englobent déjà les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif. La qualification relative au fait de savoir si un traitement de données à caractère personnel est opéré par une telle juridiction dans l'exercice de sa fonction juridictionnelle ou non est uniquement importante afin de savoir quelle autorité de contrôlé est compétente : la CNPD ou l'autorité de contrôle judiciaire. Il est dès lors superfétatoire d'exclure spécifiquement lesdites juridictions par l'article 2, paragraphe (2) point 2, lettre b) du projet de loi, alors qu'elles sont déjà englobées par l'exclusion contenue à la lettre a) dudit article visant les autorités compétentes conformément à l'article 2, point 7 de la loi susmentionnée.

B. Sur l'Autorité des données

12. D'après l'article 4, paragraphe (1) du projet de loi, le Commissariat du Gouvernement à la protection des données auprès de l'Etat est chargé des missions attribuées à l'Autorité des données dans le cadre du projet de loi et désigné tout au long par ce terme.

13. La Commission nationale tient tout d'abord à exprimer ses plus vives inquiétudes avec le choix du terme « Autorité des données », alors qu'il risque de porter confusion avec celui de la Commission nationale étant l'« Autorité de contrôle » chargée de contrôler et de vérifier notamment si les données soumises à un traitement sont conformes aux dispositions du RGPD et de la loi du 1er août 2018. De son expérience sur le terrain, la CNPD ne peut que constater que cette confusion existe déjà aujourd'hui entre les dénominations de « Commission nationale pour la protection des données » et de « Commissariat du Gouvernement à la protection des données auprès de l'État ». Pour des raisons de compréhension, elle utilisera néanmoins le terme « Autorité des données » dans son avis pour viser le Commissariat du Gouvernement à la protection des données auprès de l'Etat, même si elle estime qu'il serait plus opportun de désigner ledit Commissariat par les termes « Commissariat du Gouvernement ».

---

11 Version applicable au 22 juillet 2024 et disponible ici : https://legilux.public.lu/eli/etat/leg/recueil/etablissements_publics/20240722

12 Centre de recherche public Luxembourg lnstitute of Health (LIH), Centre de recherche public Luxembourg lnstitute of Science and Technology (LIST), le Centre de recherche public Luxembourg lnstitute of Socio-Economic Research (USER)

13 Comme par exemple la Chambre des métiers, la Chambre de commerce, la Chambre des fonctionnaires et des employés publics ou encore la Chambre des salaries.

14 A l'instar des dispositions de l'article 2 du règlement (UE) 2016/679 et de l'article 1er de la directive (UE) 2016/6801 transposée en droit luxembourgeois par la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité national.

15 V. article 2 paragraphe (2) point 2°, lettres a) et b) du projet de loi.

14. Elle constate ensuite que les missions que l'Autorité des données assumera dans l'état actuel du projet de loi sont très vastes. En effet, elle aura non seulement des missions qui découlent de la mise en œuvre du règlement 2022/868, notamment en étant désignée « organisme compétent » conformément à l'article 7 paragraphe (1) dudit règlement et habilitée à octroyer ou refuser l'accès à des fins de réutilisation des données, mais également des missions dans le cadre des nouvelles dispositions nationales[16] en étant, par exemple, en charge d'autoriser ou de refuser le traitement ultérieur de données à caractère personnel par les entités publiques.[17]

15. L'article 32 du projet de loi confère dans ce contexte certains pouvoirs de contrôle à l'Autorité des données. Après vérification des résultats d'un traitement ultérieur de données à caractère personnel par une entité publique ou d'une réutilisation de données par un réutilisateur, elle pourrait notamment interdire l'utilisation de ces résultats s'ils portent une atteinte disproportionnée aux droits et intérêts de tiers.

16. Comme les traitements ultérieurs de données et, le cas échant, les réutilisations de données peuvent porter sur des données à caractère personnel au sens de l'article 4, point 1) du RGPD, la CNPD se demande si les dispositions précitées ne sont pas susceptibles d'entrer en conflit avec ses propres missions et pouvoirs. Le commentaire des articles précise à cet égard que « *[l]es dispositions de l'article 32 s'entendent sans préjudice des prérogatives de la Commission nationale pour la protection des données d'interdire les traitements de données à caractère personnel opérés en contravention aux conditions reprises dans l'autorisation émise par l'Autorité des données, conformément au règlement (UE) 2016/679, lu ensemble avec la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.* »[18]

17. Néanmoins, sur base des pouvoirs qu'elle détient en vertu de l'article 58 du RGPD et de l'article 12 de la loi du 1er août 2018, la CNPD estime que ses pouvoirs de contrôle et de sanctions ne se limitent pas à la vérification des conditions que l'Autorité des données va prévoir dans ses autorisations, mais dès qu'une entité est à considérer comme responsable du traitement ou comme sous-traitant au sens de l'article 4, points 7 et 8) du RGPD, la CNPD est compétente pour vérifier l'application et le respect de l'intégralité des dispositions du RGPD et de la loi du 1er août 2018. D'autant plus, il serait possible que la CNPD ne soit pas d'accord avec certaines prises de positions de l'Autorité des données émises dans ses autorisations ce qui crée un risque de décisions divergentes entre l'Autorité des données et la CNPD, voire de régimes parallèles et incohérents entre le RGPD et le règlement 2022/868 et sa future loi d'implémentation.

18. Par ailleurs, la CNPD tient à souligner que ses pouvoirs de sanctions sont beaucoup plus étendus et ne se limitent pas à l'imposition d'une interdiction de traitement de données à caractère personnel prévue par l'article 58, paragraphe (2), point f) du RGDP. Si elle constate dès lors qu'une entité publique, voire un réutilisateur de données ne respecte pas un des principes ou obligations du RGPD, elle dispose de tous ses pouvoirs prévus par l'article 58 du RGPD. Par exemple, si la CNPD estime qu'un réutilisateur en sa qualité de responsable du traitement ne respecte pas, dans le cadre de l'accès aux données à caractère personnel lui accordé sur base de l'autorisation émise par l'Autorité des données, le principe de limitation des finalités ou de minimisation des données prévus par les articles 5, paragraphe (1), lettres b) et c) du RGPD, elle pourrait, entre autres, lui ordonner de se mettre en conformité ou même lui imposer une amende administrative en application de l'article 83 du RGPD, en notant toutefois que l'article 48, paragraphe (1) de la loi du 1er août 2018 prévoit que la CNPD ne peut pas imposer d'amende administrative à l'encontre de l'Etat ou des communes.

19. La CNPD ne peut que se référer dans ce contexte au Comité européen de la protection des données (ci-après l'« EDPB ») et au Contrôleur européen de la protection des données (ci-après le « CEPD ») qui ont déjà estimé en 2021 dans un avis sur l'ancienne proposition du règlement 2022/868 que « *lorsque des données à caractère personnel sont réutilisées sur la base de la proposition, l'EDPB et le CEPD estiment que les autorités de contrôle chargées de la protection des données devraient être*

16 V. point 3 du présent avis.

17 V. notamment l'article 4 du projet de loi.

18 V. commentaire de l'article 32 du projet de loi.

les seules compétentes pour surveiller le traitement de ces données à caractère personnel. Ces autorités devraient être dotées de ressources adéquates pour leur permettre d'accomplir cette mission de manière efficace et efficiente.

Par ailleurs, dans le cas où des organismes spécifiques seraient désignés pour aider les organismes du secteur public et les réutilisateurs de données et chargés d'octroyer l'accès aux données, y compris aux données à caractère personnel, en vue d'une réutilisation, ces organismes ne pourraient être qualifiés de « compétents » puisqu'ils n'agiraient pas en tant qu'autorité de contrôle capable de surveiller les dispositions relatives au traitement des données à caractère personnel et de veiller à leur respect. Pour garantir la sécurité juridique et la cohérence dans l'application de l'acquis de l'Union dans le domaine de la protection des données à caractère personnel, les activités et obligations de ces organismes désignés doivent aussi être soumises à la compétence et au contrôle directs d'autorités chargées de la protection des données lorsque des données à caractère personnel sont enjeu. »[19].

20. Finalement, il convient de se demander si l'Autorité des données pourra jouer en toute neutralité son rôle d'arbitrage pour accorder ou refuser un traitement ultérieur ou un accès et une réutilisation de données, alors qu'elle fera partie du futur Conseil consultatif de la valorisation des données dans un environnement de confiance (ci-après le « Conseil consultatif ») prévu par l'article 8 du projet de loi. En effet, d'une part l'Autorité des données devra trancher sur une demande de traitement ultérieur ou d'accès et de réutilisation de données et d'autre part elle pourra en tant que membre dudit Conseil aviser les mêmes demandes. L'article 29 paragraphe (7) du projet de loi prévoit même expressément que « *[l]'Autorité des données peut transmettre la demande de traitement ultérieur de données à caractère personnel visée à l'article 27 et la demande d'accès et de réutilisation visée à l'article 28 au Conseil consultatif pour avis.* ».

C. Sur le Centre des technologies de l'information de l'Etat et le LNDS

21. La CNPD constate que, sur base de l'article 5 du projet de loi, le Centre des technologies de l'Information de l'Etat (ci-après le « CTIE ») et le groupement d'intérêt économique PNED G.I.E – Plateforme nationale d'échange de données (ci-après le « LNDS ») sont désignés organismes compétents au sens de l'article 7, paragraphe (1) du règlement 2022/868 pour fournir une assistance technique à l'Autorité des données dans l'exercice de ses missions conformément aux dispositions du projet de loi. Elle n'a pas d'observations dans ce contexte.

D. Sur le tiers de confiance

22. L'article 2, paragraphe (2) point 3° du projet de loi définit le « tiers de confiance » comme « *toute entité fonctionnellement indépendante des entités publiques visées au titre V, des organismes du secteur public détenant les données et du réutilisateur de données visés au titre VI, qui remplit les conditions prévues à l'article 6.* »

23. De longue date, la CNPD recommande dans ses avis juridiques l'encadrement général de l'activité d'un tiers de confiance permettant d'accompagner le développement de services innovants en matière de pseudonymisation et d'anonymisation au Luxembourg, d'une part, et que de tels services devraient être réservés à des acteurs présentant des garanties d'indépendance, de compétence et ne se trouvant pas en situation de conflit d'intérêts au regard des données qu'ils traitent dans le cadre de leurs diverses activités[20].

24. De manière générale, elle ne peut donc que féliciter les auteurs du projet de loi d'avoir suivi finalement cette recommandation. Néanmoins, bien que l'article 6 du projet de loi énumère les missions du tiers de confiance et les conditions qu'il doit remplir, la CNPD a des difficultés à comprendre comment et par qui le tiers de confiance sera désigné.

---

19 Avis conjoint 03/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), Version 1.1 du 9 juin 2021, points 104 et 105.

20 V. par exemple délibération n°1005/2016 du 2 décembre 2016 de la Commission nationale pour la protection des données, doc. parl. n°7061/03, p. 4 ou délibération n°96/AV42/2023 du 10 novembre 2023 de la Commission nationale pour la protection des données, doc. parl. 8251/02, point 27.

25. Elle constate que les auteurs du projet de loi ont inscrit dans les missions de l'Autorité des données, du CTIE et du LNDS de « *collaborer avec le tiers de confiance mandaté par le Centre* ».[21] De même, dans l'exposé des motifs, il est mentionné que « *[p]our éviter d'éventuels conflits d'intérêts et pour maintenir la confiance des citoyens dans une gestion prudente de leurs données par les acteurs publics, la loi prévoit la possibilité pour le Centre des technologies de l'information de l'État de recourir aux services d'un tiers de confiance.* »

26. Comme ce volet ne ressort pas du texte actuel du projet de loi, la CNPD se demande, sur base de ce qui précède, si la seule possibilité pour devenir tiers de confiance est que l'on soit mandaté par le CTIE ? Ou est-ce qu'une entité publique pourrait aussi prendre recours aux services d'un tiers de confiance qu'elle a désigné elle-même ? Se pose aussi la question de savoir si la désignation d'un tiers de confiance est limitée aux missions encadrées par le présent projet de loi ou si, par contre, un tel tiers de confiance pourrait aussi être désigné par une entité publique dans le cadre d'autres missions légales qu'elle poursuit ? De même, il ne ressort pas du projet de loi qui aurait les compétences et les pouvoirs pour contrôler si un tiers de confiance, soit désigné par le CTIE ou par une autre entité publique, remplit les conditions énumérées à l'article 6, paragraphe (2) du projet de loi.

27. La Commission nationale recommande dès lors d'intégrer des précisions dans ce contexte dans le corps du texte du projet de loi.

E. Sur le point d'information unique

28. Conformément à l'article 8 du règlement 2022/868, l'article 7 du projet de loi prévoit l'instauration d'un point d'information unique sous l'autorité du ministre ayant la digitalisation dans ses attributions.

29. La CNPD comprend donc que ce point d'information unique est structurellement différent de l'Autorité des données, même si les deux organismes sont placés sous l'autorité du ministre ayant la digitalisation dans ses attributions.

30. Par ailleurs, le commentaire des articles mentionne la « possibilité » pour ledit ministre de sous-traiter les missions du point d'information unique au LNDS. La CNPD constate dans ce contexte que cette option n'est pas expressément mentionnée dans le projet de loi, d'une part, et si cette désignation est vraiment le souhait du législateur, elle se demande pourquoi le LNDS n'est pas directement désigné dans l'article 7 du projet de loi comme point d'information unique, d'autre part.

31. Finalement, l'article 7, paragraphe (2), lettre c) du projet de loi prévoit que le point d'information unique doit « mettre à disposition » par voie électronique une série d'informations conformément à l'article 8, paragraphe (2) du règlement 2022/868. La CNPD suppose qu'il s'agit d'une mise à disposition d'informations pour le grand public. De même, elle se demande comment ladite mise à disposition aura lieu dans la pratique : Est-ce que la création d'un système national d'échange est envisagé ou est-ce que lesdites informations seront simplement publiées sur le site internet du point d'information unique ?

F. Sur le Conseil consultatif

32. La Commission nationale se permet de renvoyer au point 20 du présent avis en ce qui concerne la problématique relative au fait que l'Autorité des données fera partie du futur Conseil consultatif, prévu par l'article 8 du projet de loi.

*

21 V. article 4, paragraphe (4), lettre b), article 5, paragraphe (2) lettre e) et paragraphe (3) lettre d) du projet de loi.

III. SUR LE VOLET NATIONAL

A. Sur le traitement de données à caractère personnel par les entités publiques nécessaire à l'exécution de la mission d'intérêt public ou relevant de l'autorité publique

33. L'article 3 du projet de loi vise à introduire en droit national une base légale générale pour l'ensemble des traitements de données à caractère personnel effectués par les entités publiques qui seraient nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique. D'après les auteurs du projet de loi, cette disposition vise à « *renforcer la sécurité juridique en matière de traitement de données à caractère personnel par les entités publiques dans le cadre de l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies* »[22].

34. La Commission nationale avise négativement l'introduction d'une telle disposition, dans la mesure où elle estime que cette disposition soulève un grand nombre de problématiques détaillées ci-après.

a. *Sur la reproduction partielle ou intégrale d'une disposition du RGPD dans l'ordre juridique interne*

35. La première problématique relève de la reproduction partielle ou intégrale d'une disposition d'un règlement européen dans l'ordre juridique interne. En effet, le Conseil d'État rappelle régulièrement dans ses avis la jurisprudence de la Cour de justice de l'Union européenne selon laquelle les États membres ne doivent pas entraver l'applicabilité directe des règlements ni en dissimuler la nature européenne[23].

36. Or, les dispositions de l'article 3 du texte sous avis se bornent à réitérer les dispositions de l'article 6.1.e) et 6.3 du RGPD.

b. *Sur la position constante de la CNPD en ce qui concerne les dispositions de l'article 6.1.e) et 6.3 du RGPD*

37. Les auteurs du projet de loi estiment qu'« *il suffit, d'après l'article 6, paragraphe 3 du règlement (UE) 2016/679 que le traitement de données à caractère personnel prévu à l'article 6, paragraphe 1er, point e) du règlement (UE) 2016/679 soit nécessaire à « l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* ». Dès lors, ils considèrent que la définition des finalités dans un texte spécifique n'est pas requise.

38. Les auteurs du projet de loi justifient une telle approche car « *il paraît difficilement concevable que le législateur adopte pour chacun des traitements de données à caractère personnel nécessaires au bon fonctionnement et à la réalisation des missions des entités publiques (dont le nombre d'hypothèses est en réalité considérable voire illimité) une loi spécifique au sens formel* »[24].

Toutefois, la CNPD ne partage pas et n'approuve pas l'approche de prévoir une base légale générale pour tous les traitements de données à caractère personnel qui seraient mis en œuvre par toutes les « entités publiques » dans le cadre de l'exécution de leurs missions d'intérêt public.

39. Elle estime que l'article 6.1.e) du RGPD, lu en combinaison avec l'article 6.3 du RGPD, prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect de l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ce cas de figure, le fondement, c'est-à-dire la mission d'intérêt

---

22 V. commentaire des articles.

23 V. avis du Conseil d'État CE 61.218, doc. parl. n°8089, l'avis du Conseil d'Etat du 17 juillet 2020 sur le projet de loi n°7537 relative à certaines modalités de mise en oeuvre du règlement (UE) n° 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne.

24 Ad article 3 du projet de loi

public en cause, et notamment les finalités des traitements de données doivent ressortir soit du droit de l'Union européenne, soit du droit de l'Etat membre auquel le responsable du traitement est soumis et ce fondement doit répondre « *à un objectif d'intérêt public* » et être « *proportionné à l'objectif légitime poursuivi* ».

Par ailleurs, la Commission nationale tient à rappeler que sa position en la matière est étayée par la jurisprudence de la Cour de justice de l'Union européenne (ci-après la « CJUE »), des avis du Conseil d'État ainsi que des arrêts de la Cour constitutionnelle.

c. *La protection des données, une matière réservée à la loi*

40. L'article 31 de la Constitution, qui figure dans la section consacrée aux libertés publiques, dispose que « *[t]oute personne a droit à l'autodétermination informationnelle et à la protection des données à caractère personnel la concernant. Ces données ne peuvent être traitées qu'à des fins et dans les conditions déterminées par la loi* ». Ainsi, la protection des données à caractère personnel est une matière réservée à la loi par la Constitution. L'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc.

41. Cependant, les droits fondamentaux ne sont pas des prérogatives absolues puisque la possibilité d'une ingérence ou d'une limitation est prévue par l'article 8.2 de la Convention européenne des droits de l'homme, par l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne, ainsi que par l'article 37 de la Constitution qui prévoit que « *[t]oute limitation de l'exercice des libertés publiques doit être prévue par la loi et respecter leur contenu essentiel. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires dans une société démocratique et répondent effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui* ».

42. Par conséquent, la Commission nationale estime que si les traitements de données mis en œuvre par une entité publique dans le cadre de l'exécution de ses missions d'intérêt publique constituent une ingérence dans la vie privée des citoyens, alors ces traitements doivent être spécifiquement encadrés par une loi au sens formel.

43. En effet, une ingérence ou limitation dans l'exercice des libertés publiques peut uniquement être justifiée à condition qu'elle soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante, respecte le contenu essentiel du droit à la protection des données et réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui. L'ingérence doit également être nécessaire dans une société démocratique, sous réserve du principe de proportionnalité[25].

44. Enfin, au sujet de ces textes, le Conseil d'État a considéré[26] que la « *Cour constitutionnelle, en affinant sa jurisprudence antérieure, a, dans son arrêt n°177 du 3 mars 2023, retenu que « [d]'après l'article 32, paragraphe 3, de la Constitution[27], dans les matières réservées par la Constitution à la loi, la fixation des objectifs des mesures d'exécution doit être clairement énoncée de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir*

---

25 Pour une analyse plus détaillée de ces conditions, voir délibération n°2/2021 du 4 février 2021 de la Commission nationale pour la protection des données, doc. parl. n° 7425/09, point I.1.b). Voir aussi arrêt de la CJUE du 7 mars 2024, C-740/22, point 52, « *[…] les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel ne sont pas des prérogatives absolues ainsi que l'indique le considérant 4 du RGPD, mais doivent être pris en considération par rapport à leur fonction dans la société et être mis en balance avec d'autres droits fondamentaux. Des limitations peuvent ainsi être apportées, pourvu que, conformément à l'article 52, paragraphe 1, de la Charte, elles soient prévues par la loi et qu'elles respectent le contenu essentiel des droits fondamentaux ainsi que le principe de proportionnalité. En vertu de ce dernier principe, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui. Elles doivent s'opérer dans les limites du strict nécessaire et la réglementation comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause* ».

26 Avis du Conseil d'Etat n° CE 61.798 relatif au projet de loi portant organisation de l'Administration du cadastre et de la topographie, doc. parl. n°8330B/02.

27 En l'occurrence, il s'agit de l'article 45, paragraphe 2, de la Constitution révisée, à contenu identique sur ce point.

exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi »[28].

45. Il résulte de ce qui précède que la Commission nationale ne partage pas l'avis des auteurs du projet de loi selon lequel « *le fait pour une entité publique de pouvoir démontrer le respect de la double condition : premièrement qu'elle est investie d'une mission d'intérêt public ou qui relève de l'exercice de l'autorité publique dont elle est investie et, deuxièmement, que le traitement de données à caractère personnel est « nécessaire » pour réaliser cette mission, suffit à légitimer la collecte et le traitement des données en question* ».

d. *Sur la position du Conseil d'Etat*

46. Les auteurs du projet de loi estiment que la position du Conseil d'Etat serait identique à la leur. Ils s'appuient sur un avis du 30 mars 2018 pour étayer leur prétention. Dans cet avis, le Conseil d'Etat avait estimé qu'« *[a]ux termes de l'article 6 du [RGPD], la licéité du traitement dans le secteur public est vérifié si le traitement est nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique. Dans cette logique, il ne s'impose pas de donner à chaque traitement de données une base spécifique légale ou réglementaire* ».

47. Toutefois, la position du Conseil d'Etat a fortement évolué et sa position actuelle diffère de celle citée par les auteurs du projet de loi. La nouvelle position du Conseil d'Etat semble constante et est étayée par de nombreux avis récents, surtout depuis l'entrée en vigueur de la Constitution révisée le 1er juillet 2023.

Ainsi, le Conseil d'État rappelle que l'accès à des fichiers et la communication de données à des tiers constituent une ingérence dans la vie privée et partant, une matière réservée à la loi formelle[29]. Par ailleurs, dans un avis récent du 11 juin 2024, celui-ci a considéré qu' :

« *[e]n ce qui concerne l'échange d'informations, le Conseil d'État note, à la lecture du commentaire de l'article, qu'il s'agit de données à caractère personnel et rappelle, à cet égard, que l'article 31 de la Constitution, qui figure dans la section consacrée aux libertés publiques, dispose que « [t]oute personne a droit à l'autodétermination informationnelle et à la protection des données à caractère personnel la concernant. Ces données ne peuvent être traitées qu'à des fins et dans les conditions déterminées par la loi », tandis que l'article 37 de la Constitution précise, dans sa première phrase, que « [t]oute limitation à l'exercice des libertés publiques doit être prévue par la loi et respecter leur contenu essentiel ».*

Il s'ajoute à ce rappel des textes fondamentaux que la Cour constitutionnelle, en affinant sa jurisprudence antérieure, a, dans son arrêt 5 n°177 du 3 mars 2023, retenu que « [d]'après l'article 32, paragraphe 38 , de la Constitution, dans les matières réservées par la Constitution à la loi, la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi ».

Il y a lieu de déterminer, dans l'ordre juridique national, les conditions dans lesquelles les données à caractère personnel peuvent être traitées pour une finalité autre que celle pour laquelle elles ont été collectées au sens de l'article 6, paragraphe 4, du 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 le « règlement (UE) 2016/679 », ce qui couvre les hypothèses dans lesquelles des données sont communiquées par un ministre à un autre ou par une administration à une autre, tout comme celles dans lesquelles les données collectées et traitées par une administration

---

28 Cour constitutionnelle, 3 mars 2023, n° 177, Mém. A n° 127 du 10 mars 2023, Cour constitutionnelle, 4 juin 2021, n° 166, Mém. A n°440 du 10 juin 2021 et Cour constitutionnelle, 3 mars 2023, n° 177, Mém. A, n° 127 du 10 mars 2023.

29 V. notamment avis du Conseil d'Etat n° CE 60.250 du 22 mars 2022, doc. parl. n° 7578/01, p. 5 ; avis du Conseil d'Etat n°CE 53.322 du 12 juillet 2019, doc. parl. n° 7425/04, p. 9 ; avis du Conseil d'Etat n° CE 51.586 du 7 juin 2016, doc. parl. n° 6975/05, p. 4 ; Avis du Conseil d'Etat n° CE 61.798 du 12 juillet 2024 , doc. parl. n°8330B/02 ; Avis du Conseil d'Etat n° CE 61.070 du 11 juin 2024, doc. parl. n°8031/08

sont accessibles à une autre administration ou font l'objet d'un traitement organisé selon une modalité de connexion, voire d'interconnexion.

Afin d'assurer la conformité de la disposition sous examen aux articles 31 et 37 de la Constitution, il convient, sous peine d'opposition formelle, de compléter cette disposition en précisant notamment la nature des données à caractère personnel échangées, ainsi que la finalité et les conditions dans lesquelles cet échange a lieu ».

48. Par conséquent, à la lumière des développements ci-avant, la CNPD estime que la lecture faite par les auteurs du projet de loi quant à l'article 6.1.e) et 6.3 du RGPD ne peut être retenue.

49. Enfin, l'argumentation des auteurs du projet de loi selon laquelle il resterait « *admissible aux termes de l'article 31 de la Constitution, en particulier au regard du principe de primauté du droit de l'Union européenne rappelé récemment par la [CJUE]* » n'est pas pertinente, alors que l'article 6.3 du RGPD laisse la possibilité au droit de l'Etat membre de régler le fondement du traitement visé au à l'article 6.1.e) du RGPD par une disposition nationale.

En outre, le considérant 41 du RGPD énonce clairement que « *[l]orsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préiudice des obligations prévues en vertu de l'ordre constitutionnel de l'Etat membre concerné* » (mise en évidence ajoutée).

e. *Sur la disposition de droit allemand*

50. Par analogie au droit allemand, les auteurs du projet de loi entendent introduire en droit national une base légale qui s'inspire de la disposition de droit allemand tirée de l'article 3 du Bundesdatenschutzgesetz qui dispose que « *[d]ie Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulassig wenn sie zur Erfüllung der in der Zustandigkeit des Verantwortlichen liegenden Aufgabe oder Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist* ».

51. Au sujet de cette base légale, l'Autorité de protection des données fédérale (der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) estime que :

« *Ergänzend regelt Art. 6 Abs. 3 DSGVO, dass sich in den Fällen der Buchst. c) und e) des Art. 6 Abs. 1 Satz 1 DSGVO die Rechtsgrundlage für die Verarbeitung entweder aus dem Unionsrecht oder dem mitgliedstaatlichen Recht ergeben muss. Im Unionsrecht können sich die Rechtsgrundlagen insbesondere aus EU-Verordnungen ergeben, da sie unmittelbar anwendbar sind. Ein Beispiel ist etwa die Veröffentlichung der Empfänger von Agrarsubventionen auf der Grundlage der entsprechenden EU-Verordnungen. Im mitgliedstaatlichen Recht hat der Gesetzgeber auf Bundesebene mit Blick auf Art. 6 Abs. 3 DSGVO dafür Sorge getragen, dass lückenlose Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes geschaffen worden sind, sodass ein unmittelbarer Rückgriff auf Art. 6 Abs. 1 Satz 1 Buchst. c) und e) nicht notwendig ist. Wie bereits oben dargestellt, wird sich die Rechtsgrundlage für eine Verarbeitung personenbezogener Daten weiterhin aus dem bereichsspezifischen Datenschutzrecht und subsidiar aus § 3 BDSG ergeben* »[30].

52. Selon la compréhension de la Commission nationale, la base de licéité des traitements de données à caractère personnel se trouve toujours ancrée dans les législations spécifiques et uniquement de manière subsidiaire dans la disposition du Bundesdatenschutzgesetz citée par les auteurs du projet de loi. La disposition allemande n'a donc pas vocation à être une base de licéité générale mais subsidiaire.

53. Dès lors, cette disposition semble difficilement transposable en droit interne alors que l'argumentation des auteurs du projet de loi semble différente.

30 Info 6 / Die DSGVO in der Bundesverwaltung

f. *Remarques finales*

54. Enfin, il convient de relever que la base légale envisagée par le projet de loi pourrait être invoquée par les « entités publiques ». Comme développé supra au point 7 du présent avis, la Commission nationale réitère ses inquiétudes en ce qui concerne la potentielle ampleur d'une telle définition.

55. En effet, compte tenu des différentes entités et différents domaines qui seraient couverts par cette définition, les traitements effectués pourraient être très différents et concerner, le cas échéant, des catégories particulières de données.

Ainsi, la CNPD se demande si l'ensemble des établissements publics listés au recueil « établissements publics » pourront invoquer cette base légale. A titre d'exemple, le centre hospitalier de Luxembourg, le centre hospitalier neuropsychiatrique ainsi que les caisses de maladie (CMFEP, CMFEC, Entraide médicale de la SNCFL) qui figurent au recueil pourront-ils invoquer l'article 3 sous examen ?

56. Si la base légale devait être adoptée telle quelle, la Commission nationale craint plus particulièrement que les garanties suffisantes, telles qu'exigées à l'article 9 du RGPD, permettant de protéger efficacement les catégories particulières de données contre les risques d'abus, ne soient pas mises en œuvre.

57. Par conséquent, la CNPD avise négativement l'introduction en droit interne d'une telle disposition. Une telle base légale mènerait indubitablement à créer une insécurité juridique, contrairement à ce qui est avancé par les auteurs du projet de loi qui estiment que cet article aurait pour objet de « *renforcer la sécurité juridique en matière de traitement de données à caractère personnel* ».

B. Sur les informations et données à caractère personnel obtenues par les entités publiques auprès d'une entité publique « *once only* »

1. *Remarques générales*

58. Le Titre IV du projet de loi entend introduire en droit luxembourgeois, le principe du « *once only* ». D'après le commentaire des articles, ce principe a pour objet de « *supprimer certaines démarches administratives pesant lourdement sur les administrés dans le cadre de la présentation d'une demande ou d'une déclaration auprès d'une entité publique* ».

59. Le « once only » entend faciliter le « *traitements par les entités publiques des demandes et déclarations présentées par les administrés, d'une part, en obligeant les entités publiques à échanger entre elles toutes informations, données à caractère personnel ou pièces justificatives nécessaires au traitement desdites demandes ou déclarations et, d'autre part, en permettant aux administrés ayant déjà produit des pièces justificatives auprès d'une entité publique de ne pas être tenus de les produire à nouveau* »[31].

60. Les dispositions du Titre IV du projet de loi érigent en « *obligation légale le traitement de données à caractère personnel nécessaire pour la mise en œuvre* » du « *once only* ». Par ailleurs, ce système reposera « *sur trois caractéristiques essentielles* :

- *La réalisation d'une démarche à l'initiative de l'administré ;*
- *La limitation des informations et des données à caractère personnel échangées à celles strictement nécessaires à la démarche initiée par l'administré ; et*
- *La possibilité, pour les seules entités publiques agissant dans le cadre de leurs missions légales ou réglementaires, et régulièrement habilitées à connanre ces informations et données, de bénéficier de ces échanges* »[32].

---

31 Commentaire des articles ad article 9

32 Commentaire des articles ad article 9

61. En ce qui concerne les problématiques liées à la protection des données qui ont pu être relevées concernant le système du « *once only* », il y a lieu de souligner que le Contrôleur européen de la protection des données (ci-après le « CEPD ») a estimé que pour « *une mise en œuvre réussie du principe « une fois pour toutes » à l'échelle de l'UE (...) ledit principe doit être appliqué conformément aux principes pertinents de la protection des données* »[33].

62. Ainsi, il a notamment estimé que le « *once only* » pouvait potentiellement soulever des problématiques en ce qui concerne la base juridique du traitement, la limitation de la finalité et la minimisation des données et les droits des personnes concernées.

63. Sans reprendre de manière exhaustive l'ensemble des développements formulés par le CEPD, il y a lieu de souligner que ce dernier a notamment recommandé, en ce qui concerne le choix de la base juridique du traitement, que « *dans toute la mesure du possible, le traitement ultérieur de données à caractère personnel basé sur le principe* « *une fois pour toutes* » » devrait être « *spécifié dans un instrument législatif offrant des garanties adéquates pour assurer le respect de la législation en matière de protection des données, notamment le principe de limitation de la finalité et le respect des droits des personnes concernées* »[34].

64. En ce qui concerne le principe de la limitation de la finalité, le CEPD a souligné en ce qui concerne le respect du principe de la limitation des finalités qu'il ne s'agit « *toutefois pas d'une autorisation illimitée d'adopter tout texte législatif général et large permettant de réutiliser sans fin des données à caractère personnel entre différents ministères. Conformément à la Charte des droits fondamentaux, la loi doit respecter certaines exigences pour qu'il puisse être dérogé au principe de la limitation de la finalité* »[35] et a encore estimé que « *conformément aux observations qui précèdent et à moins qu'un motif approprié de limitation visé à l'article 23.1 du RGPD soit disponible ou que les personnes concernées aient donné leur consentement, le principe de limitation de la finalité doit être respecté, même lorsqu'une législation de l'Union ou d'un Etat membre prévoit l'application du principe « une fois pour toutes »* »[36].

65. Enfin, l'autorité de protection des données française a également eu l'occasion de se prononcer à plusieurs reprises sur le principe « *dites-le nous une fois* »[37] à l'occasion de son introduction en droit français. Ainsi, cette dernière a considéré que « *si la simplification des démarches administratives et l'amélioration des relations entre le public et les administrations constituent des objectifs légitimes, la mise en œuvre des échanges de données à caractère personnel dans ce cadre doit être limitée aux données strictement nécessaires et garantir le respect des droits des personnes ainsi que la sécurité et la confidentialité de leurs données à caractère personnel* »[38].

66. Dès lors, les développements ci-après porteront notamment une attention particulière au respect des principes énoncés ci-avant et le projet de loi sera analysé à la lumière des remarques formulées *supra*.

2. *Sur les acteurs visés par le « once only »*

67. La CNPD se permet de réitérer ses vives inquiétudes quant au champ d'application du « *once only* », compte tenu du nombre très important d'acteurs qui seraient visés. En effet, compte tenu de la

33 Avis 8/2017, avis du CEPD sur la proposition de règlement établissant un portail numérique unique et sur le principe « une fois pour toutes », page 9

34 Avis 8/2017, avis du CEPD sur la proposition de règlement établissant un portail numérique unique et sur le principe « une fois pour toutes », page 9

35 Avis 8/2017, avis du CEPD sur la proposition de règlement établissant un portail numérique unique et sur le principe « une fois pour toutes », page 11.

36 Avis 8/2017, avis du CEPD sur la proposition de règlement établissant un portail numérique unique et sur le principe « une fois pour toutes », page 12.

37 L'équivalent français du « once only ».

38 Délibération 2021-035 du 25 mars 2021 délibération n°2022-101 du 6 octobre 2022.

définition des entités publiques par le projet de loi[39], la CNPD s'interroge sur la nécessité de prévoir un tel mécanisme pour des établissements publics et des groupements d'intérêts économiques.

Ainsi, la Commission nationale regrette que le système du « *once only* » ne vise pas que des administrations à l'instar de la France.

3. *Sur le respect du principe de la limitation des finalités et du principe de minimisation des données*

68. En vertu du principe de la limitation des finalités, les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités[40]. Le principe de minimisation des données implique quant à lui que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées[41].

69. En ce qui concerne le principe de la limitation des finalités, comme relevé par le CEPD, le projet de loi doit respecter certaines exigences afin qu'il puisse y être dérogé.

70. Force est de constater que l'article 9.3 du projet de loi énumère les finalités pour lesquelles les données peuvent être traitées dans le cadre de la mise en œuvre du « *once only* ». L'article 9.2 du projet de loi précise que seules les données « nécessaires » peuvent être échangées entre entités publiques.

71. Il convient encore de noter que l'article 9.2 alinéa 2 du projet de loi prévoit, à l'instar des dispositions françaises[42], un échange de données entre entités publiques afin de pouvoir informer les administrés concernant leurs droits et le cas échéant leur octroyer des prestations ou avantages. Il y a lieu de regretter que les raisons pour lesquelles les auteurs aient décidé d'introduire cette finalité en même temps que celle du « *once only* » n'ait pas plus été détaillée par les auteurs du projet de loi.

Aussi, la CNPD aurait préféré à l'instar des dispositions françaises que seules les données strictement nécessaires puissent faire l'objet d'un tel échange[43]. L'ajout du terme « strictement » constitue une garantie supplémentaire afin de respecter le principe précité.

72. L'article 11.3 du projet de loi dispose encore que « *[l]es informations et les données à caractère personnel collectées et échangées en application du présent titre ne peuvent être utilisées ultérieurement à des fins de détection systématique d'une fraude* ». Cependant, le texte en projet précise également que cette interdiction « *ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à procéder auxdites détection et ce pour les détections sur lesquelles porte cette habilitation* ».

73. S'il convient de saluer l'introduction de dispositions qui prévoient que les données ne peuvent pas être utilisées ultérieurement à des fins de détection systématique d'une fraude, l'exception qui est également précisée à l'article 11.3 du projet de loi porte à confusion.

74. Ainsi, comme relevé par l'autorité de protection des données française, si les échanges de données effectués aux fins de répondre à une démarche administrative d'un usager ne posent pas « *de difficulté de principe dès lors que l'atteinte à la vie privée apparait faible* »[44], tel n'est pas le cas si les données utilisées dans le cadre des dispositions de l'article 9.2 sont par la suite utilisées pour des finalités ultérieures différentes, à savoir la détection d'une fraude[45].

La CNPD regrette que les auteurs du projet de loi n'aient pas reproduits les dispositions légales françaises qui prévoient que « *[l]es informations et les données ainsi recueillies et les traitements mis*

---

39 V. points 7 et suivant du présent avis.

40 Article 5.1, b) du RGPD.

41 Article 5.1, c) du RGPD.

42 Article L114-8 II du Code des relations entre le public et l'administration

43 Article L114-8 du Code des relations entre le public et l'administration

44 Délibération CNIL 25 mars 2021

45 Délibération CNIL 25 mars 2021

en œuvre en application du présent article pour procéder à ces échanges ne peuvent être ultérieurement utilisés à d'autres fins, en particulier pour la détection ou pour la sanction d'une fraude »[46].

75. Enfin, les dispositions de l'article 11 du projet de loi peuvent se lire comme une garantie aux principes de limitation de la finalité et de minimisation des données alors que « *[l]'entité publique ne sollicite pas l'échange d'informations et de données à caractère personnel auprès d'une autre entité publique s'il est manifeste qu'elle n'est pas compétente pour traiter la demande ou la déclaration présentée par l'administré* ».

4. *Sur les catégories de données à caractère personnel faisant l'objet d'un échange entre entités publiques et sur leur origine*

76. Il ne ressort pas des dispositions en projet quelles seraient les catégories de données à caractère personnel qui pourraient faire l'objet de ces échanges de données « à grande échelle » en application du système « *once only* ».

77. Cependant, il y a lieu de noter que pour chaque demande effectuée par l'administré auprès d'une entité publique, celle-ci l'informera des données à caractère personnel nécessaires au traitement de sa demande et également les coordonnées de l'entité publique d'où proviennent les données à caractère personnel[47].

78. De plus, il est également précisé à l'article 11.6 du projet de loi qu'un « *règlement grand-ducal détermine les informations ou données à caractère personnel, qui en raison de leur nature, ne peuvent faire l'objet de ces échanges entre entités publiques* ». La CNPD déplore qu'un tel projet de règlement grand-ducal ne lui ait pas été transmis concomitamment à sa saisine dans le cadre de ce projet de loi.

Or, de telles informations auraient été les bienvenues alors qu'elle se demande si des catégories particulières de données seraient échangées ou si des données visées à l'article 10 du RGPD[48] seraient échangées. Ce d'autant plus alors que des garanties appropriées doivent être mises en place lors du traitement de telles données.

79. Par ailleurs, à l'instar des dispositions françaises les auteurs du projet de loi ne pourraient-ils pas d'ores et déjà préciser que les données qui « *en raison de leur nature, notamment parce qu'elles touchent au secret médical et au secret de la défense nationale, ne peuvent faire l'objet de ces échanges entre administrations* » ?

80. De même, il convient de regretter qu'il ne soit pas précisé dans le texte en projet qu'une entité publique ne peut se procurer des documents contenant des données à caractère personnel qu'auprès des administrations détentrices des données d'origine en cause et non pas auprès d'une entité qui est seulement un destinataire des documents.

81. A ce titre, la CNPD regrette que le texte en projet ne s'inspire pas des dispositions françaises visées à l'article D114-9-1 du Code des relations entre le public et l'administration qui encadre « l'origine des données » par la colonne nommée « *Administrations chargées de la mise à disposition* ».

Pour une meilleure compréhension de ses propos la Commission nationale se permet de reproduire partiellement le texte légal français précité :

---

46 L114-8 II Code des relations entre le public et l'administration

47 Article 11.2 du projet de loi

48 Il s'agit des traitements de données à caractère personnel relatives aux condamnations pénales et aux infractions.

Personnes concernées	*Types d'informations ou de données*	*Administrations chargées de la mise à disposition*
Particuliers	Situation du foyer fiscal	Direction générale des finances publiques
Particuliers	Droits sociaux, revenus et prestations ; Situation de la famille	Organismes de protection sociale et organismes mentionnés au premier alinéa de l'article L. 133-5 du code de la sécurité sociale, au I de l'article 3 de l'ordonnance n° 77-1102 du 26 septembre 1977 et au I de l'article 19 de l'ordonnance n° 96-1122 du 20 décembre 1996
Particuliers	Situation de l'enfant au regard de l'obligation scolaire	Ministère chargé de l'éducation nationale

Son homologue français avait notamment relevé que cette liste, partiellement reproduite ci-dessus, permet « *d'établir des administrations de référence pour la mise à disposition de chaque donnée recherchée par une administration tierce, permettant ainsi de s'assurer que la donnée est bien collectée directement auprès de l'administration détentrice de la donnée d'origine, fiable et unique, et non auprès de tout autre administration qui en disposerait également. Elle estime que cette mesure est de nature à éviter des erreurs dans les données échangées et la propagation de données inexactes ou non actualisées auprès des administrations* ».

Par conséquent, la CNPD estime nécessaire et primordial que des dispositions similaires soient introduites expressément dans le texte en projet.

82. Ainsi, la CNPD avise négativement les dispositions prévues à l'article 10 du projet de loi qui prévoient qu'il revient aux administrés pour chaque démarche entreprise auprès d'une « entité publique » de « *certifier l'exactitude des informations et des données à caractère personnel* » obtenues à travers le système du « *once only* ».

83. Cet article prévoit encore que si les données s'avèrent inexactes l'administré est tenu de les rectifier auprès « *de l'entité publique d'où elles proviennent et de communiquer les informations et les données à caractère personnel rectifiées à l'entité publique en charge du traitement de la demande ou de la déclaration présentée par l'administré* ».

84. En effet, de telles dispositions sont contraires à l'esprit du « *once only* » qui est de faciliter les démarches des administrés. Par ailleurs, en vertu de l'article 16 du RGPD, l'administré dispose d'ores et déjà d'un droit de rectification.

5. *Sur le droit des personnes concernées*

85. La CNPD tient à rappeler l'importance du respect des droits des personnes concernées en matière de protection de données dans le cadre de la mise en œuvre du principe du « *once only* ». De même qu'elle tient à souligner l'importance du principe de transparence dans le contexte précité[49].

86. Il y a tout particulièrement lieu d'attirer l'attention des auteurs du projet sur le fait que chaque entité qui échangera des données en vertu des dispositions sous avis devra accorder une attention particulière aux modalités de délivrance de l'ensemble des informations visées à l'article 13 du RGPD, afin de s'assurer que la transparence peut ainsi être garantie.

La CNPD rappelle également l'importance de s'assurer que l'information des personnes concernées soit complète et de qualité au regard des exigences posées par l'article 14 du RGPD. De plus, elle recommande notamment que les informations soient transmises avant chaque étape de la démarche administrative initiée par une personne concernée. En outre, en cas d'exercice du droit d'opposition par la personne concernée, cette information devrait aussi indiquer les modalités alternatives pour effectuer la démarche entreprise sans bénéficier du dispositif du « *once only* ».

49 Article 5.1, a) du RGPD ainsi que le chapitre III, section 1 du RGPD

87. Par ailleurs, chacun des responsables du traitement devra s'assurer de l'effectivité des droits des personnes concernées, tel que le droit d'opposition, de rectification des données, ainsi que le droit d'accès.

Ainsi, la CNPD estime essentiel qu'une traçabilité précise des échanges soit assurée, permettant l'exercice du droit d'accès sur les données. Cette traçabilité doit permettre de retracer les échanges qui ont eu lieu, entre quelles administrations, à quel moment. A cet égard, elle recommande la mise en place de moyens techniques qui permettraient à chaque administré de prendre connaissance, de manière simple et consolidée, de l'ensemble des échanges de données le concernant.

88. Elle se demande également si à l'instar des dispositions prévues à l'article 38 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, il ne serait pas possible de permettre aux personnes concernées d'obtenir sur MyGuichet.lu une liste des entités publiques ayant eu recours au système du « *once only* » liée aux démarches entreprises par l'administré ou aux démarches proactives effectuées par les entités publiques, le cas échéant.

6. *Sur les mesures techniques et organisationnelles*

89. Conformément au principe d'intégrité et de confidentialité[50], les données personnelles doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel. Le responsable du traitement doit assurer l'intégrité et la confidentialité des données à l'aide de mesures techniques et organisationnelles appropriées, notamment contre un traitement non-autorisé ou illégal et contre la perte, destruction ou altération accidentelle des données.

90. La CNPD estime que le respect de ce principe est primordial dans le cadre de la mise en œuvre du système « *once only* » et regrette donc que le projet de loi reste muet à ce sujet. Ainsi, il est primordial que l'échange de données entre les administrés et les entités publiques d'une part et l'échange de données entre les entités publiques entre elles d'autre part, garantissent la sécurité et la confidentialité des données personnelles des personnes concernées[51].

91. Il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait que les mesures techniques et organisationnelles devraient comporter des moyens d'authentification forte tant pour les échanges entre administrés et entités publiques que pour les échanges entre entités publiques. De même, ces mesures devraient permettre la traçabilité des échanges, ainsi qu'une journalisation des opérations d'échanges de données.

92. En outre ces mesures techniques devraient permettre d'éviter tout accès illicite à des données personnelles et assurer le principe de minimisation des données.

93. Par ailleurs, il convient de noter qu'en France des dispositions spécifiques relatives aux mesures techniques et organisationnelles sont prévues afin d'encadrer des systèmes similaires à celui prévu par le texte sous avis[52].

Ces dispositions légales françaises prévoient également des durées de conservation spécifiques en ce qui concerne les données relatives à la traçabilité qui diffèrent selon que les données sont échangées dans le cadre du système « *once only* » ou dans le cadre du système permettant d'échanger les données pour informer proactivement un administré de son droit au bénéfice éventuel d'une prestation ou d'un droit[53]. De telles durées de conservation ne devraient-elles pas être prévues également dans le projet de loi ?

---

50 L'article 5.1.f) du RGPD les données à caractère personnel doivent être traitées « *de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)* », v. également article 32 du RGPD.

51 Délibération de la CNIL n°2021-0035 du 25 mars 2021.

52 V. articles R114-9-6 et suiv. du Code des relations entre le public et l'administration.

53 Article R114-9-7 du Code des relations entre le public et l'administration.

94. Enfin, conformément à l'article 32.1, d) du RGPD, l'efficacité de ces mesures devra être régulièrement évaluée pour assurer la sécurité des traitements.

95. Par conséquent, en l'absence de précisions en ce qui concerne le cadre technique et organisationnel, la Commission nationale estime que des précisions à ce sujet devraient être intégrées dans le texte du projet de loi.

7. *Sur les durées de conservation*

96. En vertu du principe de limitation de la conservation, les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées[54].

97. Il y a lieu de noter que les documents échangés en vertu du système « *once only* » devront être conservés en fonction des finalités déterminées par chacune des entités pour lesquelles ces documents sont traités.

98. Toutefois, il est intéressant de noter qu'en France, des durées de conservation sont spécifiées dans le Code des relations entre le public et l'administration.

Ainsi, en ce qui concerne plus particulièrement les échanges de données entre administrations « *pour informer les personnes sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou des actes réglementaires et pour leur attribuer éventuellement lesdits prestations ou avantages* »[55], il est prévu qu'« *[u]n décret en Conseil d'Etat, pris après un avis motivé de la Commission nationale de l'informatique et des libertés rendu public, détermine les conditions d'application du présent II, notamment la durée et les modalités de conservation des informations et des données collectées à cette occasion* ».

En l'absence de précision à ce sujet dans le texte en projet, il est regrettable qu'aucune précision à ce sujet ne figure dans le projet de loi.

8. *Sur l'opposabilité du secret professionnel*

99. Il y a lieu de saluer les auteurs du projet de loi pour avoir expressément prévu que les entités publiques destinataires des informations et des données ne peuvent se voir opposer le secret professionnel dès lors qu'elles sont dans le cadre de leurs missions légales, habilitées à avoir connaissance des informations ou des données à caractère personne[56].

9. *Sur les modalités de fonctionnement du « once only »*

100. L'article 12 du projet de loi fait peser sur les entités publiques l'obligation d'identifier dans les meilleurs délais les informations et les données à caractère personnel qu'elles pourraient obtenir auprès d'une autre entité publique tant dans le cadre des démarches qui pourraient être effectuées à l'initiative de l'administré tant que pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions légales en vue de leur attribuer lesdits prestations ou avantages.

101. La CNPD prend note du choix des auteurs du projet de loi de faire peser sur les entités publiques cette obligation de recensement des données à caractère personnel qui pourraient être obtenues auprès d'autres entités publiques. Au vu de l'ampleur des échanges projetés et du nombre d'acteurs qui seraient impliqués, elle regrette que les catégories de données ne soient pas définies dans le projet de loi.

102. Par ailleurs, les dispositions de l'article 12.2 du projet de loi prévoient que le ministre ayant la digitalisation dans ses attributions (ci-après le « ministre ») puisse se voir communiquer une copie de l'information « *relative à la disponibilité des informations et données* », telles que prévue par

54 Article 5.1, e) du RGPD.

55 Article L114-8, II du Code des relations entre le public et l'administration.

56 Article 11.5 du projet de loi

l'article 12.1, « *afin de permettre à ce dernier de cartographier les flux des échanges « once only », notamment pour l'identification d'éventuelles sources authentiques* »[57].

En l'absence de précisions en ce qui concerne le rôle que jouerait le ministre, il y a lieu de s'interroger sur les raisons pour lesquelles ce dernier devrait cartographier les flux des échanges « *once only* » ainsi que les raisons pour lesquelles il lui serait nécessaire d'identifier des sources authentiques. De même qu'il convient encore de se demander ce que recouvre le terme « sources authentiques », en l'absence de toute définition dans le texte sous avis.

103. L'article 13 du projet de loi crée dans le chef des entités publiques une obligation « *de formaliser chaque type d'échanges d'informations et de données à caractère personnel visé par l'obligation « once only » par le biais d'un protocole contenant tous les éléments obligatoires cités par la disposition sous examen* »[58]. Ce protocole a par la suite vocation à être publié par l'Autorité des données par voie électronique[59].

La CNPD salue une telle publication qui œuvre pour une meilleure transparence des échanges de données qui seraient effectués en vertu des dispositions sous avis. Les auteurs du projet de loi précisent effectivement dans le commentaire des articles que « *la mise en place d'une infrastructure standardisée de publication des protocoles et d'un pilotage centralisé au niveau de l'Autorité des données permettent en effet de garantir de manière efficace la transparence administrative dans le cadre de la mise en œuvre du principe « once only ». Ainsi, les administrés peuvent consulter toutes les informations sur les échanges d'informations et de données à caractère personnel effectués par les entités publiques auprès d'une seule source centralisé* ».

104. L'article 13.1 du projet de loi énumère l'ensemble des éléments qui devraient figurer dans le protocole précité. La Commission nationale regrette que la base de licéité du traitement ne soit pas reprise dans le protocole contrairement à la législation française qui le prévoit.

105. Enfin, l'article 14 prévoit la tenue par l'Autorité des données d'un registre de tous les protocoles qui lui sont transmis pour publication. Il est également prévu que le ministre puisse avoir accès à ce registre « *en vue d'identifier les sources authentiques d'informations et de données* ». Des précisions à ce sujet devraient être apportées par les auteurs du projet de loi. La CNPD renvoie à ses commentaires formulés au point 102 du présent avis.

10. *Remarques finales*

106. Compte tenu des dispositions légales nationales existantes qui pourraient s'appliquer en parallèle de la mise en œuvre de ce système, la CNPD souhaite faire part de ses interrogations ou problématiques qu'elle a pu identifier.

107. Elle s'interroge notamment sur l'articulation de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques avec le texte en projet. En effet, bien que l'utilisation du numéro d'identification (dit « matricule ») ne soit pas expressément visée par le projet de loi, la Commission nationale voit difficilement comment la mise en œuvre du « *once only* » pourrait fonctionner sans l'utilisation du matricule des administrés.

De manière générale, elle constate la tendance actuelle consistant à utiliser le matricule pour la mise en œuvre des démarches électroniques entre un administré et une administration. Bien que la CNPD puisse comprendre une telle utilisation, ne faudrait-il pas adapter la loi relative à l'identification des personnes physiques en ce sens ? En effet, il convient de se demander compte tenu de la multiplication des démarches en ligne, s'il ne serait désormais pas possible de tenir un historique des « traces administratives » d'un administré ?

108. En outre, l'autre problématique identifiée par la Commission nationale est relative à la multitude de bases de licéité des traitements de données qui seraient applicables en sus du projet de loi. A titre

57 V. ad article 12

58 V. ad article 13

59 Article 13.3 du projet de loi

d'exemple, comment les dispositions du projet de loi s'articuleront avec les dispositions du règlement grand-ducal modifié du 23 juillet 2016 fixant la liste des administrations et personnes morales de droit public pouvant demander un bulletin n°2 ou n°3 du casier judiciaire avec l'accord écrit ou électronique de la personne concernée ?

Ainsi, il convient de regretter que les auteurs du projet de loi n'aient pas précisé dans le commentaire des articles, ce qu'il adviendrait lorsqu'une autre base de licéité s'appliquerait le cas échant en ce qui concerne l'obtention de données personnelles par une entité publique.

109. Enfin, il ressort du rapport d'activité 2015 du CTIE que « *MyGuichet est la plateforme interactive sécurisée, intégrée à Guichet.lu, qui permet aux citoyens et aux entreprises d'effectuer des démarches administratives par la voie électronique auprès des administrations compétentes.*

Ainsi, l'utilisateur remplit son formulaire en ligne, le signe de manière électronique, y joint ses pièces justificatives puis transmet le tout via MyGuichet. Les principales fonctionnalités offertes par MyGuichet sont :

- *les assistants de services (démarches) qui permettent un dialogue simplifié ;*
- *un espace de stockage pour les documents ;*
- *un module de signature électronique ;*
- *un système de messagerie qui permet entre autre un retour électronique ;*
- *le suivi des démarches.*

MyGuichet permet également de consulter des sources exactes. A travers les sources exactes l'utilisateur peut consulter les données détenues par l'Etat le concernant.

Les sources exactes permettent :

- *au Gouvernement d'appliquer le principe de transparence par rapport aux données stockées et la possibilité de présenter qui a consulté ces données ;*
- *la possibilité d'y adjoindre des démarches en vue de rectifier les données et donc d'augmenter la qualité de celles-ci ;*
- *d'appliquer le principe du « once only » puisque les sources exactes peuvent servir par la suite au pré remplissage de démarches administratives ;*
- *de rationaliser les efforts des administrations qui désirent publier des données personnelles* »[60].

La Commission nationale comprend dès lors que cette plateforme aurait vocation à servir de canal de communication sécurisé entre les citoyens et les entités publiques dans le cadre de la mise en œuvre du « *once only* ». En effet, il ressort de l'article 2, m) de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat que le « *centre a pour mission la mise en place et l'exploitation des plateformes d'échange avec les citoyens et les entreprises* ». Cependant, elle se demande s'il ne conviendrait pas d'encadrer plus précisément l'utilisation de MyGuichet alors que cette plateforme semble être de plus en plus plébiscitée dans le cadre d'échange entre citoyens et administrations.

En effet, elle constate par exemple que dans le cadre du projet de loi n°8089 relatif à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique ainsi que du projet de règlement grand-ducal fixant certaines modalités d'application de la loi relative à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique, les auteurs desdits textes ont détaillés les conditions et modalités d'utilisation de la plateforme sécurisée[61].

---

60 Disponible sous le lien suivant :
https://gouvernement.lu/dam-assets/fr/publications/rapport-activite/minist-fonction-publique-reforme-administrative/centre-des-technologies-de-l-information-de-l-etat-ctie/2015-rapport-activite-ctie/2015-rapport-activite-ctie.pdf

61 V. notamment article 5 du projet de loi

C. Sur le traitement ultérieur de données à caractère personnel par les entités publiques

1. *Remarques liminaires*

110. L'article 15 du projet de loi intitulé « Finalités du traitement ultérieur autorisées et licéité du traitement », autorise le « *traitement ultérieur de données à caractère personnel par des entités publiques s'il est réalisé pour l'une ou plusieurs des finalités énoncées à l'article 15, sous réserve que les conditions énoncées au titre V de la loi soient remplies* ».

Les auteurs du projet de loi précisent dans le commentaire des articles encore que ces dispositions permettent aux entités publiques d'effectuer un traitement ultérieur de données « *pour des finalités déterminées par le texte, sans devoir réaliser le test de compatibilité des finalités conformément aux critères énoncés à l'article 6.4 du [RGPD]* »[62]. Ces derniers ajoutent encore que cette disposition permettant la mise à disposition des données que leur partage ainsi que le traitement ultérieur qui serait mis en œuvre par les entités publiques.

111. Il y a lieu de rappeler que le considérant 50 du RGPD énonce que « *[l]orsque […] le traitement est fondé sur […] le droit d'un Etat membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir, en particulier, d'importants objectifs d'intérêt public général, le responsable du traitement devrait être autorisé à effectuer un traitement ultérieur des données à caractère personnel indépendamment de la compatibilité des finalités* ». En effet, les conditions de l'article 6.4 du RGPD ne s'appliquent notamment pas lorsque le traitement se fonde sur le droit d'un Etat membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23.1 du RGPD.

112. Les auteurs du projet de loi estiment dans le commentaire des articles que « *l'allégement de la charge administrative sur les personnes physiques ou les organisations, l'efficacité accrue des procédures administratives et l'économie de temps et de ressources, constituent sans nul doute des objectifs d'intérêt public valables* ». Ainsi, selon les auteurs du projet de loi les dispositions du projet de loi, lues à la lumière de l'article 23.1 du RGPD, poursuivraient des objectifs d'intérêt public.

Toutefois, la Commission nationale ne souscrit pas à une telle analyse, alors qu'elle partage la position du CEPD qui dans son avis sur la proposition de règlement établissant un portail numérique unique et sur le principe « une fois pour toutes », a estimé que « *[l]'allégement de la charge administrative sur les personnes physiques ou les organisations, l'efficacité accrue des procédures administratives et l'économie de temps et de ressources, qui sont souvent les objectifs premiers des applications du principe « une fois pour toutes » constituent sans nul doute des objectifs d'intérêt public valables. Néanmoins, ils ne sont pas spécifiquement mentionnés dans la liste visée à l'article 23, paragraphe 1, et ne constituent pas en soi un motif licite permettant de restreindre la portée du principe de limitation de la finalité pour atteindre ces objectifs. Cela étant, comme indiqué plus haut, on ne peut exclure que dans certains cas spécifiques, l'un ou l'autre des fondements juridiques des limitations visées à l'article 23, paragraphe 1, point d), puisse être approprié* ».

Par ailleurs, en ce qui concerne les traitements ultérieurs à des fins de recherche scientifique ou à des fins statistiques, selon le considérant 50 du RGPD de tels traitements devraient être considérés comme des opérations de traitement compatibles et licites.

En tout état de cause, force est de constater que les articles 63 et suivants de la loi du 1er août 2018 prévoient d'ores et déjà d'encadrer de tels traitements. Sur ce point il est encore renvoyé au point 115 du présent avis.

2. *Un enchevêtrement de bases légales*

113. Les auteurs du projet de loi précisent dans le commentaire des articles que le système envisagé « *s'applique sans préjudice de la possibilité pour les entités publiques d'effectuer des traitements ultérieurs de données à caractère personnel sur base de leur compatibilité ou de procéder à des traitements ultérieurs de données à caractère personnel sur base d'une disposition spécifique du droit de*

62 V. Ad article 15.

l'Union ou du droit national applicable, telles que l'article 4, paragraphe 4 de la loi du 3 décembre 2014 ayant pour objet l'organisation des centres de recherches publics ou l'article 423, point 4° du Code de la sécurité sociale ».

114. La CNPD relève que plusieurs textes légaux sont susceptibles de s'appliquer, outre ceux déjà précisés ci-avant par les auteurs du projet de loi.

115. En effet, comment les dispositions sous avis s'articulent avec les dispositions de l'article 89 du RGPD ainsi qu'avec les dispositions du Chapitre 2 intitulé « Traitement à des fins de recherche scientifique ou historique ou à des fins statistiques » de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données » ?

De même, dans une moindre mesure, il convient également de s'interroger sur l'articulation des dispositions du projet de loi avec celles de la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public.

116. Enfin, dans ce contexte, la Commission nationale se demande si l'ajout d'un nouveau texte légal, tel que celui projeté, ne va pas complexifier la tâche des entités publiques et nuire à la sécurité juridique.

3. *Sur les traitements ultérieurs de données pour les finalités énumérées à l'article 15 du projet de loi*

a. *L'article 15 du projet de loi*

117. Les finalités visées par l'article 15 du projet de loi sont les suivantes :

- l'analyse statistique ;
- les activités d'éducation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;
- la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;
- l'évaluation et la planification des politiques envisagées ou planifiées par le Gouvernement et approuvées par décision du Gouvernement en conseil, ou en ce qui concerne les communes, envisagées ou planifiées par le Conseil communal ;
- lorsque la mise en œuvre d'un accord international requiert la communication d'informations ou lorsque le traitement ultérieur des données à caractère personnel permet de répondre aux demandes d'informations officielles provenant de gouvernements étrangers ou d'organisations internationales approuvées par décision du Gouvernement en conseil ;
- les activités de développement, d'évaluation, de démonstration, de sécurité et d'innovation de dispositifs ou de services ;
- la formation, le test et l'évaluation d'algorithmes, y compris dans les dispositifs, les systèmes d'intelligence artificielle et les applications numérique.

118. En l'absence de précisions sur les catégories de données qui seraient visées ainsi que les acteurs qui pourraient effectuer des traitements[63] sur base de cet article 15, la Commission nationale n'est pas en mesure d'apprécier si l'ensemble des principes visés à l'article 5 du RGPD seraient en mesure d'être respectés.

Toutefois, elle se demande s'il n'aurait pas été possible d'être plus précis alors que le considérant 50 du RGPD énonce que « *[s]i le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, le droit de l'Union ou le droit d'un Etat membre peut déterminer et préciser les missions et les finalités pour lesquelles le traitement ultérieur devrait être considéré comme compatible et licite* »[64].

---

63 Il est renvoyé aux points 7 et suiv. du présent avis sur la définition d'entité publique.

64 Il est renvoyé *infra* au point 112 du présent avis.

119. Par ailleurs, la Commission nationale note que les auteurs du projet de loi entendent introduire une base de licéité en ce qui concerne les traitements effectués par les entités publiques à des fins d'intelligence artificielle, notamment en ce qui concerne la création d'algorithme. A défaut de précisions dans le projet de loi, la Commission nationale n'est toutefois pas en mesure d'apprécier si un traitement pour une telle finalité respecte les principes généraux du RGPD.

120. En tout état de cause, il y a lieu de souligner que le considérant 50 du RGPD énonce que « *l'application des principes énoncés dans le [RGPD] et, en particulier, au sujet de ces autres finalités et de ses droits, y compris le droit de s'opposer au traitement, devraient être assurées* »[65].

b. *Les dispositions légales étrangères*

121. Les auteurs du projet de loi indiquent dans le commentaire des articles s'inspirer de dispositions légales allemandes ainsi que finlandaises similaires.

122. Or, il convient de relever que les dispositions légales allemandes diffèrent grandement des dispositions légales envisagées de sorte que le parallèle effectué par les auteurs du projet de loi ne s'avère pas pertinent en l'espèce.

En effet, les dispositions du § 23 du BDSG visent le traitement ultérieur de données soit dans l'intérêt manifeste de la personne concernée, ou justifié par des motifs impérieux d'intérêt public. Ainsi, par exemple en ce qui concerne le traitement ultérieur de données dans l'intérêt manifeste de la personne concernée, il ne doit pas y avoir de raisons de penser que la personne concernée refuserait de donner son consentement si elle avait connaissance du nouvel usage de ces données. En outre, les finalités visées par lesdites dispositions diffèrent encore de celles énumérées par le projet de loi.

Ainsi, l'analogie avec le droit allemand ne fait pas de sens aux yeux de la CNPD.

123. En ce qui concerne les dispositions finlandaises citées par les auteurs du projet de loi, la même analyse est retenue par la Commission nationale alors que le champ d'application de la législation finlandaise a un champ d'application beaucoup plus restreint qui se limite notamment à la réutilisation de données dans le contexte de la santé[66].

4. *Sur les garanties appropriées*

124. L'article 16 paragraphes 1 et 2 du projet de loi conditionne la réutilisation des données pour des finalités ultérieures différentes à l'anonymisation sinon à la pseudonymisation des données. La Commission nationale comprend que ces données doivent être préalablement anonymisées ou pseudonymisées par l'entité détentrice des données.

Il est encore précisé que lorsque le « *traitement ultérieur de données à caractère pseudonymisées ne permet pas d'atteindre la finalité poursuivie »,* les données non anonymisées et non pseudonymisées pourraient être traitées ultérieurement pour les finalités énoncées à l'article 15 du projet de loi *« dans les limites du strict nécessaire* »[67]

Il convient de regretter que le commentaire des articles ne précise pas quelles situations seraient visées par les « *limites du strict nécessaire* ». En tout état de cause, il conviendrait autant que possible que des données non anonymisées et non pseudonymisées ne soient pas utilisées pour des traitements de données ultérieurs pour des finalités différentes de celles initiales pour lesquelles elles sont traitées.

Il y a lieu de saluer que les garanties visées à l'article 35 du projet de loi doivent être mises en œuvre dans le cadre des traitements ultérieurs de données visées à l'article 15 du projet de loi. En outre, l'obligation d'introduire une demande à formuler devant l'Autorité des données en ce qui concerne le traitement ultérieur des données[68], semble également constituer une garantie appropriée. La CNPD reviendra supra plus en détail sur ce point.

---

65 V. points 146 et suiv. du présent avis.

66 Disponible sous le lien suivant : Muistiopohja.

67 V. article 16.3 du RGPD

68 V. articles 27 et suiv. du projet de loi.

125. De même qu'il convient encore de saluer que toute réidentification de l'identité de toute personne concernée à laquelle se rapporte les données est interdite par le projet de loi aux entités publiques.

126. Par ailleurs, la CNPD prend note que le terme anonymisation est défini par l'article 2.2 du projet de loi. Les auteurs du projet de loi indiquent que « *pour des raisons de sécurité juridique, une définition en droit interne du terme « anonymisation »* est prévue. Ils précisent encore que cette définition tient compte de la neutralité technologique.

Cependant, la CNPD se demande si l'introduction en droit interne de cette définition ne constitue pas un risque ultérieur de se voir enfermer dans cette définition en cas d'évolution technique ou jurisprudentielle sur la question. Elle préfèrerait dès lors que cette définition soit omise du texte en projet.

5. *Sur le traitement ultérieur de données à caractère personnel par la même entité publique*

127. Il convient de saluer que l'article 17 prévoit des garanties supplémentaires en ce qui concerne les traitements ultérieurs de données visées aux articles 9 et 10 du RGPD. En effet, conformément à l'article 17.2 du projet de loi, les données à caractère personnel visées aux articles précitées ne peuvent pas être traitées de manière non-anonymisées ou non-pseudonymisées.

6. *Sur le traitement ultérieur de données à caractère personnel par une autre entité publique ou par plusieurs entités publiques*

128. Il y a lieu de noter que l'article 18 du projet de loi prévoit des conditions spécifiques aux traitements ultérieurs de données à caractère personnel par une autre entité publique ou par plusieurs entités publiques. La CNPD comprend que les dispositions dudit article encadrant une telle réutilisation sont plus strictes. Elle tient à saluer les auteurs du projet de loi pour avoir prévu un régime plus strict alors que le traitement ultérieur par une autre entité publique ou par plusieurs entités publiques est d'une plus grande ampleur.

7. *Sur les modalités applicables au traitement ultérieur des données à caractère personnel*

129. Les articles 27, 29 et 31 conditionnent le traitement ultérieur de données à une demande à introduire devant l'Autorité des données, qui autorisera ou non le traitement. L'article 27 énumère les informations à fournir lors de l'introduction d'une telle demande.

130. L'article 32 précise encore le contrôle qui pourrait être effectué par l'Autorité des données quant à la demande pour un traitement ultérieur de données à caractère personnel formulée par une entité publique.

Enfin l'article 34 prévoit que les autorisations délivrées dans ce contexte par l'Autorité des données figurent dans le registre public des autorisations tenu par cette dernière. Il convient de saluer cette publication d'un point de vue du principe de la transparence[69].

131. En outre, et comme relevé tout au long de cet avis, la CNPD émet de vives inquiétudes quant à l'articulation de ses pouvoirs de sanction au sens de l'article 58 du RGPD avec les pouvoirs octroyés par le projet de loi à l'Autorité des données[70].

Elle se demande plus particulièrement si les dispositions légales envisagées ne vont pas accentuer un sentiment de confusion dans le chef des responsables du traitement entre les pouvoirs et missions de l'Autorité des données avec les pouvoirs et missions de la CNPD[71]. Ainsi, les procédures envisagées par le projet de loi ne vont-elles pas entraîner une insécurité juridique ?

*

69 Il est renvoyé également aux points 141 et suiv. du présent avis.

70 V. points 15 à 18 et points 140 et suiv. du présent avis.

71 V. points 12 et suivant du présent avis.

IV. SUR LE VOLET EUROPEEN

A. Sur l'accès et réutilisation des données détenues par des organismes du secteur public par des réutilisateurs de données

D'après le commentaire des articles, le titre VI du projet de loi met en œuvre le chapitre II du règlement 2022/868 concernant l'accès et la réutilisation des données détenues par des organismes du secteur public par des réutilisateurs de données. Néanmoins, la CNPD constate que ledit chapitre II du règlement 2022/868 est uniquement intitulé « *Réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public* », tandis que le titre VI du projet de loi ne mentionne pas uniquement la réutilisation, mais aussi l'accès aux « *données détenues par des organismes du secteur public par les réutilisateurs de données* ».

L'article 2 point 2) du règlement 2022/868 définit dans ce contexte le terme « réutilisation » comme « *l'utilisation, par des personnes physiques ou morales, de données détenues par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les données ont été produites, à l'exception de l'échange de données entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public.* ». L'article 2 point 11) dudit règlement quant à lui contient une définition du terme « accès » visant « *l'utilisation de données conformément à des exigences techniques, juridiques ou organisationnelles particulières, sans que cela implique nécessairement la transmission ou le téléchargement de données.* ».

B. Sur les dispositions générales

132. La Commission nationale note que l'article 19 du projet de loi sur les catégories de données protégées disponibles à l'accès et à la réutilisation exclut de son champ d'application non seulement les données de l'article 3, paragraphe (2) du règlement 2022/868[72], mais également les « *cas visés par les autres titres de la présente loi.* ». En d'autres termes et comme le mentionnent d'ailleurs aussi les auteurs du projet de loi dans le commentaire des articles, les entités publiques ne sont pas en droit de solliciter un accès et une réutilisation de données sur base du Titre VI du projet de loi, alors qu'elles sont déjà visées par le traitement ultérieur de données à caractère personnel encadré par le titre V du projet de loi.

133. Dès lors, les entités publiques sont uniquement concernées par le titre VI du projet de loi en tant que détenteur de données à caractère personnel et, le cas échéant, par la mise à disposition desdites données dans ce contexte. De même, elle comprend sur base de ce qui précède que les « réutilisateurs » demandant un accès et une réutilisation de données détenues par des organismes du secteur public, peuvent seulement être des personnes physiques ou morales du secteur privé, alors que les entités publiques doivent se baser sur le titre V du projet de loi sur le traitement ultérieur de données.

134. Par ailleurs, la CNPD constate que sur base de l'article 21 du projet de loi, le principe est que les données à caractère personnel détenues par des organismes du secteur public doivent être anonymisées préalablement à l'accès et à la réutilisation par le réutilisateur de données. Ce n'est que si ledit accès et la réutilisation de données anonymisées ne permet pas d'atteindre la finalité poursuivie que l'accès et à la réutilisation de données à caractère personnel préalablement pseudonymisées est possible.

Le commentaire des articles précise dans ce contexte qu'« *il peut être fait usage de données à caractère personnel préalablement pseudonymisées, à condition de démontrer que la réutilisation de données anonymisées ne permet pas d'atteindre les finalités poursuivies.* » Elle estime qu'il revient au réutilisateur de procéder à cette analyse de la nécessité d'accéder à des données pseudonymisées et que la CNPD pourrait, le cas échéant, contrôler si le principe de minimisation des données prévu par l'article 5, paragraphe (1), lettre c) du RGPD a été respecté dans ce contexte.

---

72 L'article 3 paragraphe (2) du règlement 2022/868 prévoit par exemple que le chapitre II sur la réutilisation ne s'applique pas aux données détenues par des entreprises publiques ou encore aux données détenues par des radiodiffuseurs de service public ou par des établissements culturels et des établissements d'enseignement.

C. Sur les conditions applicables à la réutilisation de données à caractère personnel

135. L'article 22 du projet de loi contient les conditions applicables à l'accès et la réutilisation de données à caractère personnel par des réutilisateurs de données qui sont notamment contrôlées par l'Autorité des données lorsqu'elle analyse la demande de réutilisation conformément à l'article 31 du projet de loi. La CNPD tient à renvoyer dans ce contexte notamment aux points 17 et 18 du présent avis afin d'insister que dès qu'un réutilisateur est à considérer comme responsable du traitement ou comme sous-traitant au sens de l'article 4, points 7 et 8) du RGPD, la CNPD est compétente pour vérifier l'application et le respect de l'intégralité des dispositions du RGPD et de la loi du 1er août 2018. Ses pouvoirs de contrôle et de sanctions ne dépendent pas de l'analyse des conditions précitées par l'Autorité des données.

136. L'article 23 du projet de loi quant à lui contient les conditions applicables à l'accès et la réutilisation de données à caractère non personnel. A la différence du traitement ultérieur par des entités publiques qui ne concerne que des données à caractère personnel, l'accès et la réutilisation peut dès lors porter aussi sur des données non personnelles.

La CNPD accueille favorablement à cet égard que l'article 24 du projet de loi prévoit qu'en cas d'accès et de réutilisation de données à caractère personnel et non personnel, toutes les conditions des articles 19 à 23 du projet de loi sont à respecter.

D. Sur les modalités applicables à l'accès et à la réutilisation de données par des réutilisateurs de données

137. L'article 25 du projet de loi prévoit que les dispositions du titre VII couvrent tant les cas de figure visés au titre V (traitement ultérieur de données à caractère personnel par les entités publiques)[73] que ceux du titre VI du projet de loi sous examen (accès et réutilisation de données détenues par des organismes du secteur public) et qui sont soumis à autorisation de l'Autorité des données.

138. Par ailleurs, l'article 32 du projet de loi accorde certains pouvoirs de contrôle et de sanction à l'Autorité des données. Après vérification des résultats d'un traitement ultérieur de données à caractère personnel par une entité publique ou d'une réutilisation de données par un réutilisateur, elle pourrait notamment interdire l'utilisation de ces résultats s'ils portent une atteinte disproportionnée aux droits et intérêts de tiers. Le commentaire des articles mentionne à cet égard que « *[l]es dispositions de l'article 32 s'entendent sans préjudice des prérogatives de la Commission nationale pour la protection des données d'interdire les traitements de données à caractère personnel opérés en contravention aux conditions reprises dans l'autorisation émise par l'Autorité des données, conformément au règlement (UE) 2016/679, lu ensemble avec la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.* ».

139. La Commission nationale se permet de renvoyer aux points 15 à 18 du présent avis où elle a déjà précisé qu'elle devrait pouvoir sanctionner une entité publique ou un réutilisateur de données non seulement pour interdire un traitement de données à caractère personnel opéré en contravention aux conditions reprises dans l'autorisation émise par l'Autorité des données à cette fin. Elle estime que ses pouvoirs de contrôle et de sanctions ne se limitent pas à la vérification des conditions repises dans les autorisations de l'Autorité des données, mais qu'elle est compétente pour vérifier l'application et le respect de l'intégralité des dispositions du RGPD et de la loi du 1er août 2018.

De même, les pouvoirs de sanctions de la CNPD sont beaucoup plus étendus et ne se limitent pas à l'imposition d'une interdiction de traitement de données à caractère personnel prévue par l'article 58, paragraphe (2), point f) du RGDP, mais elle dispose de tous les pouvoirs prévus à l'article 58 du RGPD.

140. De plus, l'article 34, paragraphe (1) du projet de loi prévoit que l'Autorité des données « *tient un registre public des traitements ultérieurs de données à caractère personnel et des accès et*

---

73 Sauf les traitements ultérieurs par la même entité publique qui ne sont pas soumis à autorisation de l'Autorité des données et ne sont donc pas concernés par le titre VII du projet de loi.

réutilisations de données autorisés. » Néanmoins, il n'est pas clair si ledit registre devra contenir uniquement les traitements ultérieurs et les réutilisations de données actives, donc ceux qui sont encore en cours, ou si, par contre, il contiendra aussi un historique des traitements ultérieurs et des réutilisations terminés. La CNPD estime que, dans un but de transparence, garder un historique en la matière pendant un certain temps devrait être envisageable.

141. Par ailleurs, l'article 34, paragraphe (2) du projet de loi prévoit que la « *publication par l'Autorité des données des éléments d'informationà destination des personnes concernées, telle que visée au paragraphe 1er, alinéa 2, point 3°, vaut information de la personne concernée au sens des articles 12 à 14 du règlement (UE) 2016/679 pour les traitements ultérieurs de données visés au titre V et les accès et réutilisations visés au titre VI.* »

142. La Commission nationale tient tout d'abord à souligner que dans le cadre des traitements de données à caractère personnel concernés par le présent projet de loi, l'obligation d'information à respecter est surtout celle inscrite à l'article 14 du RGPD qui s'applique au cas de figures dans lesquels les données n'ont pas été collectées directement auprès de la personne concernée. En effet, dans le cadre d'un traitement ultérieur[74] ou d'une réutilisation, une entité publique ou un réutilisateur ne collecte pas les données auprès de la personne concernée, mais auprès de l'entité publique, voire de l'organisme public qui détient les données et donc les données sont collectées de manière indirecte.

Ensuite, alors que la transparence constitue un aspect fondamental des principes relatifs au traitement des données à caractère personnel, des exceptions à l'obligation d'informer individuellement la personne concernée lorsque des données à caractère personnel n'ont pas été collectées auprès d'elle sont prévues à l'article 14, paragraphe (5) du RGPD. Dans les lignes directrices sur la transparenc[75] de l'ancien Groupe de Travail Article 29, des lignes directrices reprises et re-approuvées par l'EDPB,[76] il est précisé que ces « *dérogations devraient, en règle générale, être interprétées et appliquées stricto sensu* ».

L'article 14. 5. c) du RGPD prévoit notamment que l'obligation d'information ne s'applique pas si « *l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée.* »[77] *Néanmoins*, les lignes directrices sur la transparence précisent dans ce contexte que « *le responsable du traitement devrait signaler clairement aux personnes concernées qu'il obtient ou communique les données à caractère personnel en accord avec le droit en question […]* » ; une obligation qui serait dès lors à respecter par les responsables du traitement dans le contexte du projet de loi sous avis.

Par contre, si le législateur veut introduire dans le projet de loi une limitation générale de la portée du droit à l'information sur base de l'article 23 du RGPD, toutes les conditions y énumérées sont à respecter et l'article 34 du projet de loi devrait être adapté en ce sens. L'article 23 du RGPD prévoit notamment en son paragraphe 1er que les droits de la personne concernée peuvent être limités lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs énumérés dans ce paragraphe. Par ailleurs, il y a lieu de soulever que lorsqu'une telle restriction aux droits des personnes est prévue par une mesure législative, elle doit contenir des dispositions spécifiques relatives aux informations énumérées au paragraphe 2 de l'article 23 du RGPD.[78]

---

74 Le seul cas où les données seraient potentiellement collectées auprès de la personne concernée c'est le traitement ultérieur par la même entité publique , mais ce cas n'est pas soumis à autorisation de l'Autorité des données et n'est donc pas concerné par le titre VII du projet de loi.

75 Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, version révisée adoptée le 11 avril 2018, WP260 rev.01, point 57.

76 Voir décision Endorsement 1/2018 de l'EDPB du 25 mai 2018.

77 V. l'arrêt précité de la CJUE du 28 novembre 2024, ECLI:EU:C:2024:988.

78 Il s'agit des finalités du traitement ; des catégories de données à caractère personnel; de retendue des limitations introduites ; des garanties destinées à prévenir les abus ou l'accès ou le transfert illicites; la détermination du responsable du traitement; les durées de conservation et les garanties applicables ; les risques pour les droits et libertés des personnes concernées et le droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation.

143. Finalement, sans préjudice des commentaires qui précèdent, la CNPD constate que l'article 34 du projet de loi ne prévoit pas de délai de publication des informations par l'Autorité des données. Elle estime que dans un but de transparence, les informations en cause devraient être publiées au même moment où l'Autorité des données accorde une autorisation à l'entité publique ou au réutilisateur.

E. Sur la gouvernance en matière de services d'intermédiatlon de données et d'altruisme des données

En vertu des articles 39 et 44 du projet de loi, la CNPD est désignée « autorité compétente » responsable pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données, telle que visée à l'article 13 du règlement 2022/868, ainsi que pour le registre public national des organisations altruistes en matière de données, tel que visé à l'article 23 du règlement 2022/868.

144. L'article 41 du projet de loi prévoit qu'un règlement interne de la CNPD définit la procédure de notification pour les services d'intermédiation de données conformément à l'article 11 du règlement 2022/868.

145. La CNPD tient à souligner dans ce contexte que le Conseil d'Etat avait soulevé dans son avis sur le projet de loi n° 7184 dont est issu la loi du 1er août 2018[79] qu'en « *vertu de l'article 108bis de la Constitution, les établissements publics ne disposent d'un pouvoir réglementaire que « dans la limite de leur spécialité ». Le Conseil d'État s'oppose formellement au pouvoir réglementaire non autrement délimité de la CNPD, et ce conformément aux arrêts de la Cour constitutionnelle dans lesquels il est précisé « que le pouvoir normatif des établissements publics est tributaire du principe de spécialité dans leur domaine de compétence et reste réservé à des mesures de détail précises, de nature technique et à portée pratique, destinées à permettre à celles-ci l'exercice, de façon autonome, d'une mission de régulation sectorielle facilitant la mise en œuvre des normes établies par la loi et, le cas échéant, le règlement grand-ducal.* »[80]

Dès lors, il est primordial que l'article 41 du projet de loi délimite précisément le pouvoir normatif de la CNPD en matière de services d'intermédiation de données. Elle estime que ledit article ne devrait pas uniquement faire référence à l'article 11 du règlement 2022/868 sur la notification des prestataires de services d'intermédiation de données. Plus précisément, il convient de préciser à l'article 41 du projet de loi que le pouvoir normatif de la CNPD englobe aussi la mise en œuvre de l'article 14 du règlement précité intitulé « Contrôle du respect des dispositions » afin de lui permettre de prévoir dans un règlement interne la procédure relative au contrôle et à la surveillance des prestataires de services d'intermédiation de données. Pour des raisons de transparence, la CNPD se demande si ce règlement devrait être publié au Journal officiel du Grand-Duché du Luxembourg.

Par ailleurs, la CNPD constate qu'une disposition accordant un pouvoir normatif à la CNPD en matière d'enregistrement des organisations altruistes fait défaut. Elle estime dès lors nécessaire de compléter la section II du Titre VIII du projet de loi en ce sens. Un tel article pourrait avoir la teneur suivante : « *Un règlement interne de la CNPD définit la procédure et le contrôle en matière d'enregistrement des organisations altruistes, conformément aux articles 17 à 19 et 24 du règlement (UE) 2022/86.* ». La CNPD se demande également si ce règlement ne devrait pas être publié au Journal officiel du Grand-Duché du Luxembourg.

146. En ce qui concerne l'article 34 du règlement 2022/868, ce dernier prévoit que les États membres déterminent le régime des sanctions applicables aux violations, entre autres, de l'obligation de notification incombant aux prestataires de services d'intermédiation de données en vertu de l'article 11 et des conditions liées à la fourniture desdits services en vertu de l'article 12, d'une part, et aux violations

79 Avis du Conseil d'Etat n° CE 52.422 portant création de la Commission nationale pour la protection des données et la mise en œuvre du 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, portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État et abrogeant la loi du 2 août 2002 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, doc. parl. n°7184/12.

80 Arrêts 76-96/13 du 19 mars 2013 de la Cour constitutionnelle.

des conditions liées à l'enregistrement en tant qu'organisation altruiste en matière de données reconnue en vertu des articles 18, 20, 21 et 22, d'autre part.

147. La CNPD constate dans ce contexte que l'article 43 du projet de loi prévoit le régime des sanctions applicables pour les prestataires de services d'intermédiation, tandis qu'un tel régime fait défaut pour les organisations altruistes en matière de données. Afin de renforcer l'efficacité de ses pouvoirs de contrôle prévus à l'article 24 du règlement 2022/868 et à l'article 45 du projet de loi, il est essentiel que la CNPD puisse disposer de pouvoir de sanction en la matière, en cas de non-respect. Elle est dès lors d'avis que la section II du Titre VIII du projet de loi devra en tout état de cause être complétée à cet égard.

148. Finalement, sur base de ce qui précède, la CNPD comprend que ce n'est pas l'Autorité des données, mais elle-même qui est de facto membre du Comité européen de l'innovation dans le domaine des données institué sur base de l'article 29 du règlement 2022/868. En effet, il ressort dudit article que ce Comité est d'office composé des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données, alors que les organismes compétents en matière de réutilisation de données n'y sont pas mentionnés[81].

Ainsi adopté à Belvaux en date du 20 décembre 2024.

La Commission nationale pour la protection des données

Tine A. LARSEN
Présidente

Thierry LALLEMANG
Commissaire

Marc LEMMER
Commissaire

Alain HERRMANN
Commissaire

81 L'article 29, paragraphe (1) du règlement 2022/868 prévoit ce qui suit : « *La Commission institue un comité européen de l'innovation dans le domaine des données sous la forme d'un groupe d'experts, qui se compose de représentants des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de tous les États membres, du comité européen de la protection des données, du Contrôleur européen de la protection des données, de l'ENISA, de fa Commission, du représentant de l'UE pour les PME ou d'un représentant désigné par le réseau des représentants des PME, et d'autres représentants d'organismes compétents dans des secteurs particuliers ainsi que d'organismes disposant d'une expertise particulière. Lorsqu'elle nomme des experts individuels, la Commission s'efforce de parvenir à un équilibre entre les hommes et les femmes ainsi qu'à un équilibre géographique parmi les membres du groupe d'experts* »

Impression: CTIE – Division Imprimés et Fournitures de bureau

20250515_Avis

N° 8395[5]

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AVIS DE LA CHAMBRE DE COMMERCE

(6.12.2024)

Le projet de loi sous avis (ci-après, le « Projet de loi ») a pour objet (i) d'autoriser les entités publiques à traiter des données à caractère personnel dès lors que leur traitement est nécessaire aux fins de l'exécution de leur mission d'intérêt public[1] ; (ii) de mettre en œuvre le principe de simplification administrative dit « once only », (iii) de mettre en application pour les organismes du secteur public certaines dispositions du règlement européen sur la gouvernance des données[2], appelé « Data Governance Act » (ci-après, le « DGA ») et (iv) de mettre en application certaines dispositions du règlement général sur la protection des données[3] (ci-après, le « RGPD »).

Le Projet de loi se décompose en neuf titres, comme suit :

– Titre I – Dispositions préliminaires
– Titre II – Traitement de données à caractère personnel par les entités publiques nécessaire à l'exécution de la mission d'intérêt public ou relevant de l'exercice de l'autorité publique
– Titre III – Acteurs compétents en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données
– Titre IV – Informations et données à caractère personnel obtenues par les entités publiques auprès d'une autre entité publique (« *once only* »)
– Titre V – Traitement ultérieur de données à caractère personnel par les entités publiques

1 ou de leurs missions relevant de l'exercice de l'autorité publique dont elles sont investies par une disposition de droit de l'Union européenne ou de droit luxembourgeois.

2 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)

3 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

– Titre VI – Accès et réutilisation des données détenues par des organismes du secteur public par des réutilisateurs de données
– Titre VII – Modalités applicables au traitement ultérieur des données à caractère personnel par les entités publiques et à l'accès et à la réutilisation de données par des réutilisateurs de données
– Titre VIII – Gouvernance en matière de services d'intermédiation de données et d'altruisme des données
– Titre IX – Dispositions finales

Le Projet de loi s'accompagne d'un projet de règlement grand-ducal (ci-après, le « Projet de règlement grand-ducal ») qui a pour objet de déterminer certaines modalités d'application du Projet de loi, concernant le Conseil consultatif institué par l'article 8 du Projet de loi (composition, fonctionnement et attributions) ainsi que les redevances prévues à l'article 30 du Projet de loi (règles relatives au calcul et à la perception des redevances, à payer par les acteurs privés, en contrepartie de la mise à disposition de données protégées détenues par les organismes publics).

En bref

- La Chambre de Commerce se félicite des dispositions projetées qui contribueront au développement de l'économie numérique en encourageant la réutilisation des données (ouvertes ou protégées) et en garantissant un environnement de confiance pour les citoyens et les entreprises.
- Elle salue tout particulièrement l'objectif de simplification administrative découlant de la mise en oeuvre du principe dit du « *once only* », qui devrait profiter aux entreprises, idéalement via le portail unique My guichet.
- Elle salue également le soutien aux PME et aux jeunes pousses qui pourront accéder et réutiliser les données protégées détenues par les organismes publics (en lien avec la mise en œuvre du DGA), moyennant une redevance réduite ou à titre gratuit, à des fins d'analyse statistique, d'activités d'éducation, de formation ou d'enseignement, de recherche scientifique, de développement de technologies ou de produits et d'évaluation des politiques publiques.
- Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver les projets de loi et de règlement grand-ducal sous avis, sous réserve de la prise en compte de ses observations.

*

RESUME

La Chambre de Commerce se félicite des dispositions projetées qui contribueront au développement de l'économie numérique en encourageant la réutilisation des données – ouvertes ou protégées – et en garantissant un environnement de confiance pour les citoyens et les entreprises.

Cette initiative est la bienvenue au regard des conclusions de la dernière enquête *World Digital Competitiveness Ranking 2024* de l'*International Institute for Management Development* (IMD) qui vient de paraître[4], selon lesquelles le Luxembourg peinerait à suivre le rythme des autres pays en ce qui concerne les transformations digitales.

A titre liminaire, elle souligne toutefois que la définition lacunaire de l'« entité publique » donnée par le Projet de loi[5] qui vise notamment « *les personnes morales d'utilité publique listées expressément par règlement grand-ducal aux fins d'application des dispositions des titres IV et V* » à défaut pour les auteurs d'avoir communiqué ce projet de règlement grand-ducal avec le Projet de loi, ce qui empêche la Chambre de Commerce de prendre toute la mesure du champ d'application du Projet de loi.

La Chambre de Commerce accueille favorablement le Projet de loi, composé de quatre piliers de mesures, qui vise à valoriser le traitement des données et leur circulation dans un environnement de confiance en application des règlements européens que sont le DGA (applicable à tous types de données) et le RGPD (relatif aux données à caractère personnel).

4 Suivant cette enquête, « *[L]e Luxembourg, 29e, s'éloigne encore un peu plus de sa performance de 2019 (21e) et peine visiblement à suivre le rythme des autres pays en ce qui concerne les transformations digitales.* », cf. https://www.cc.lu/toute/information/actualites/detail/imd-world-digital-competitiveness-ranking-2024-il-est-temps-dinverser-la-tendance

5 cf. article 2, paragraphe 2, 2° du Projet de loi

Elle accueille favorablement la mesure qui vise à sécuriser juridiquement les traitements de données à caractère personnel (déjà) réalisés par les entités publiques dans ce cadre (premier pilier) ainsi que celles qui permettront d'améliorer la réutilisation des données publiques, en favorisant les traitements ultérieurs de données personnelles par les entités publiques elles-mêmes et entre elles (troisième pilier).

Elle salue particulièrement l'objectif de simplification administrative notamment au profit des entreprises, par la mise en place du principe dit du « *once only* » (deuxième pilier). Plus concrètement, elle soutient les intentions du gouvernement de favoriser cette simplification administrative par l'intermédiaire de l'espace *My guichet*, et insiste tout particulièrement pour que cet objectif soit mis en œuvre dans les meilleurs délais aux niveaux des procédures d'immigration / obtention d'un titre de séjour pour indépendant, de la prévention des difficultés des entreprises et des aides financières aux entreprises.

Néanmoins, eu égard notamment aux obligations auxquelles devront se conformer les administrations pour rendre ledit principe effectif, la Chambre de Commerce s'interroge sur l'opportunité d'insérer éventuellement une entrée en vigueur échelonnée de la future loi.

Enfin, la Chambre de Commerce salue encore tout particulièrement le soutien donné aux PME et aux jeunes pousses qui pourront accéder et réutiliser les données protégées détenues par les organismes du secteur public (en lien avec la mise en œuvre du DGA), moyennant une redevance réduite ou à titre gratuit, et de surcroît acquitté en ligne pour des raisons de simplification administrative ainsi que la publication d'une liste des catégories de réutilisation concernées. Très concrètement, la Chambre de Commerce voit dans le pilier 4 du Projet de loi, un moyen de développer l'activité de startups notamment dans le secteur des MedTech[6] (technologies médicales), ce qu'elle soutient puisque ce pilier 4 doit permettre aux acteurs du secteur privé d'accéder et de réutiliser les données protégées du secteur public à des fins d'analyse statistique, d'activités d'éducation, de formation ou d'enseignement, recherche scientifique, de développement de technologies ou de produits et d'évaluation des politiques.

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure de d'approuver les projets de loi et de règlement grand-ducal sous avis, sous réserve de la prise en compte de ses observations.

Appréciation du projet de loi :

Compétitivité de l'économie luxembourgeoise	++
Impact financier sur les entreprises	++
Transposition de la directive	n.a.
Simplification administrative	++
Impact sur les finances publiques	-[7]
Développement durable	+

Légende :

++	très favorable
+	Favorable
0	Neutre
-	Défavorable
--	très défavorable
n.a.	non applicable
n.d.	non disponible

*

6 Ensemble des technologies utilisées pour diagnostiquer, traiter et/ou améliorer la santé et le bien-être d'une personne.

7 cf. fiche financière jointe au Projet de loi

CONCERNANT LE PROJET DE LOI

La Chambre de Commerce accueille favorablement le Projet de loi, qui vise notamment à simplifier les démarches administratives des citoyens et entreprises, en mettant en place l'obligation pour les entités publiques de collecter les données des administrés auprès d'autres administrations (principe dit du « *once only* ») et la possibilité pour les entités publiques d'informer les administrés de manière proactive des bénéfices auxquels ils ont droit de la part de l'Etat. Le Projet de loi vise encore à valoriser le traitement des données détenues par des organismes du secteur public et leur circulation dans un environnement de confiance en application des règlements européens que sont le DGA (applicable à tous types de données) et le RGPD (relatif aux données à caractère personnel).

Ce Projet de loi s'inscrit dans la stratégie des données du secteur public du Gouvernement, qui ambitionne d'instaurer ainsi « *un cadre juridique propice et fédérateur à la création, l'utilisation, le partage et la réutilisation des données au sein du secteur public.* »[8].

Le Projet de loi est constitué de quatre piliers fonctionnant indépendamment les uns des autres, mais ayant en commun notamment des définitions et l'intervention d'acteurs aux compétences transversales.

1. Remarques préliminaires

La Chambre de Commerce souligne en premier lieu que **le champ d'application personnel diffère en fonction des piliers du Projet de loi concernés** : les trois premiers piliers s'appliquent aux « entités publiques » alors que le quatrième pilier s'applique aux « organismes du secteur public ».

Par ailleurs, seule la définition de l'« **entité publique** » est fournie par le Projet de loi (à l'article 2, paragraphe 2, point 2°)), comme suit :

> « *un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et* ***les personnes morales d'utilité publique listés expressément par règlement grand-ducal*** *aux fins d'application des dispositions des titres IV[« once only »] et V [traitement ultérieur de données par les entités publiques].* »

Quant aux termes « **organismes du secteur public** », visés par le quatrième pilier du Projet de loi mettant en œuvre une partie du DGA, la Chambre de Commerce en déduit que leur définition ressort de l'article 2, point 17) dudit DGA[9] qui vise : « *l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public* ».

Enfin, les termes « **organismes de droit public** » inclus dans la définition qui précède sont définis par l'article 2, point 1) du DGA[10] comme suit :

> « *les organismes présentant les caractéristiques suivantes:*
>
> *a) ils ont été créés pour satisfaire spécifiquement des besoins d'intérêt général et n'ont pas de caractère industriel ou commercial;*
>
> *b) ils sont dotés de la personnalité juridique;*
>
> *c) ils sont financés majoritairement par l'État, les autorités régionales ou locales ou d'autres organismes de droit public, leur gestion est soumise à un contrôle de ces autorités ou organismes, ou leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou locales ou d'autres organismes de droit public* ».

---

8 cf. Accord de coalition 2023-2028, « Lëtzebuerg fir d'Zukunft stäerken », p.4 et p.7

9 A noter que la même définition d' « organisme du secteur public » figure à l'article 2, point 2 de la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public (issue de la transposition de la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public dite « PSI »).

10 La définition d' « organisme du secteur public » figure également à l'article 2, point 2 de la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public (issue de la transposition de la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public dite « PSI »).

Ces différentes définitions ayant été rappelées, la Chambre de Commerce revient plus particulièrement sur celle d' « entité publique » donnée par le Projet de loi et regrette qu'elle soit actuellement incomplète puisqu'assujettie à un projet de règlement grand-ducal qui n'a pas été communiqué avec le Projet de loi, ce qui empêche la Chambre de Commerce de prendre toute la mesure du champ d'application des mesures projetées.

Elle s'interroge également sur la compréhension des termes « ***aux fins d'application des dispositions des titres IV et V*** » qui figurent dans le libellé de la définition de l'entité publique : « *un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, (…) les personnes morales d'utilité publique listés expressément par règlement grand-ducal* ***aux fins d'application des dispositions des titres IV*** *[once only »]* ***et V*** *[Traitement ultérieur de données à caractère personnel par les entités publiques*»] et se demande à quelles entités se rapportent ces termes ? S'agit-il de toutes les entités listées dans la définition ou seulement celles qui seront listées dans le futur règlement grand-ducal ?). En outre, si les différents titres concernés (titre IV et V) par la définition de l'entité publique ont été énumérés de manière exhaustive, les dispositions du Titre II (« Traitement de données à caractère personnel par les entités publiques nécessaire à l'exécution de la mission d'intérêt public ou relevant de l'exercice de l'autorité publique ») devraient également être mentionnées le cas échéant.

Elle invite en conséquence les auteurs à lever cette insécurité juridique.

2. Descriptions des quatre piliers du Projet de loi et des mesures transversales

a. *Premier Pilier[11] : « traitement primaire de données à caractère personnel[12] » par les « entités publiques » (Titre II du Projet de loi)*

Ce premier pilier – qui correspond au Titre II du Projet de loi – a trait au traitement de données à caractère personnel par les entités publiques, nécessaire à l'exécution de la mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

Suivant le RGPD, les traitements de données à caractère personnel ne sont licites que s'ils reposent sur une des six bases de licéité prévue dans son article 6, paragraphe 1er. Le fait que le traitement soit « *nécessaire à l'exécution d'une mission d'intérêt publique ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* »[13] figure dans cette liste.

Dans ce cadre, l'article 3 du Projet de loi, vient **consacrer en droit national l'habilitation des entités publiques[14] à traiter les données à caractère personnel nécessaires aux fins relevant de l'exécution de leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont ces autorités sont investies** par une disposition de droit de l'Union européenne ou de droit national applicable.

Ce faisant, les auteurs du Projet de loi renforcent la sécurité juridique des traitements de données à caractère personnel réalisés par les entités publiques consacrant dans la loi, l'utilisation de la base de licéité prévue à l'article 6, paragraphe 1, lettre e) du RGPD, par opposition à la lettre c) du même article[15] qui vise le traitement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumise.

---

11 cf. Titre II, article 3 du Projet de loi

12 Présentation du Projet de loi relatif à la valorisation des données dans un environnement de confiance, Ministère de la Digitalisation, https://gouvernement.lu/dam-assets/documents/actualites/2024/06/20-obertin-onceonly/20240620-presentation-mindigital.pdf

13 cf. article 6, paragraphe 1, e) du Projet de loi

14 Pour rappel, l'entité publique est définie à l'article 2, paragraphe 2, sous point 2° du Projet de loi comme « *un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et* ***les personnes morales d'utilité publique listés expressément par règlement grand-ducal*** *aux fins d'application des dispositions des titres IV[« once only »] et V [traitement ultérieur de données par les entités publiques].* »

15 L'article 6, paragraphe 1, du RGPD prévoit « *Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : […] c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;.* ». Cette base de licéité nécessite, selon le commentaire de l'article 3 du Projet de loi, un fondement en droit interne ou européen qui définit les finalités de traitement directement dans le texte de loi.

Tel que l'expliquent les auteurs sous le commentaire de l'article, cette consécration légale permet au Luxembourg de s'aligner sur la position des pays voisins.

« *Ainsi, le fait pour une entité publique de pouvoir démontrer le respect de la double condition : **premièrement** qu'elle soit investie d'une mission d'intérêt public ou qui relève de l'exercice de l'autorité publique dont elle est investie et, **deuxièmement**, que le traitement de données à caractère personnel soit « nécessaire » pour réaliser cette mission, suffit à légitimer la collecte et le traitement des données en question.* »[16].

La Chambre de Commerce accueille favorablement cette mesure qui sécurise les traitements de données à caractère personnel réalisés par les entités publiques dans ce cadre.

b. *Deuxième pilier[17] : principe « once only » entre entités publiques (Titre IV du Projet de loi)*

Le deuxième pilier (titre IV) du Projet de loi, relatif aux « informations et données à caractère personnel obtenues par les entités publiques auprès d'une autre entité publique » – dit « once only » – contient deux volets, d'une part, un volet relatif à la **simplification administrative** et d'autre part, un volet relatif à **l'administration proactive**.

Concernant la **simplification administrative**, l'article 9 paragraphe 1 du Projet de loi **impose l'échange d'informations ou de données à caractère personnel entre « entités publiques »**, afin **d'éviter qu'un administré présentant une demande ou produisant une déclaration ne soit tenu de produire des données que l'entité publique détient déjà ou qu'elle peut obtenir auprès d'une autre entité publique**.

Le volet relatif à **l'administration proactive,** permet quant à lui, aux entités publiques d'échanger entre elles des informations ou des données à caractère personnel nécessaires, **pour pouvoir informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage[18] et de pouvoir potentiellement le leur attribuer**.

La Chambre de Commerce salue l'institution du principe « once only », qui s'inscrit dans un objectif de simplification administrative cher à la Chambre de Commerce, dont la mise en œuvre sera particulièrement bienvenue, car elle simplifiera et allègera les démarches administratives pour les citoyens et les entreprises.

La Chambre de Commerce, comprend par ailleurs que le travail technique préalable à l'échange de données entre « entités publiques » est déjà en cours et s'en félicite. A cet égard, elle relève que, suivant l'accord de coalition 2023-2028[19] :

– la plateforme MyGuichet sera optimisée dans l'optique d'introduire le principe du *once only* de manière à (i) informer les entreprises en temps réel de la progression du traitement de leur demande et leur fournir un aperçu complet, comme, par exemple, au sujet des aides approuvées et des autorisations d'établissement et (ii) faciliter le partage de documents avec différentes administrations publiques et ministères ;
– le Gouvernement mettra en place un échange automatique entre administrations pour chaque registre et chaque base de données, habilitant des administrations à se connecter à un système informatique pour échanger des documents et informations, par exemple dans le cadre des aides étatiques (interconnexion accrue des systèmes informatiques des différentes administrations).

La Chambre de Commerce relève ainsi que la réduction de la charge administrative dans le cadre de la constitution et du traitement des dossiers tels que des **demandes d'autorisation d'établissement**, d'agréments, de déclaration au Centre commun de la sécurité sociale, d'autorisation de bâtir, d'exploitation dites « commodo-incommodo » ou encore en matière de marchés publics fera gagner du temps aux entreprises luxembourgeoises, qui pourra ainsi être réinvesti dans des tâches plus productives pour l'économie nationale.

---

16 cf. Commentaire des articles du Projet de loi, p.29

17 cf. Titre IV, art 9 à 14 du Projet de loi

18 L'article 9, paragraphe 2 alinéa 2 précise que la prestation ou l'avantage sont « prévus par des dispositions législatives ou réglementaires ».

19 cf. spécialement les pages 158 et 159 (simplification administrative pour les PME)

De manière plus détaillée, mais sans prétendre à l'exhaustivité, la Chambre de Commerce identifie en particulier les démarches suivantes comme prioritaires au niveau du déploiement du « once and only / gouvernement proactif » pour les entreprises, et qui devraient être idéalement accessibles depuis l'espace MyGuichet :

- au niveau de la création d'entreprise : créer un guichet unique dans l'Espace MyGuichet pour qu'un seul enregistrement soit nécessaire afin de réaliser toutes les démarches de création et affiliations nécessaires lors du lancement d'une entreprise et par la suite pour enregistrer des modifications ;
- au niveau des procédures d'immigration / obtention d'un titre de séjour pour indépendant : la procédure d'obtention d'un titre de séjour pour indépendant reste complexe et la communication de données inter-ministérielles n'est pas encore en place (toute la procédure est encore sous format papier au niveau de la Direction de l'immigration). Par ailleurs, si la procédure d'obtention de l'autorisation d'établissement est étroitement liée à la procédure d'obtention du titre de séjour, il faut actuellement mener les deux procédures en parallèle auprès des deux ministères différents, en envoyant des pièces à l'un et à l'autre, et en partageant également les décisions émises par l'un à l'autre. Dans ce contexte, il serait souhaitable de mettre en place une communication automatique entre le Ministère de l'Economie et le Ministère de l'Intérieur pour diminuer le nombre d'envois de documents par l'administré lui-même (en gardant comme idée la possibilité de visualiser « l'administrative Journey » du demandeur dans MyGuichet) ;
- le même type de remarques vaut au niveau des procédures d'immigration (dans le cadre de l'obtention d'un visa, de l'autorisation de travail, du titre de séjour) spécialement pour les travailleurs salariés, hautement qualifiés ou non, en provenance d'Etats tiers à l'Union européenne.
- au niveau de la formation professionnelle en cours d'emploi : le soutien financier de l'Etat est soumis à plusieurs conditions préalables tant dans le chef du salarié (il doit être majeur et disposer d'un contrat de travail dans le domaine du métier ou de la profession concernée) que dans le chef de l'employeur, ce qui oblige ce dernier à produire un certain nombre pièces justificatives (la convention d'apprentissage, le contrat de travail du salarié en formation en cours d'emploi et la preuve de l'affiliation de ce dernier au Centre commun de la sécurité sociale). Dans ce contexte, il serait souhaitable d'instaurer une collaboration entre le Centre commun de la sécurité sociale et le ministère chargé de l'instruction des demandes de compensation financière.au niveau de la prévention des difficultés des entreprises : la mise en place d'un bulletin d'alerte ou d'un courrier récapitulatif pouvant être téléchargé sous l'espace digital de l'entreprise dans MyGuichet, qui comprendrait toutes les informations liées à l'entreprise, y compris le cas échéant, la situation quant aux dettes publiques que cette dernière aurait accumulées (regroupement et mise à disposition des données CCSS / AED / ACD pour l'entreprise en question), serait très utile ;
- au niveau des aides financières : il serait nécessaire de centraliser, en un endroit unique, par exemple sur MyGuichet, pour chaque entreprise, l'ensemble des informations concernant le contingent des aides liées au régime *de minimis* afin que l'entreprise puisse voir le budget lui restant octroyable annuellement, ainsi que la « checklist » des aides existantes pour laquelle elle est encore éligible (liste des aides PME) et l'historique identifiant les aides accordées et les échéanciers des virements prévus par l'Etat s'il s'agit d'aides remboursables.

La Chambre de Commerce se félicite encore du cadre de confiance proposé par le Projet de loi permettant la traçabilité des informations[20] entre administrations et la transparence vis-à-vis de l'administré (citoyens et entreprises) dans le respect du droit de la protection des données à caractère personnel[21].

De même, **la Chambre de Commerce salue l'introduction de dispositions permettant la proactivité des entités publiques notamment envers les entreprises**[22] afin de pouvoir les identifier et leur proposer, entre autres, des aides financières auxquelles celles-ci pourraient prétendre, faisant ainsi basculer le pouvoir d'initiative vers l'administration. Il s'agit ici d'une excellente nouvelle pour les entreprises, spécialement les PME et TPE qui pour certaines, renoncent à l'heure actuelle à solliciter

20 cf. article 11 du Projet de loi prévoyant notamment au paragraphe 2 que l'entité publique informe l'administré de l'administration de provenance de chaque catégorie d'information.

21 Son notamment garantis les droits à la rectification (cf. article 10, paragraphe 2 du Projet de loi) et à l'opposition au traitement dans le cadre du traitement des données de « l'administration proactive » (cf. article 11, paragraphe 3, alinéa 2 du Projet de loi).

22 cf. article 9, paragraphe 2, alinéa 2 du Projet de loi

le bénéfice d'une aide, par manque de temps ou de ressources face à la complexité de l'étude des conditions d'attribution ou de constitution du dossier de demande.

Enfin, s'agissant du calendrier, elle constate que le Projet de loi ne prévoit pas de date d'entrée en vigueur, ni de dispositions transitoires. Même si la Chambre de Commerce estime qu'il est important que les administrés puissent bénéficier au plus vite des mesures introduites par le Projet de loi, elle s'interroge néanmoins sur l'opportunité d'insérer éventuellement une entrée en vigueur échelonnée de la future loi alors que :

– la mise en œuvre pratique du principe du « once only » notamment se fera certainement par étapes successives compte tenu des défis techniques et informatiques qui en découlent,
– les « entités publiques » doivent disposer du temps nécessaire pour se conformer aux nouvelles obligations découlant de la future loi telles que celles d'effectuer le recensement des informations et données à partager[23], formaliser les échanges d'informations à travers des protocoles « once only » (à conclure entre elles) ainsi que rédiger les notices d'information à l'attention des administrés[24] avant que l'obligation d'échange de données[25] ne soit en vigueur.

c. *Troisième pilier : traitement ultérieur de données à caractère personnel par les entités publiques (Titre V du Projet de loi)*

En matière de traitement de données à caractère personnel, le RGPD pose le principe général de limitation des finalités[26] qui signifie que les données personnelles doivent être collectées pour des finalités déterminées (dans le cadre d'un traitement primaire) et **qu'elles ne peuvent pas être traitées ultérieurement pour des finalités incompatibles avec les finalités initiales**.

L'article 6, paragraphe 4 du RGPD permet de réaliser des traitements ultérieurs des données initialement collectées (i) sur la base du consentement de la personne concernée, (ii) sur la base de leur compatibilité avec le traitement initial[27], ou (iii) lorsqu'une disposition spécifique du droit de l'Union européenne ou de droit national[28] le permet.

C'est cette dernière possibilité que met en œuvre le troisième pilier du Projet de loi (Titre V), en introduisant une disposition spécifique en droit national **permettant aux « entités publiques » d'effectuer un traitement ultérieur de données à caractère personnel au-delà de la finalité du traitement initial, dans des conditions précises** et en application de l'article 6, paragraphe 4 du RGPD.

La Chambre de Commerce salue l'initiative des auteurs du Projet visant à **améliorer la réutilisation des données publiques**. En effet, cette mesure, porteuse de sécurité juridique, permettra favoriser les traitements ultérieurs de données personnelles par les entités publiques elles-mêmes et entre elles.

Ainsi, en application des dispositions du Titre V du Projet de loi, le traitement ultérieur de données à caractère personnel par des entités publiques pourra être réalisé moyennant le respect :

– **d'une ou plusieurs finalités de traitement** prévues à l'article 15 du Projet de loi parmi lesquelles figurent des thématiques que la Chambre de Commerce soutien plus particulièrement telles que : « *les activités d'éducation ou d'enseignement, y compris le niveau de l'enseignement professionnel ou supérieur*[29]», « *les activités de développement, d'évaluation, de démonstration, de sécurité et d'innovation de dispositifs ou de services*[30] » et « *la formation, le test et l'évaluation d'algorithmes, y compris dans les dispositifs, les systèmes d'intelligence artificielle et les application numériques* » ;

---

23 cf. article 12, paragraphe du Projet de loi

24 cf. article 11, paragraphe 2 du Projet de loi

25 prévue à l'article 9 du Projet de loi

26 cf. article 5, paragraphe 1, b du RGPD

27 Cette compatibilité doit être analysée et documentée en vertu du principe de responsabilité (accountability) prévu à l'article 5 du RGPD.

28 La disposition spécifique du droit de l'Union européenne ou de droit national qui permet le traitement ultérieur doit, selon le texte de l'article 6, paragraphe 4 du RGPD, constituer « une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1 du RGPD. »

29 cf. article 15, paragraphe 1, point 2, lettre b

30 cf. article 15, paragraphe 1, point 2, lettre f

– **des conditions d'anonymisation, sinon de pseudonymisation, sinon des limites du strict nécessaire**, prévues à l'article 16 du Projet de loi[31] **;**
– **des conditions de confidentialité** prévues à l'article 16 du Projet de loi ; **et**
– **de mesures techniques et organisationnelles** pour empêcher la réidentification, prévues à l'article 16 du Projet de loi.

En outre, s'y ajouteront des **conditions spécifiques différentes en fonction du fait que le traitement ultérieur est réalisé par la même entité publique ou par une autre entité publique.**

Dans cette dernière hypothèse, l'entité publique qui détient les données à caractère personnel devra notamment marquer son accord[32] au traitement ultérieur.

d. *Quatrième pilier[33] : accès et réutilisation des données détenues par des « organismes du secteur public »[34] par des réutilisateurs de données (Titre VI du Projet de loi)*

Ce quatrième pilier vise à mettre en œuvre un des trois volets[35] que comporte le DGA, à savoir **l'accès et la réutilisation par les acteurs privés des données protégées détenues par des organismes du secteur public**[36]. Il se distingue des traitements de données couverts par le troisième pilier en ce que les entités publiques ne sont pas en droit d'invoquer ses dispositions pour solliciter l'accès et la réutilisation des données visées, seules les personnes physiques ou morales du secteur privé (appelés « réutilisateurs de données ») le peuvent[37].

En revanche, les entités publiques, en tant qu' « organismes du secteur public », sont visées par les dispositions du titre VI pour ce qui concerne la mise à disposition des données qu'elles détiennent au profit des réutilisateurs de données.

S'agissant des catégories de données « protégées » disponibles à l'accès et la réutilisation, il peut s'agir de **données à caractère personnel ou non-personnel,** étant précisé qu'en présence de données à caractère personnel, des obligations et garanties renforcées sont applicables, notamment en vertu du RGPD. Leur protection repose sur des motifs suivants : confidentialité commerciale (y compris le secret d'affaires, le secret professionnel et le secret d'entreprise) ; secret statistique ; protection des droits de propriété intellectuelle de tiers ; ou protection des données à caractère personnel.

---

31 cf. article 16, paragraphe 3 du Projet de loi : « *(3) Lorsque le traitement ultérieur de données à caractère personnel pseudonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel peuvent être traitées ultérieurement aux fins énoncées à l'article 15, paragraphe 1er point 2° de manière non pseudonymisées dans les limites du strict nécessaire.* »

32 Selon l'article 18, paragraphe 1, point 1 du Projet de loi « L'entité publique qui détient les données pourra (i) donner un **accord de principe** en inscrivant les données à caractère personnel disponibles sur la liste des ressources consultable tenues par le point d'information unique ou (ii) marquer son **accord spécifique** au traitement ultérieur en contresignant la demande de traitement ultérieur émanant de l'entité publique sollicitant le traitement ultérieur ».

33 cf. Titre VI (accès et réutilisation), articles 19 à 24 et Titre VII (Modalités), articles 25 à 38.

34 La définition d' « organisme du secteur public » qui vise : « *L'Etat, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un plusieurs de organismes de droit public* » ne ressort pas du Projet de loi sous avis lui-même, mais de l'article 2, numéro 17 du DGA qui figure également à l'article 2, point 2 de la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public (issue de la transposition de la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public dite « PSI »).

35 Les deux autres volets du DGA étant (i) l'accès aux données détenues par les auteurs privés assurant un service de partage et (ii) l'accès à des acteurs publics aux données détenues par les entreprises privées lorsque cela s'impose pour protéger l'intérêt général.

36 Le DGA vise notamment à augmenter le nombre de données en circulation, à faciliter leur partage en complémentarité avec la mise à disposition des données en « open data » ou « données ouvertes » (cf. loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public).

37 La Chambre de Commerce comprend que si les entités publiques souhaitent réutiliser des données à caractère personnel, elles pourront le faire sur la base du troisième pilier (titre V) du Projet de loi. Néanmoins, la notion « d'entité publique » ne correspondant pas à celle « d'organisme du secteur public », la possibilité pour ces derniers de réaliser un traitement ultérieur de données à caractère personnel n'est pas prévue par le Projet de loi. Ils pourraient uniquement se prévaloir des dispositions y relatives de la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public, dans la limite de celles-ci.

En application des dispositions du Titre VI du Projet de loi, un réutilisateur de données pourra accéder et détenir les données protégées détenues par des organismes du secteur public moyennant le respect :

– **de certaines finalités limitativement énumérées**[38] (analyse statistique ; activités d'éducation, de formation ou d'enseignement ; recherche scientifique ; développement de technologies ou de produits ; évaluation des politiques publiques) ;
– **de conditions d'anonymisation sinon de pseudonymisation (obligatoires dans le cas de données à caractère personnel), sinon des limites du strict nécessaire**,
– d'une obligation de **confidentialité**[39] ainsi que de **mesures techniques et organisationnelles** pour empêcher la réidentification,
– d'un régime d'autorisation et de réutilisation de ces données.

S'agissant des modalités applicables à l'accès et la réutilisation par les acteurs privés des données protégées détenues par des organismes du secteur public, la Chambre de Commerce relève en particulier que plusieurs autorisations seront requises :

– de l'Autorité des données, d'une part,
– de l'organisme du secteur public qui détient les données, d'autre part, qui devra avoir marqué :
  (i) son accord de principe à la mise à disposition des données à caractère personnel (ou non personnel) aux fins d'accès et de réutilisation en inscrivant les données disponibles sur la **liste des ressources consultable tenue par le point d'information unique**[40] ;
  (ii) son accord spécifique à la mise à disposition des données à caractère personnel (ou non personnel) aux fins d'accès et de réutilisation.

L'Autorité des données[41] tiendra un registre public des accès et réutilisations de données autorisées.

e. *Concernant les acteurs compétents en matière de traitement ultérieur de données à caractère personnel (pilier 3) et d'accès et de réutilisation de données (pilier 4) (Titre III du Projet de loi)*

Dans le prolongement de l'article 7, paragraphe (2) du DGA qui impose aux Etats membres la désignation d' « un ou de plusieurs organismes compétents », le Projet de loi désigne « un organisme compétent » unique dénommé « **Autorité des données** », avec pour mission d'octroyer ou de refuser les accès et les réutilisations de certaines catégories de données protégées détenues par des organismes du secteur public, dont les données à caractère personnel ainsi que les données protégées pour des motifs de confidentialité commerciale (y compris le secret d'affaires, le secret professionnel et le secret d'entreprise), de secret statistique, ou de protection des droits de propriété intellectuelle de tiers.

Le **Commissariat du Gouvernement à la protection des données**[42] auprès de l'Etat sera chargé des missions à l'« Autorité des données » suivant le Projet de loi, pour permettre une application cohérente de la loi.

Pour l'aider dans ses missions, il pourra compter sur l'assistance technique et la collaboration :

1) du Centre des technologies de l'information de l'Etat (**CTIE**) ;
2) du groupement d'intérêt économique PNED G.I.E. – Plateforme nationale d'échange de données, désigné comme « **LNDS** » ;

---

38 cf. article 20 du Projet de loi

39 interdisant la divulgation de toute information compromettant les droits et intérêts protégés par la future loi qu'ils pourraient avoir acquis malgré les garanties mises en place.

40 tel que décrit dans le titre e. p.13 du présent avis

41 cf. définition §5 du présent avis

42 L'exposé des motifs indique que cette désignation est faite « *pour des raisons d'économie budgétaire et de gestion efficace des finances publiques* » (cf. p. 32 et 33).

3) du « **tiers de confiance** »[43] mandaté par le CTIE, chargé d'effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données).

De même, dans le prolongement de ce qu'exige l'article 8 du DGA, un « **point d'information unique** » (prévu à l'article 7 du Projet de loi) sera instauré sous l'autorité du ministre en charge de la digitalisation, avec pour missions de :

1) recevoir les demandes d'accès et de réutilisation de données visées par le titre VI, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;
2) rendre disponibles au public toutes les informations pertinentes concernant l'application des articles 5 et 6 du DGA ainsi que toute autre information dont la publication est sollicitée par l'Autorité des données ;
3) mettre à disposition, conformément à l'article 8, paragraphe 2 du DGA, par voie électronique une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données conformément au titre VI, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

La Chambre de Commerce fait valoir qu'il serait pertinent d'utiliser l'option ouverte par l'article 8 paragraphe 3 du DGA qui permet au point d'information unique, d'être un canal d'informations distinct, simplifié et bien documenté pour les PME et les jeunes pousses afin de répondre à leurs besoins et à leurs capacités en matière de demande de réutilisation des données (visées à l'article 3, paragraphe 1 du DGA).

Enfin, il est institué sous l'autorité du ministre en charge de la digitalisation, un Conseil consultatif de la valorisation des données dans un environnement de confiance, désigné « **Conseil consultatif** » dans le Projet de loi, qui agira comme organe consultatif de l'Autorité des données, et sera chargé de se prononcer sur toute question en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données qui lui est soumise par le ministre en charge de la digitalisation; et de promouvoir l'accès et la réutilisation des données visés au titre VI (pilier 4).

Pour le surplus, la composition et le fonctionnement de ce Conseil consultatif sont fixés par le projet de règlement grand-ducal qui accompagne le Projet de loi.

*

CONCERNANT LE PROJET DE REGLEMENT GRAND-DUCAL

L'article 1er du Projet de règlement grand-ducal qui accompagne le Projet de loi détermine la **composition et le fonctionnement – convocation, mode de délibération, et attributions – du « Conseil consultatif de la valorisation des données dans un environnement de confiance »**[44] (tel qu'institué par l'article 8 du Projet de loi), dénommé le « Conseil consultatif ».

Le Comité consultatif est l'instance consultative qui devra rendre un avis à l'Autorité des données. Ses avis seront publiés en annexe des autorisations qui seront adoptées par ladite Autorité des données en réponse à des demandes (i) de traitement ultérieur de données personnelles (article 27 du Projet de loi) ou (ii) d'accès et de réutilisation des données (article 28 du Projet de loi).

Sous le commentaire des articles, les auteurs indiquent que « *[la] composition plurielle du Conseil consultatif par des représentants des ministères et administrations de l'État lui permet de rendre un avis cohérent et équilibré prenant en compte les exigences liées aux droits protégés et les modalités techniques applicables aux traitements ultérieurs de données à caractère personnel et aux réutilisations des données* ».

---

43 Le tiers de confiance est défini comme « toute entité fonctionnellement indépendante des entités publiques visées au titre V, des organismes du secteur public détenant les données et du réutilisateur de données visé au titre VI, qui remplit les conditions prévues à l'article 6 » suivant l'article 2, paragraphe 2, point 3° du Projet de loi.

44 cf. article 1er du Projet de règlement grand-ducal

Par ailleurs, les auteurs indiquent qu'à des fins de transparence administrative, il est prévu qu'un procès-verbal soit établi pour chaque réunion du Conseil consultatif, ce que la Chambre de Commerce salue.

Ces dispositions n'appellent pas d'autres commentaires particuliers de la part de la Chambre de Commerce.

Quant aux articles 2 à 6 du Projet de règlement grand-ducal, ils précisent les règles relatives au calcul et à la perception des redevances (prévues à l'article 30 du Projet de loi) que l'Autorité des données est habilitée à percevoir, dans le cadre du traitement des demandes de réutilisation des catégories de données.

En cas de perception de redevances, la Chambre de Commerce relève avec satisfaction que :

– d'une part, que les redevances devront pouvoir être acquittées en ligne, pour des raisons de simplification administrative ;
– d'autre part, que l'Autorité des données prendra des mesures pour inciter **la réutilisation des catégories de données par les PME et les jeunes pousses** conformément aux règles en matière d'aides d'État, en précisant que pour ces acteurs, la mise à disposition de ces données pourra se faire **moyennant une redevance réduite ou à titre gratuit, afin d'éviter de constituer un obstacle à leur entrée sur le marché;**
– à cette fin, l'Autorité des données pourra établir une **liste des catégories de réutilisation pour lesquelles les données à des fins de réutilisation sont mises à disposition moyennant une redevance réduite ou à titre gratuit. Cette liste, ainsi que les critères utilisés pour l'établir, seront rendus publics**.

Plus subsidiairement, la Chambre de Commerce relève qu'une erreur matérielle s'est glissée dans le dispositif du Projet de règlement grand-ducal (référence à un article erronée). Ainsi, sous l'article 6, il y a lieu de lire : « *Le calcul des coûts consiste à faire la somme de tous les éléments de coûts éligibles prévus à l'article **5**6, paragraphe 1er (...)* ».

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure de d'approuver les projets de loi et de règlement grand-ducal sous avis, sous réserve de la prise en compte de ses observations.

Impression: CTIE – Division Imprimés et Fournitures de bureau

20250514_Avis_3

N° 8395[6]

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AVIS DE LA CHAMBRE DES METIERS

(7.1.2025)

RESUME STRUCTURE

Le projet de loi sous avis vise à mettre en œuvre au Luxembourg les dispositions du règlement UE 2022/898 sur la gouvernance européenne des données relatives à la réutilisation des données protégées du secteur public.

En complément aux règles de gouvernance en matière de réutilisation des données, le projet de loi sous avis propose de favoriser la circulation des données à caractère personnel entre entités publiques via l'instauration de trois nouveaux principes, à savoir : (i) le principe de la licéité des traitements de données opérés par les entités publiques en lien avec l'exécution leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique ; (ii) la définition d'un cadre juridique pour les traitements ultérieurs de données à caractère personnel entre les autorités publiques ; (iii) et le principe selon lequel les administrés ne doivent fournir leurs données qu'une seule fois aux entités publiques (ou principe once only).

Le projet de loi sous avis propose de constituer une Autorité des données sous la dépendance du Commissariat du gouvernement à la protection des données pour se prononcer sur les demandes de réutilisation des données protégées du secteur public émanant du secteur privé, mais aussi pour apprécier les demandes de traitements ultérieurs de données à caractère personnel à l'intérieur de la sphère publique.

L'Autorité des données sera accompagnée par un Conseil consultatif de la valorisation des données dans un environnement de confiance (ou Conseil consultatif), et il est proposé de créer un point d'information pour la réutilisation des données protégées et pour les traitements ultérieurs de données à caractère personnel sous l'autorité du ministre ayant la digitalisation dans ses attributions.

Un projet de règlement grand-ducal est joint afin de préciser la composition et le mode de fonctionnement du Conseil consultatif, ainsi que la procédure applicable concernant la perception des redevances pour les réutilisations de données protégées.

Si la Chambre des Métiers salue les nouveaux principes et procédures mises en œuvre elle estime que l'Autorité des données devrait être constituée sous la forme d'un établissement public qui serait indépendant de la tutelle de l'Etat à l'instar de la CNPD ou de l'Autorité nationale de concurrence afin de garantir auprès des citoyens une parfaite neutralité politique des décisions de cette autorité.

La mission du Conseil consultatif semble antinomique, car il est difficilement compréhensible comment cet organe peut intervenir tant en amont des décisions de l'Autorité des données que par après sur saisine des parties prenantes à un traitement ultérieur ou une réutilisation. De plus la composition de ce Conseil devrait être modifiée afin d'intégrer des experts conformément à sa mission.

La Chambre des Métiers estime de plus que la notion d'« entité publique », notion essentielle puisqu'elle délimite le champ d'application des nouvelles mesures favorisant la circulation des données à caractère personnel dans la sphère publique, devrait être mieux précisée dans la loi.

Tout en accueillant favorablement l'obligation once only, la Chambre des Métiers considère que des incertitudes concernant sa portée devraient aussi être levées. Ces incertitudes résultent non seulement des exceptions à l'application du once only qui sont trop largement prévues, mais aussi de la question du champ d'application du nouveau cadre légal pour les traitements ultérieurs entre entités publiques : à défaut de précisions, la portée réelle du once only risque d'être très réduite si l'on considère que les protocoles once only sont juridiquement à qualifier de traitements ultérieurs de données.

Enfin, la Chambre des Métiers propose que l'activité de tiers de confiance soit intégrée à celle de prestataire de service d'intermédiation qui est organisée et favorisée par le règlement sur la gouvernance des données, il conviendrait aussi que cette activité soit définie par le droit d'établissement applicable au Luxembourg.

*

Par sa lettre du 12 juin 2024, Madame la Ministre de la digitalisation a bien voulu demander l'avis de la Chambre des Métiers au sujet du projet de loi repris sous rubrique.

*

1. CONSIDERATIONS GENERALES

Le règlement (UE) 2022/868 du Parlement et du Conseil portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (ou « règlement sur la gouvernance des données »[1]) est applicable depuis le 24 septembre 2023.

Le règlement sur la gouvernance des données vise à améliorer la gouvernance des données car il est constaté que les données sont au cœur de la transformation de l'économie et de la société par les technologies numériques.

En fixant des règles favorisant la disponibilité des données du secteur public, le règlement sur la gouvernance des données propose de réduire la fracture numérique et d'éviter des effets de verrouillage, notamment vis-à-vis des micro, petites et moyennes entreprises.[2]

Afin de favoriser la circulation des données, le règlement sur la gouvernance des données fixe en premier lieu les principes applicables à la réutilisation des données protégées détenues par le secteur public sans pour autant créer de nouvelle base juridique pour le traitement des données protégées.

Les données protégées comprennent les données à caractère personnel, mais aussi les données protégées pour des motifs de confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise, les données protégées par le secret statistique, et les données protégées par des droits de propriété intellectuelle.[3]

---

1 En anglais « Data Gouvenance Act » (ou DGA)

2 Considérant (2) du règlement sur la gouvernance des données.

3 Article 3 (1) du règlement sur la gouvernance des données

Le règlement sur la gouvernance des données vise ensuite à augmenter la confiance dans les intermédiaires de données qui peuvent être des services d'intermédiation de données ou des organisations altruistes en matière de données.[4]

Les prestataires de services d'intermédiation de données sont des intermédiaires neutres qui doivent respecter un certain nombre de règles définies par le règlement sur la gouvernance des données permettant d'augmenter la confiance dans le partage des données en donnant plus de contrôle aux personnes concernées et aux services détenteurs.

Ces intermédiaires de données sont donc des modèles alternatifs aux grandes plateformes du numériques parce qu'ils s'engagent à respecter une parfaite neutralité fondée sur l'absence de conflit d'intérêts, mais aussi, ils s'engagent à ne pas entrer en concurrence avec les utilisateurs[5] et à assurer un caractère équitable, transparent et non discriminatoire de leurs offres de service.[6]

Le règlement sur la gouvernance des données vise aussi à renforcer les mécanismes de partage de données dans l'Union européenne avec la création du Comité européen de l'innovation dans le domaine des données.[7]

En plus de mettre en œuvre au Luxembourg le règlement sur la gouvernance des données concernant la réutilisation des données protégées du secteur public, le projet de loi sous avis propose de développer la circulation des données protégées à l'intérieur du secteur public, notamment par la mise en œuvre d'un principe « phare » suivant lequel un administré n'est censé fournir qu'une seule fois les données le concernant aux entités publiques, ou principe du once only.

1.1. Définition des acteurs compétents au Luxembourg en matière de gouvernance des données

1.1.1. *L'Autorité des données*

Le règlement sur la gouvernance des données impose la désignation dans chaque Etat membre d'un organisme pour assister techniquement les organismes du secteur public lorsqu'ils doivent octroyer ou refuser l'accès aux fins de la réutilisation des données protégées.[8]

Le projet de loi propose de constituer l'Autorité des données sous la dépendance du Commissariat du gouvernement à la protection des données qui est une administration placée sous l'autorité du Premier ministre et de lui attribuer compétence pour octroyer ou refuser les demandes de réutilisation des données protégées détenues par des organismes du secteur public, mais aussi pour se prononcer sur les demandes de traitement ultérieur de données à caractère personnel entre entités publiques.

Afin d'assurer l'impartialité des décisions de l'Autorité des données relatives à des demandes de traitements ultérieurs portant sur des données à caractère personnel[9], le projet de loi sous avis pose le principe d'indépendance entre le personnel chargé de la mission de délégué à la protection des données auprès de certains ministères ou communes[10] et le personnel qui sera chargé de prendre les décisions en matière de réutilisation de données à caractère personnel.[11]

---

4 Il n'y a pas de contrainte tarifaire en cas d'intermédiation contrairement à l'altruisme où les personnes concernées ne peuvent recevoir de compensation que pour les coûts qu'elles supportent lorsqu'elles mettent leurs données à disposition pour des motifs d'intérêt général (considérant 45 du règlement sur la gouvernance des données).

5 L'intermédiaire n'est autorisé qu'à fournir les services suivants : stockage temporaire, organisation, conversion, anonymisation et pseudonymisation le cas échéant.

6 Un service d'intermédiation de données est un modèle d'affaire transparent, contrairement aux actuels « data brockers » dont l'objectif est d'accroitre la valeur des données sans établir de relation commerciale entre les détenteurs de données et les utilisateurs, mais en intervenant sur plusieurs marchés.

7 Le Comité européen sera composé d'experts et aura pour mission de proposer des lignes directrices pour favoriser des espaces européens communs de données dans des domaines stratégiques impliquant à la fois les acteurs privés et publics dans des secteurs tels que la santé, l'environnement, l'énergie, l'agriculture, la mobilité, la finance, l'industrie manufacturière, ou l'administration publique.

8 Article 7 du règlement sur la gouvernance des données.

9 Demandes visées à la section Ii du titre VII du projet de loi sous avis.

10 Articles 56 et suivants de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données.

11 Projet d'article 4 (6).

Il est prévu que les décisions de cette autorité pourront être contestées devant le Tribunal administratif.[12]

1.1.2. *Le Centre des technologies de l'information de l'Etat et la Plateforme nationale d'échange de données*

Le projet de loi désigne le Centre des technologies de l'information de l'Etat (le CTIE) et la Plateforme nationale d'échange de données (le groupement d'intérêt économique LNDS) pour assister l'Autorité des données dans l'accomplissement de ses missions.

Ces entités seront désignées, avec l'Autorité des données, comme « organismes compétents » au sens de l'article 7 du règlement sur la gouvernance des données.

1.1.3. *L'activité de tiers de confiance*

Le projet de loi encadre l'activité de « tiers de confiance » afin de garantir que des réutilisations ou des traitements ultérieurs soient effectués de manière à éviter le risque de réidentification des personnes concernées.

Un tiers de confiance est une entité fonctionnellement indépendante, non seulement des entités publiques effectuant une réutilisation de données à caractère personnel, mais aussi des entités publiques détenant les données et des réutilisateurs de données.[13]

L'activité de tiers de confiance est d'effectuer les opérations techniques de stockage, mais aussi de gérer les clés d'anonymisation ou de pseudonymisation et d'agrégation des données.

L'activité de tiers de confiance est encadrée par le projet de loi sous avis qui liste une série de grands principes à respecter, dont celui de disposer des ressources suffisantes, de respecter une obligation de secret, et de soumettre son personnel à certaines contraintes, que ce soit de qualification, de ne pas avoir de conflit d'intérêt, et de soumettre ce personnel à une obligation de secret professionnel.

1.1.4. *Le point d'information unique*

Suivant l'article 8 du règlement sur la gouvernance des données, les Etats membres doivent définir un point d'information unique pour la réutilisation des données protégées détenues par le secteur public.

Les points d'information uniques des Etats sont chapeautés par un point d'accès unique européen mettant à disposition un registre électronique consultable des données disponibles au niveau des points d'information uniques nationaux ainsi que d'autres informations sur la manière de demander des données par l'intermédiaire de ces points d'information uniques nationaux.

Le projet de loi sous avis instaure le point d'information unique pour le Luxembourg sous l'autorité du ministre ayant la digitalisation dans ses attributions, avec possibilité de sous-traiter cette mission au groupement d'intérêt économique de la Plateforme nationale d'échange de données (LNDS).

Le point d'information aura pour missions, d'une part de réceptionner les demandes de réutilisation et de les transférer à l'Autorité des données, et, d'autre part, d'établir et de rendre accessible la liste de données protégées qui sont disponibles à l'accès et à la réutilisation.

1.1.5. *Le Conseil consultatif*

Le projet de loi désigne un conseil consultatif de la valorisation des données dans un environnement de confiance (ou « Conseil consultatif ») ayant pour mission de régler d'éventuelles difficultés d'application de la loi en rendant des avis à l'Autorité des données, et d'être un organe de réflexion.

1.2. Le nouveau principe de licéité pour les traitements primaires de données à caractère personnel par une entité publique

Le projet de loi sous avis ajoute au Luxembourg le principe de licéité des traitements de données à caractère personnel par une entité publique lorsque les traitements sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.[14]

---

12 Projet d'article 38.

13 Projet d'article 2 (2) 3°.

14 Article 3 du projet de loi sous avis.

Il faut souligner que ce principe n'est pas imposé par le règlement sur la gouvernance des données mais qu'il s'inscrit conformément au règlement européen sur la protection des données (RGPD) et qu'il permet d'assoir la licéité des traitements de données à caractère personnel sur cette base sans pour autant que ces traitements ne soient spécifiquement visés par une loi particulière.[15]

1.3. L'échange des données entre entités publiques, ou le principe once only

Le principe once only est prévu par le Titre IV du projet de loi sous avis pour les « *informations et données à caractère personnel obtenues par les entités publiques auprès d'une autre entité publique* ».

Ce nouveau principe peut être qualifié comme étant l'obligation pour les entités publiques d'échanger entre elles les informations et les données à caractère personnel dans l'intérêt d'un administré.

Le principe once only s'applique dans deux situations : la première est lorsque l'administré effectue une demande ou une déclaration en application d'une disposition légale ou réglementaire ; la seconde est lorsque l'administration doit informer l'administré de son droit à une prestation ou à un avantage prévu par une disposition législative ou réglementaire.

L'introduction du principe once only va imposer aux entités publiques d'échanger entre elles les informations et données à caractère personnel qui sont nécessaires, soit pour traiter une demande d'un administré, soit pour informer un administré de son droit à une prestation ou à un avantage.

1.3.1. *Le protocole once only*

Afin de mettre en œuvre le principe once only, il sera demandé à chaque entité publique de recenser les informations et données à caractère personnel qu'elle peut obtenir auprès d'une autre entité publique (ci-après « entité publique source »).

Ce recensement permettra à l'entité publique de pouvoir notifier à l'entité publique source les échanges des informations et des données à caractère personnel qui auront été identifiées.

L'entité publique source sera alors tenue de répondre dans le délai d'un mois, soit en confirmant la disponibilité et la possibilité d'échange, soit en informant de la non-détention ou de l'impossibilité de l'échange, avec copie de la réponse au ministre ayant la digitalisation dans ses attributions.

En cas de disponibilité et possibilité d'échange, les entités publiques concernées doivent signer un protocole once only endéans un délai de 3 mois.

Le protocole once only formalise chaque type d'échange d'informations et de données à caractère personnel entre les entités publiques concernées et contient les informations permettant d'assurer la conformité de l'échange avec les exigences liées au RGPD.[16]

Chaque protocole once only sera publié par l'Autorité des données via un registre qui comprendra les différents protocoles en vigueur ; les protocoles qui ne sont plus applicables resteront publiés pendant une durée de 2 ans avec la mention de leur non-application.

1.3.2. *Les limites à l'obligation once only*

Le projet de loi sous avis énumère de manière très large différentes limites au once only, ce qui permet de considérer que l'obligation de partage des données entre les entités publiques ne sera qu'une obligation de principe assorties de plusieurs limites et garde-fous.

On notera ainsi le cas « d'impossibilité » pour une entité publique d'appliquer le once only, ou si les informations ou données à caractère personnel ne peuvent pas faire l'objet d'un échange entre entités publiques « en raison de leur nature ».[17]

---

15 Article 6 (1) e) du RGPD prévoit que : « Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie: (…) e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;», et le considérant 45 suivant lequel « Une disposition légale peut suffire pour fonder plusieurs opérations de traitement basées sur une obligation légale à laquelle le responsable du traitement est soumis ou lorsque le traitement est nécessaire pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique. »

16 Les informations sont listées par le projet d'article 13 du projet de loi sous avis.

17 Projet d'article 11 paragraphes 4 & 6.

Une autre limite à l'obligation once only est l'application du principe suivant lequel les informations et les données à caractère personnel collectées et échangées ne peuvent être utilisées ultérieurement à des fins de détection systématique d'une fraude, sauf habilitation législative spéciale.[18]

Enfin, dans la situation où c'est l'administration qui informe l'administré d'un droit, le principe once only est accompagné de l'obligation de l'entité publique d'informer l'administré de son droit de s'opposer à la poursuite du traitement de ses données à caractère personnel et d'obtenir que les informations ou données à caractère personnel obtenues à la suite de l'échange entre entités soient détruites.[19]

1.4. Le traitement ultérieur de données à caractère personnel par les entités publiques

Le titre V du projet de loi sous avis encadre le traitement ultérieur de données à caractère personnel par une entité publique en listant de manière limitative les finalités dans lesquelles un tel traitement ultérieur est autorisé et en imposant des conditions d'anonymisation et de pseudonymisation.

1.4.1. *Les finalités*

La liste limitative des finalités pour les traitements ultérieurs de données à caractère personnel par des entités publiques est la suivante : a) l'analyse statistique ; b) les activités d'éducation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ; c) la recherche scientifique dans l'intérêt public ou dans l'intérêt général ; d) l'évaluation et la planification des politiques envisagées ou planifiées par le Gouvernement et approuvées par décision du Gouvernement en conseil, ou en ce qui concerne les communes, envisagées ou planifiées par le Conseil communal ; e) lorsque la mise en œuvre d'un accord international requiert la communication d'informations ou lorsque le traitement ultérieur des données à caractère personnel permet de répondre aux demandes d'informations officielles provenant de gouvernements étrangers ou d'organisations internationales approuvées par décision du Gouvernement en conseil ; f) les activités de développement, d'évaluation, de démonstration, de sécurité et d'innovation de dispositifs ou de services ; g) la formation, le test et l'évaluation d'algorithmes, y compris dans les dispositifs, les systèmes d'intelligence artificielle et les applications numériques.[20]

1.4.2. *Le principe d'anonymisation*

Pour les traitements ultérieurs de données à caractère personnel, le projet de loi sous avis pose le principe de l'anonymisation des données assorti de possibilités de simple pseudonymisation, voire d'absence d'anonymisation ou de pseudonymisation, dès lors qu'il est rapporté que le traitement ultérieur de données anonymisées, respectivement pseudonymisées, ne permet pas d'atteindre la finalité poursuivie.[21]

Le projet de loi distingue les traitements ultérieurs au sein d'une même entité publique, pour lesquels l'obligation d'anonymisation ou de pseudonymisation s'applique pour les données dites sensibles listées par l'article 9 et 10 paragraphe 1er du RGPD, des traitements ultérieurs par une autre entité publique, ou par plusieurs entités, pour lesquels la demande doit être soumise à l'autorisation de l'Autorité des données suivant une procédure très détaillée (cf. infra § 1.6.).[22]

On notera aussi que l'entité publique qui détient les données concernées aura toujours la possibilité de refuser le partage malgré l'autorisation de l'Autorité des données, et que, dans ce cas, le projet de loi sous avis prévoit la possibilité, pour l'entité qui demande les données, de saisir le Conseil consultatif.[23]

---

18 Projet d'article 11 paragraphe 3 alinéa 1er.

19 Projet d'article 11 paragraphe 3.

20 Projet d'article 15 paragraphe 1.

21 Projet d'article 16 paragraphes 2 et 3.

22 Projet d'article 27.

23 Projet d'article 18 paragraphe 2.

1.5. Le nouveau cadre pour la réutilisation des données protégées du secteur public

Une nouvelle gouvernance est proposée concernant la réutilisation des données protégées secteur public par des « réutilisateurs » de données.

La réutilisation de données protégées vise « *l'utilisation, par des personnes physiques ou morales, de données détenues par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les données ont été produites, à l'exception de l'échange de données entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public*. »[24]

1.5.1. *Champ d'application*

Les données protégées sont celles bénéficiant d'une des protections suivantes : la confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise ; le secret statistique ; la protection des droits de propriété intellectuelle de tiers ; la protection des données à caractère personnel.

Certaines catégories de données sont exclues de la réutilisation, à savoir : a) les données détenues par des entreprises publiques ; b) les données détenues par des radiodiffuseurs de service public ; c) les données détenues par des établissements culturels et des établissements d'enseignement ; d) les données détenues par des organismes du secteur public qui sont protégées pour des raisons de sécurité publique, de défense ou de sécurité nationale ; e) les données dont la fourniture est une activité qui ne relève pas de la mission de service public dévolue aux organismes du secteur public concernés.[25]

1.5.2. *Finalités*

Le projet de loi sous avis soumet l'autorisation à l'accès et la réutilisation des données protégées du secteur public à la liste limitative des finalités suivantes : a) l'analyse statistique ; b) les activités d'éducation, de formation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ; c) la recherche scientifique dans l'intérêt public ou dans l'intérêt général ; d) le développement, l'évaluation, la démonstration, la sécurité et l'innovation de technologies ; e) le développement, l'évaluation, la démonstration, la sécurité et l'innovation de produits ; f) l'évaluation des politiques publiques luxembourgeoises ou européennes.[26]

1.5.3. *Les garanties pour préserver le caractère protégé des données*

L'accès aux données à des fins de réutilisation n'est octroyé que lorsque l'organisme du secteur public ou l'organisme compétent, à la suite d'une demande de réutilisation, a fait en sorte que les données aient été, soit anonymisées s'il s'agit de données à caractère personnel, soit, pour les autres données protégées, modifiées, agrégées ou traitées selon toute autre méthode de contrôle de la divulgation dans le cas des informations commerciales confidentielles, y compris des secrets d'affaires et des contenus protégés par des droits de propriété intellectuelle.

Concernant la réutilisation de données personnelles, l'article 22 du projet de loi sous avis impose le respect des conditions suivantes : 1°) l'autorisation de l'accès et de la réutilisation par l'Autorité des données ; 2°) l'accord de l'entité publique qui détient les données ; 3°) l'absence d'atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ; 4°) l'anonymisation ou la pseudonymisation des données préalablement à leur accès et à leur réutilisation ; 5°) le respect de l'environnement de traitement sécurisé visé à l'article 36 du projet de loi.

Concernant la réutilisation de données non personnelles, l'article 23 du projet de loi impose le respect des conditions suivantes : 1°) l'autorisation de l'accès et de la réutilisation par l'Autorité des données ; 2°) l'accord de l'entité publique qui détient les données ; 3°) l'absence d'atteinte disproportionnée aux droits protégés ; 4°) que les données soient « *modifiées, agrégées, supprimées ou traitées selon toute*

---

24 Article 2, point 2) du règlement sur la gouvernance des données.

25 Article 3 (2) du règlement sur la gouvernance des données.

26 Article 20 du projet de loi sous avis.

autre méthode de contrôle de la divulgation préalablement à leurs accès et à leur réutilisation » et 5°) le respect de l'environnement de traitement sécurisé visé à l'article 36.

1.6. *La procédure d'autorisation devant l'Autorité des données*

Le titre VII du projet de loi sous avis précise la procédure applicable pour les demandes d'autorisation des traitements ultérieurs des données à caractère personnel soumis à autorisation et pour les demandes de réutilisation de données protégées du secteur public.

La forme et le contenu de la demande de traitement ultérieur ou d'accès et de réutilisation, ainsi que la procédure d'instruction de la demande par l'Autorité des données, sont détaillées dans le projet de loi sous avis.

Conformément au règlement sur la gouvernance des données, le projet de loi fixe un délai de 2 mois avec possibilité que ce délai soit augmenté pour une durée allant jusqu'à 30 jours en cas de demande « *exceptionnellement détaillée et complexe* ».[27]

L'Autorité des données pourra exiger, pour chaque demande de réutilisation, une redevance pour couvrir les frais administratifs occasionnés par le traitement de la demande et par la mise à disposition des données dans l'environnement de traitement sécurisé.

Il est renvoyé à un règlement grand-ducal le soin de détailler la procédure applicable à la perception de cette redevance, projet qui est utilement joint au projet de loi sous avis.[28]

Le projet de loi sous avis prévoit une publicité des autorisations et impose à l'Autorité des données la tenue d'un registre public des traitements ultérieurs de données à caractère personnel et des accès et réutilisations de données autorisées.[29]

1.7. Les services d'intermédiation et les organisations altruistes

Le projet de loi sous avis fixe le cadre national en matière de gouvernance pour les intermédiaires en matière de données, à savoir les services d'intermédiation et les organisations altruistes.

1.7.1. *Les services d'intermédiation de données*

Un service d'intermédiation en matière de données est un service de mise en relation entre des détenteurs de données, qui peuvent être directement des personnes concernées, et des utilisateurs de données, afin d'établir des relations commerciales.

Suivant le règlement sur la gouvernance des données, trois types de service d'intermédiation de données sont envisageables en fonction des personnes qu'ils mettront en relation.

Un service d'intermédiation pourra, en fonction de son modèle d'affaires, mettre en relation :

- soit des détenteurs et des utilisateurs de données, comme par exemple une plateforme d'échanges B2B ;
- soit des personnes concernées et des utilisateurs de données, comme par exemple un système de gestion des informations personnelles ;
- soit par le biais d'une coopérative de données, comme par exemple une mutualisation des données en vue d'une gestion commune.[30]

Afin de susciter la confiance dans ces intermédiaires, le règlement sur la gouvernance des données impose dans chaque Etat membre la mise en place d'une procédure de notification de l'activité, ainsi que le respect d'une série de règles contraignantes telles que l'interdiction pour le service d'intermédiation d'utiliser les données à d'autres fins que leur mise à disposition des utilisateurs de données, la définition d'un plan de continuation en cas d'insolvabilité, la garantie que l'accès aux données ne soit pas discriminatoire.

Le projet de loi sous avis désigne la Commission nationale pour la protection des données (CNPD) comme autorité compétente pour la notification pour des services d'intermédiation de données, et encadre sa mission de contrôle, et organise le pouvoir de sanction.

---

27 Article 29 (2) du projet de loi sous avis.

28 Article 30 du projet de loi sous avis.

29 Article 34 du projet de loi sous avis.

30 Article 10 du règlement sur la gouvernance des données.

1.7.2. *Les organisations altruistes en matière de données*

L'altruisme en matière de données est une modalité de partage de données, qu'elles soient à caractère personnel ou pas.

Les organisations altruistes échappent au régime des services d'intermédiations parce qu'elles ne visent pas à établir des relations commerciales, et qu'elles interviennent à titre gratuit.

Le partage des données est fondé sur le consentement des personnes concernées et pour des motifs d'intérêt général qui doivent être prévus par le droit national.

Afin de susciter la confiance dans les organisations altruistes en matière de données, le règlement sur la gouvernance des données leur impose le respect d'une série de grands principes, dont l'exercice des activités dans un but non lucratif, une indépendance juridique et une conformité avec le recueil de règles adoptées par la Commission.

Les organisations altruistes en matière de données doivent s'enregistrer au niveau national et le projet de loi désigne la CNPD comme autorité responsable de la tenue du registre public national des organisations altruistes en matière de données reconnues.

*

2. OBSERVATIONS PARTICULIERES

2.1. L'Autorité des données

2.1.1. *L'indépendance de l'Autorité des données à l'égard du pouvoir politique*

La Chambre des Métiers est consciente que l'Etat Luxembourgeois œuvre pour garantir un maximum de sécurité des informations liées aux activités des entités publiques.

Cependant, considérant le rôle de la nouvelle Autorité des données et afin de garantir auprès des citoyens une parfaite neutralité politique des décisions de cette Autorité, un signal fort serait de constituer cette autorité sous la forme d'un établissement public qui serait indépendant de la tutelle de l'Etat à l'instar de la CNPD ou de l'Autorité nationale de concurrence.

2.1.2. *Concernant l'activité du Conseil consultatif*

La Chambre des Métiers estime qu'une antinomie existe concernant les missions dévolues au Conseil consultatif, car cet organe peut intervenir, en amont comme conseil de l'Autorité des données[31], et en aval, dans le cadre de recours administratifs.

En effet, le conseil consultatif pourra notamment être saisi pour avis :

- par une entité publique qui se voit opposer un refus de partage d'un traitement ultérieur de données à caractère personnel par une autre entité publique[32] ;
- par un réutilisateur de données qui se voit opposer un refus d'accès de réutilisation de données par un organisme du secteur public malgré l'autorisation préalable de l'Autorité des données.[33]

Afin de renforcer le point des avis de cet organe, il conviendrait de mieux préciser ces missions et aussi de revoir sa composition.

La composition et le mode de fonctionnement du Conseil consultatif sont précisés par le règlement grand-ducal sous avis qui propose la désignation de onze délégués représentant le Premier ministre et différents ministères, ainsi que le Commissariat du gouvernement à la protection des données auprès de l'Etat et le CTIE. La Chambre des Métiers note, dans ce contexte, l'absence des experts délégués de la part de la CNPD.

---

31 Article 8 paragraphe 2 point 1° du projet de loi sous avis.

32 Article 18 (2) du projet de loi sous avis.

33 Article 22 (3) du projet de loi sous avis.

Il est aussi prévu que le Conseil consultatif peut demander l'avis d'experts, mais sans voix délibérative.

Concernant la mission purement consultative de ce Conseil, la Chambre des Métiers estime que des experts et des spécialistes en matière de données devraient faire partie intégrante de cet organe.

2.2. Les incertitudes concernant la notion d'entité publique

La notion d'entité publique telle que proposé par le projet de loi sous avis est fondamentale puisqu'elle définit le champ d'application des trois nouveaux principes suivants : (i) le principe de licéité basé sur l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, (ii) le principe du once only, et (iii) le principe des traitements ultérieurs de données à caractère personnel dans la sphère public.

La notion d'entité publique proposée par le projet de loi sous avis est la suivante : « *un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal aux fins d'application des dispositions des titres IV et V. Toutefois, ne sont pas considérées comme entité publique aux fins d'application de la présente loi :*

a) les autorités compétentes visées par l'article 2, point 7° de loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale lorsqu'elles effectuent un traitement de données à caractère personnel relevant du champ d'application de la loi du 1er août 2018 ;

b) les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif, lorsqu'elles effectuent un traitement de données à caractère personnel dans l'exercice de leurs fonctions juridictionnelles ; »[34]…

La Chambre des Métiers regrette que le projet de règlement grand-ducal qui doit définir les personnes morales d'utilité publique devant être qualifiées d'entités publiques pour l'application du titre IV (le principe once only) et du titre V (les traitements ultérieurs) ne soit pas annexé au projet de loi.

Considérant les missions d'intérêt public qui lui sont légalement dévolue, la Chambre des Métiers ne s'opposerait pas à ce que les Chambres professionnelles soient, dans la mesure où elles effectuent une mission d'intérêt public, ajoutées dans la liste des entités publiques pour l'application des titres IV et V du projet de loi sous avis.

2.3. Concernant le champ d'application des nouvelles dispositions en matière de réutilisation

La nouvelle gouvernance concernant la réutilisation des données protégées par des réutilisateurs de données vise, non pas les données détenues par des entités publiques, mais les données détenues par des « organismes du secteur public.»

Au sens du règlement sur la gouvernance des données, les organismes du secteur publics sont ceux présentant toutes les caractéristiques suivantes : « *a) ils ont été créés pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial ; b) ils sont dotés de la personnalité juridique ; et c) soit ils sont financés majoritairement par l'État, les autorités régionales ou locales ou d'autres organismes de droit public, soit leur gestion est soumise à un contrôle de ces autorités ou organismes, soit leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou locales ou d'autres organismes de droit public* ».[35]

La Chambre des Métiers, tout en partageant que la définition d'organisme du secteur public est identique à la notion « d'organisme de droit public » qui délimite le champ d'application rationae

34 Projet d'article 2 (2)

35 Article 2, point 18 du règlement sur la gouvernance des données.

personae de la législation spécifique des marchés publics, estime que les chambres professionnelles sont à qualifier d'organisme du secteur public.[36]

Cette analyse est d'ailleurs confirmée par le champ d'application de la loi du 14 septembre 2018 relative à une administration transparente et ouverte bien que cette loi utilise la notion de « document administratif ».[37]

Il est aussi partagé que la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public, bien qu'ayant un champ d'application plus large qui inclut dans une certaine mesure les documents détenus par les entreprises publiques, reprend la notion identique de documents détenus par les « organismes du secteur public » mais sans proposer de définition.[38]

2.4. Incertitudes sur la portée de l'obligation once only

Parmi les exceptions à la mise en œuvre du once only, deux exceptions devraient être mieux précisées, à savoir :

- la possibilité pour l'entité publique détenant des données de ne pas échanger les informations et les données à caractère personnel nécessaire à la mise en œuvre du once only en cas « d'impossibilité dûment motivée » ;
- la possibilité pour un règlement grand-ducal de déterminer les informations ou données à caractère personnel qui, « en raison de leur nature », ne pourront pas faire l'objet d'un échange entre entités publiques.[39]

En effet, les notions « « d'impossibilité dûment motivée » et d'impossibilité par « nature » » ne sont pas explicites et elles devraient être mieux cernées dans le texte de la loi.

Une autre incertitude réside sur la considération que nombre de protocoles once only devraient être qualifiés juridiquement de traitement ultérieur, et qu'une lecture stricte du champ d'application du nouveau cadre légal pour les traitements ultérieurs limitera sensiblement le champ d'application du once only.

De plus, tout en soulignant la sécurité juridique pour les personnes concernées que le cadre légal propose pour les traitements ultérieurs de données à caractère personnel par les entités publiques, la Chambre des Métiers estime que ce cadre légal ne devrait pas remettre en cause des dispositions légales ou conventionnelles, existantes ou à venir, qui peuvent organiser, dans le cadre de besoins plus spécifiques, des traitements ultérieurs conformément aux possibilités énumérées par le RGPD.[40]

Aux fins de sécurité et d'efficacité juridique, la Chambre des Métiers estime que l'articulation de ce nouveau cadre légal avec d'autres possibilités légales ou conventionnels de traitements ultérieurs devrait être précisée dans le projet de loi sous avis, comme ceci est d'ailleurs mentionné dans le commentaire des articles.[41]

2.5. Concernant l'activité de tiers de confiance et celle de prestataire de services d'intermédiation

Le projet de loi sous avis propose de distinguer l'activité de prestataire de service d'intermédiation, activité qui est définie et encadré par le règlement sur la gouvernance des données, de celle de « tiers de confiance » qui ne l'est pas.

---

36 Il est renvoyé à l'article 2. d) de la Loi du 8 avril 2018 sur les marchés publics

37 Suivant l'article 1er de cette loi, les « documents administratifs » sont les « documents détenus par les administrations et services de l'État, les communes, les syndicats de communes, les établissements publics placés sous la tutelle de l'État ou sous la surveillance des communes ainsi que les personnes morales fournissant des services publics, dans la mesure où les documents sont relatifs à l'exercice d'une activité administrative. Elles ont également accès aux documents détenus par la Chambre des Députés, le Conseil d'État, le Médiateur, la Cour des comptes et les Chambres professionnelles, qui sont relatifs à l'exercice d'une activité administrative. »

38 Suivant l'article 2 point 2° de cette loi sont organismes du secteur public : « l'État, les communes, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités, ou un ou plusieurs de ces organismes de droit public.»

39 Projet d'article 11 paragraphes 4 & 6.

40 Il est renvoyé à l'article 6 (4) du RGPD.

41 Ad article 15, page 52.

La Chambre des Métiers regrette cette distinction et estime que l'activité de « tiers de confiance » devrait être incluse dans celle d'un prestataire de service d'intermédiation.

Une autre incertitude concerne le champ de l'activité de ce « tiers de confiance » car le projet de loi sous avis prévoit implicitement que le CTIE mandate un tel prestataire dans le cadre de ses missions techniques.[42]

Ce mandat implicite est d'ailleurs mentionné dans l'exposé des motifs qui explique que « *pour éviter d'éventuels conflits d'intérêts et pour maintenir la confiance des citoyens dans une gestion prudente de leurs données par les acteurs publics, la loi prévoit la possibilité pour le Centre des technologies de l'information de l'État de recourir aux services d'un tiers de confiance*. »[43]

De plus, la Chambre des Métiers estime que l'activité de prestataire de services d'intermédiation, et de tiers de confiance, devrait être appréhendée par le droit d'établissement applicable au Luxembourg.

2.6. La question des redevances réduites ou gratuites pour certaines réutilisations à des fins non commerciales

Le projet de loi également joint pour avis prévoit que l'Autorité des données fixera pour chaque demande de réutilisation une redevance pour couvrir les frais administratifs occasionnés par le traitement de la demande et par la mise à disposition des données dans l'environnement de traitement sécurisé et il renvoie à un règlement grand-ducal le soin de déterminer la procédure de perception.[44]

Le projet de règlement grand-ducal également joint pour avis ouvre, conformément à l'option ouverte par l'article 6 paragraphe 4 du règlement sur la gouvernance des données, qu'une redevance réduite ou gratuite vis-à-vis de certains utilisateurs, notamment les utilisations à des fins de recherche scientifique, les PME et les jeunes pousses, doit être prévue par l'Autorité des données.

La Chambre des Métiers salue cette option, mais elle estime qu'une politique nationale visant à favoriser l'altruisme en matière de données devrait aussi être proposée conformément à l'article 16 du règlement sur la gouvernance des données, qui mentionne cette possibilité pour notamment « *aider les personnes concernées à mettre à disposition volontairement, à des fins d'altruisme en matière de données, des données à caractère personnel les concernant détenues par des organismes du secteur public, et déterminer les informations nécessaires qui doivent être fournies aux personnes concernées en ce qui concerne la réutilisation de leurs données dans l'intérêt général*.»

*

La Chambre des Métiers ne peut approuver le projet de loi et le projet de règlement grand-ducal lui soumis pour avis que sous la réserve expresse de la prise en considération de ses observations ci-avant formulées.

Luxembourg, le 7 janvier 2025

Pour la Chambre des Métiers

Le Directeur Général,
Tom WIRION

Le Président,
Tom OBERWEIS

---

42 Les projet d'articles 5 (2) et (3); 31 (5) 1° c) et 2° c) et 32 (3), 35 (2) et 36 mentionnent le « tiers de confiance mandaté par le Centre. »

43 Exposé des motifs, page 32.

44 Article 30 du projet de loi sous avis.

Impression: CTIE – Division Imprimés et Fournitures de bureau
8395 - Dossier consolidé : 161

20250522_AmendementParlementaire

N° 8395[7]
N° 8395A[1]
N° 8395B[1]

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

PROJET DE LOI

relative à la désignation des organismes et autorités compétents et au point d'information uniquement prévus aux articles 7, 8, 13 et 23 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)

PROJET DE LOI

relative à

1° la valorisation des données dans un environnement de confiance ;

2° la mise en oeuvre du principe « once only » ;

3° la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4° la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil

du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AMENDEMENTS PARLEMENTAIRES

DEPECHE DU PRESIDENT DE LA CHAMBRE DES DEPUTES AU PRESIDENT DU CONSEIL D'ETAT

(22.4.2025)

Monsieur le Président,

J'ai l'honneur de vous soumettre ci-après une série d'amendements au projet de loi sous rubrique, adoptés par la Commission de l'Enseignement supérieur, de la Recherche et de la Digitalisation (ci-après « Commission ») lors de sa réunion du 22 avril 2025.

Je joins en annexe, à toutes fins utiles, un texte coordonné du projet de loi sous rubrique reprenant les amendements parlementaires exposés *sub* III (**figurant en caractères gras et soulignés**) et les adaptations découlant directement de la scission du projet de loi exposée *sub* I ainsi que les erreurs matérielles que la Commission propose de rectifier exposées *sub* II (figurant en caractères soulignés).

*

I. SCISSION DU PROJET DE LOI INITIAL

La Commission décide de scinder le projet de loi n°8385 en deux projets de loi distincts, à savoir :

– le projet de loi n°8395A relative à la désignation des organismes et autorités compétents et au point d'information uniquement prévus aux articles 7, 8, 13 et 23 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;
– le projet de loi n°8395B relative à
  1° la valorisation des données dans un environnement de confiance ;
  2° la mise en œuvre du principe « *once only* » ;
  3° la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;
  4° la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Le projet de loi n°8395A comprend les articles 4, paragraphe 1er, 7, paragraphe 1er, 39, 40, 44 et 45 du projet de loi n°8395 initial.

En ce qui concerne la structure du projet de loi n°8395A, cette dernière se présente comme suit :

Projet de loi 8395	*Projet de loi 8395A*
Article 4, paragraphe 1er	Article 1er
Article 7, paragraphe 1er	Article 2
Article 39	Article 3
Article 40	Article 4
Article 44	Article 5
Article 45	Article 6

La renumérotation des articles à la suite de cette scission, nécessite l'adaptation de deux renvois dans le dispositif du projet de loi n°8395A :

1° à l'article 40 du projet de loi n°8395, devenant l'article 4 du projet de loi, il y a lieu de remplacer le renvoi à l'article 39 par un renvoi à l'article 3 ;

2° à l'article 45 du projet de loi n°8395, devenant l'article 6 du projet de loi n°8395A, il y a lieu de remplacer le renvoi à l'article 44 par un renvoi à l'article 5.

Le projet de loi n°8395B comprend les articles du projet de loi n°8395 initial ne faisant pas partie du projet de loi n°8395A.

À toutes fins utiles, un tableau de concordance du projet de loi n°8395B est joint à la présente.

À noter que l'intégration des articles 44 et 45 dans le projet de loi n°8395A a comme conséquence qu'au titre VII du projet de loi n°8395B, la section II ne contient plus d'article. Il y a dès lors lieu de supprimer cette section et de renuméroter les sections suivantes.

Cette scission est motivée par l'urgence de notifier les différents organismes et autorités compétents prévus au règlement (UE) 2022/868 à la Commission européenne. En effet, la Commission a appris que la Commission européenne insiste que ces organismes et autorités, qui auraient déjà dû lui être notifiés le 24 septembre 2023, seront communiqués dans les meilleurs délais.

La Commission propose dès lors de procéder dans les meilleurs délais au vote des dispositions prévoyant la désignation de ces entités dorénavant prévues au projet de loi n°8395A et laissant le temps nécessaire à tous les acteurs impliqués dans la procédure législative de dûment analyser les autres dispositions du projet de loi n°8395 qui sont dorénavant prévues au projet de loi n°8395B.

*

II. REDRESSEMENT D'ERREURS MATERIELLES

La Commission a procédé au redressement des erreurs matérielles suivantes dans le dispositif du projet de loi n°8395B :

1° à l'article 7, paragraphe 1er (initialement l'article 7, paragraphe 2, du projet de loi n°8395), il convient de rectifier les erreurs matérielles suivantes :

a) à la lettre a), devenant le point 1° en vertu de l'amendement 13 repris ci-dessous, il y a lieu de remplacer les termes « par le » par le terme « au » ;

b) à la lettre c), devenant le point 3° en vertu de l'amendement 13 repris ci-dessous, il y a lieu d'insérer une virgule après les termes « paragraphe 2 » ;

2° à l'article 16, il convient de redresser les erreurs matérielles suivantes :

a) au paragraphe 1er, il y a lieu d'insérer une virgule après les termes « paragraphe 1er » ;

b) au paragraphe 2, il y a lieu d'insérer une virgule après les termes « paragraphe 1er » ;

c) au paragraphe 3, il y a lieu d'insérer des virgules après les termes « paragraphe 1er » et « point 2° » ;

3° à l'article 17, paragraphe 2, il y a lieu d'insérer une virgule après les termes « paragraphe 1er » ;

4° à l'article 22, paragraphe 1er, il convient de redresser les erreurs matérielles suivantes :

a) à la phrase liminaire, il y a lieu d'insérer une virgule après les termes « point 2° » ;

b) à lettre a), il y a lieu d'insérer une virgule après les termes « paragraphe 2 » ;

5° à l'article 23, paragraphe 1er, il convient de redresser les erreurs matérielles suivantes :

a) à la phrase liminaire, il y a lieu d'insérer une virgule après les termes « points 1° à 3° » ;

b) au point 2°, lettre a), il y a lieu d'insérer une virgule après les termes « paragraphe 2 » ;

6° à l'article 27, paragraphe 2, point 4°, il y a lieu d'insérer une virgule après les termes « paragraphe 3 » ;

7° à l'article 28, il convient de redresser les erreurs matérielles suivantes :

a) au paragraphe 1er, point 14°, il y a lieu d'insérer des virgules après les termes « point 2, lettre b) » et « article 23, paragraphe 2 » ;

b) au paragraphe 3, il y a lieu d'insérer une virgule après les termes « paragraphe 3 » ;

c) au paragraphe 4, point 3°, il y a lieu d'insérer une virgule après les termes « paragraphe 3 » ;

8° à l'article 31, il convient de redresser les erreurs matérielles suivantes :

a) au paragraphe 2, point 1°, lettre b), point i, il y a lieu d'insérer une virgule après les termes « paragraphe 2 » ;

b) au paragraphe 5, alinéa 1er, il y a lieu d'insérer des virgules après les termes « point 7 » et « point 10° » ;

*

III. AMENDEMENTS

Amendements visant le dispositif du projet de loi n°8395A

Amendement 1

L'article 4, paragraphe 1er, du projet de loi n°8395, devenant l'article 1er du projet de loi n°8395A, est amendé comme suit :

« **Art. 4 1er. ~~Autorité des données~~ Organismes compétents**

~~(1)~~ Le Commissariat du Gouvernement à la protection des données auprès de l'État **~~est chargé des missions attribuées à l'Autorité des données par la présente loi. Dans l'exercice de ces missions, le Commissariat du Gouvernement à la protection des données auprès de l'État est désigné ci-après par le terme « Autorité des données »~~ est désigné organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), dénommé ci-après « règlement (UE) 2022/868 », habilité, conformément à l'article 7, paragraphe 2, du même règlement, à octroyer ou à refuser l'accès aux fins de réutilisation des données**.».

Commentaire :

L'amendement sous rubrique modifie l'article 4, paragraphe 1er, du projet de loi initial qui devient l'article 1er du projet de loi n°8395A. Plus précisément, le libellé est amendé pour prévoir que le Commissariat du Gouvernement à la protection des données auprès de l'État est désigné organisme compétent au sens de l'article 7, paragraphe 1er, du règlement sur la gouvernance des données. Par ailleurs, ledit Commissariat sera également habilité à octroyer ou refuser l'accès aux fins de réutilisation des données tel que le prévoit l'article 7, paragraphe 2, du même règlement. Ainsi, le nouveau libellé regroupe la plupart des éléments initialement prévus à l'article 4, paragraphes 1er et 2, du projet de loi initial, et n'apporte dès lors aucun élément nouveau au dispositif en ce qui concerne son fond.

Amendement 2

L'article 7, paragraphe 1er, du projet de loi n°8395, devenant l'article 2 du projet de loi n°8395A, est amendé comme suit :

« **Art. ~~7~~ 2. Point d'information unique**

~~(1)~~ Sous l'autorité du ministre ayant la digitalisation dans ses attributions est instauré un point d'information unique conformément à l'article 8 du règlement (UE) 2022/868**~~, ci-après désigné par le terme « point d'information unique »~~**. ».

Commentaire :

Étant donné que les articles suivants du projet de loi n°8395A ne renvoient pas au point d'information unique, le bout de phrase prévoyant une forme abrégée pour désigner ce point d'information unique dans la suite du dispositif devient superfétatoire.

Amendement 3

L'article 39 du projet de loi n°8395, devenant l'article 3 du projet de loi n°8395A, est amendé comme suit :

« **Art. ~~39~~ 3. Autorité compétente en matière d'intermédiation de données**

La Commission nationale pour la protection des données, désignée ci-après **~~par le terme~~** « CNPD », est l'autorité compétente pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données, telle que visée à l'article 13 du règlement (UE) 2022/868. ».

Commentaire :

L'amendement sous rubrique adapte l'intitulé de l'article 39 du projet de loi n°8395, devenant l'article 3 du projet de loi n°8395A, afin de faciliter la distinction entre les articles 3 et 5 du projet de loi n°8395A.

Par ailleurs, cet amendement prévoit la suppression des termes « par le terme » étant donné que ces derniers sont superfétatoires.

Amendement 4

L'intitulé de l'article 40 du projet de loi n°8395, devenant l'article 4 du projet de loi n°8395A, est amendé comme suit :

« **Art. ~~40~~ 4. Pouvoirs de l'autorité compétente en matière d'intermédiation de données** ».

Commentaire :

Cet amendement vise à faciliter la distinction entre les articles 4 et 6 du projet de loi n°8395A.

Amendement 5

L'intitulé de l'article 44 du projet de loi n°8395, devenant l'article 5 du projet de loi n°8395A, est amendé comme suit :

« **Art. ~~44~~ 5. Autorité compétente en matière d'altruisme des données** ».

Commentaire :

Cet amendement vise à faciliter la distinction entre les articles 3 et 5 du projet de loi n°8395A.

Amendement 6

L'intitulé de l'article 45 du projet de loi n°8395, devenant l'article 6 du projet de loi n°8395A, est amendé comme suit :

« **Art. ~~45~~ 6. Pouvoirs de l'autorité compétente en matière d'altruisme des données** ».

Commentaire :

Cet amendement vise à faciliter la distinction entre les articles 4 et 6 du projet de loi n°8395A.

Amendement 7

À la suite de l'article 6 du projet de loi n°8395A est inséré un article 7 nouveau libellé comme suit :

« **Art. 7. Intitulé de citation**

La référence à la présente loi se fait sous la forme suivante : « loi du […] relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 ». ».

Commentaire :

Étant donné que l'article 2 du projet de loi n°8395B tel qu'amendé renvoie au projet de loi n°8395A, la Commission estime qu'il est opportun de prévoir un intitulé de citation.

Amendements visant le dispositif du projet de loi n°8395B

Amendement 8

L'article 1er du projet de loi n°8395, devenant l'article 1er du projet de loi n°8395B, est amendé comme suit :

1° le titre est modifié comme suit :

« **Art. 1er. Objet** » ;

2° le paragraphe 1er, point 4°, est modifié comme suit :

« 4° l'accès et la réutilisation de certaines catégories de données collectées par les organismes du secteur public, en application du chapitre II du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant

le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), ~~désigné~~ **dénommé** ci-après ~~par le terme~~ « règlement (UE) 2022/868 » ; ».

Commentaire :

L'amendement sous rubrique vise à apporter deux adaptations d'ordre légistique au dispositif de l'article 1er du projet de loi n°8395B.

Amendement 9

L'article 2 du projet de loi n°8395, devenant l'article 2 du projet de loi n°8395B, est amendé comme suit :

« **Art. 2. Définitions**

(1) ~~Sauf dispositions particulières contraires au paragraphe 2 du présent article, les~~ **Les** termes et expressions ~~utilisés dans la présente loi ont la signification que leur donnent le~~ **définis à l'article 2 du** règlement (UE) 2022/868 et ~~le~~ **à l'article 4 du** règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), **dénommé** ci-après ~~désigné par le terme~~ « règlement (UE) 2016/679 »**, ont la même signification dans la présente loi**.

(2) Aux fins de la présente loi, on entend par :

1° « anonymisation » : le processus consistant à rendre anonymes des données à caractère personnel de telle sorte que la personne concernée à laquelle celles-ci se rapportent ne soit pas ou plus identifiée ou identifiable, compte tenu de l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique directement ou indirectement ;

2° « Autorité des données » : le Commissariat du Gouvernement à la protection des données auprès de l'État ;

~~2°~~ **3°** « entité publique » : un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal aux fins d'application des dispositions des titres IV et V. Toutefois, ne sont pas considérées comme entité publique aux fins d'application de la présente loi :

a) la Chambre des Députés ;

b) les autorités compétentes visées par l'article 2, point 7°**,** de loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale lorsqu'elles effectuent un traitement de données à caractère personnel relevant du champ d'application ~~de la loi du 1er août 2018~~ **de la même loi** ;

c) les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif, lorsqu'elles effectuent un traitement de données à caractère personnel dans l'exercice de leurs fonctions juridictionnelles ;

4° « point d'information unique » : le point d'information unique visé à l'article 2 de la loi du […] relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 ;

~~3°~~ **5°** « tiers de confiance » : toute entité fonctionnellement indépendante des entités publiques visées au titre V, des organismes du secteur public détenant les données et du réutilisateur de données visés au titre VI, qui remplit les conditions prévues à l'article 6. ».

Commentaire :

L'amendement sous rubrique prévoit plusieurs adaptations de l'article 2 du projet de loi n°8395B.

Premièrement, le libellé du paragraphe 1er est adapté dans un souci de cohérence avec d'autres textes renvoyant à des définitions prévues dans un règlement européen. En l'occurrence, la Commission s'est inspirée d'une proposition de texte du Conseil d'État dans son avis relatif au projet de loi relatif à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique.

Deuxièmement, un point 2° nouveau est inséré au paragraphe 2 afin de définir la notion d'« Autorité des données ». Cette notion était définie à l'article 4, paragraphe 1er, du projet de loi initial. En conséquence de la scission du projet de loi, il est proposé d'intégrer la définition à l'article 2 du projet de loi n°8395B.

Troisièmement, le paragraphe 2, point 3°, est complété par une lettre a) nouvelle afin d'exclure explicitement la Chambre des Députés de la notion d'« entité publique ». Dans sa teneur initiale, le point 3° manque de clarté quant à la situation de la Chambre des Députés étant donné qu'elle n'est visée ni par l'énumération des entités visées par cette notion ni par celle des entités exclues de la notion. Après consultation, les organes compétents de la Chambre des Députés ont décidé que l'institution devrait être explicitement exclue de la notion d'« entité publique », de sorte qu'elle ne sera pas visée par les dispositions du projet de loi n°8395B s'appliquant aux entités publiques.

Quatrièmement, en conséquence de la scission du projet de loi n°8395 initial, la Commission insère un point 4° nouveau au paragraphe 2 prévoyant la définition de la notion de « point d'information unique ». Cette définition renvoie au point d'information unique prévu au projet de loi n°8395A.

Ces modifications entraînent la renumérotation de plusieurs points et lettres au paragraphe 2.

Amendement 10

L'article 4, paragraphes 2 à 6, du projet de loi n°8395, devenant l'article 4, paragraphes 1er à 5, du projet de loi n°8395B, est amendé comme suit :

« **Art. 4. Autorité des données**

(**2** **1**) L'Autorité des données **~~est désignée organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868, habilité, conformément à l'article 7, paragraphe 2, du même règlement, à~~** octro**~~y~~i~~r~~** ou refuse**~~r~~** l'accès aux fins de réutilisation des données **visées à l'article 3, paragraphe 1er, du règlement (UE) 2022/868** conformément aux dispositions des titres VI et VII.

(**~~3~~** **2**) L'Autorité des données est habilitée à autoriser ou refuser le traitement ultérieur de données à caractère personnel par les entités publiques conformément aux dispositions des titres V et VII.

(**~~4~~** **3**) L'Autorité des données a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** de collaborer étroitement avec le Centre des technologies de l'information de l'État, **~~dénommé~~ désigné** ci-après **~~par le terme~~** « Centre », le tiers de confiance mandaté par le Centre et le groupement d'intérêt économique PNED G.I.E. – Plateforme nationale d'échange de données, désigné ci-après **~~par le terme~~** « LNDS » ;

~~c)~~ **3°** de fonctionner comme organe de réflexion et d'impulsion dans le domaine du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation de données et de formuler des avis et des propositions en la matière au ministre ayant la digitalisation dans ses attributions ;

~~d)~~ **4°** de proposer au ministre ayant la digitalisation dans ses attributions des mesures en matière de politique de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données ;

~~e)~~ **5°** de conseiller, sur demande, le ministre ayant la digitalisation dans ses attributions sur les mesures en matière de traitement ultérieur de données à caractère personnel ;

~~f)~~ **6°** de promouvoir les bonnes pratiques à travers les entités publiques, en matière de traitement ultérieur de données à caractère personnel, et à travers les organismes de droit public en matière d'accès et de réutilisation de données ;

~~g)~~ **7°** de sensibiliser les entités publiques, les organismes de droit public et le public en matière de traitement ultérieur de données à caractère personnel et en matière d'accès et de réutilisation de données.

(**~~5~~** **4**) L'Autorité des données dispose des ressources nécessaires pour exercer ses missions. Il peut recourir aux services d'experts.

(**~~6~~** **5**) L'Autorité des données veille à ce que son personnel chargé des missions prévues aux paragraphes **~~2 et 3~~** **1er et 2** ne soit pas impliqué dans la préparation des demandes visées **~~à la~~**

~~section II du titre VII~~ **au titre VII, section II,** dans l'exercice de ses missions prévues aux articles 57 et 58 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. ».

Commentaire :

L'amendement sous rubrique apporte plusieurs adaptations au dispositif de l'article 4 du projet de loi n°8395B.

Premièrement, le paragraphe 1er (anciennement le paragraphe 2 du projet de loi n°8395) est adapté pour tenir compte du fait que le projet de loi n°8395A prévoit la désignation du Commissariat du Gouvernement à la protection des données auprès de l'État en tant qu'organisme compétent. Ainsi, il n'est plus nécessaire de réitérer ce point au projet de loi n°8395B. Cependant, comme le projet de loi n°8395B prévoit les procédures applicables aux demandes d'accès à la réutilisation de données, il y a lieu de préciser que les décisions d'octroi et de refus par l'organisme compétent se font en conformité avec les dispositions des titres VI et VII.

Deuxièmement, dans un souci de cohérence à travers l'intégralité du dispositif, la Commission procède à l'uniformisation des énumérations dans le dispositif du projet de loi n°8395B. En l'occurrence, il y a dès lors lieu de remplacer les lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Troisièmement, en raison de la renumérotation des paragraphes en conséquence de la scission du projet de loi initial, il y a lieu d'adapter le renvoi au paragraphe 5.

Enfin, des légères modifications d'ordre légistique sont effectuées.

Amendement 11

À l'article 5, paragraphes 2 à 4, du projet de loi n°8395, devenant l'article 5, paragraphes 2 à 4, du projet de loi n°8395B, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

Dans un souci de cohérence à travers le dispositif du projet de loi n°8395B, il est proposé de procéder à l'uniformisation de la forme des énumérations. En l'occurrence, ceci implique le remplacement des lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Amendement 12

À l'article 6, paragraphes 1er et 2, du projet de loi n°8395, devenant l'article 6, paragraphes 1er et 2, du projet de loi n°8395B, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

Dans un souci de cohérence à travers le dispositif du projet de loi n°8395B, il est proposé de procéder à l'uniformisation de la forme des énumérations. En l'occurrence, ceci implique le remplacement des lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Amendement 13

À l'article 7, paragraphes 2 et 3, du projet de loi n°8395, devenant l'article 7, paragraphes 1er et 2, du projet de loi n°8395B, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

Dans un souci de cohérence à travers le dispositif du projet de loi n°8395B, il est proposé de procéder à l'uniformisation de la forme des énumérations. En l'occurrence, ceci implique le remplacement des lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Amendement 14

L'article 8, paragraphe 1er, du projet de loi n°8395, devenant l'article 8, paragraphe 1er, du projet de loi n°8395B, est amendé comme suit :

« (1) Il est institué, sous l'autorité du ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions, un Conseil consultatif de la valorisation des données dans un environnement de confiance, **dénommé** ci-après **~~désigné par le terme~~** « Conseil consultatif ». ».

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 15

À l'article 9, paragraphe 3, du projet de loi n°8395, devenant l'article 9, paragraphe 3, du projet de loi n°8395B, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

Dans un souci de cohérence à travers le dispositif du projet de loi n°8395B, il est proposé de procéder à l'uniformisation de la forme des énumérations. En l'occurrence, ceci implique le remplacement des lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Amendement 16

L'article 11 du projet de loi n°8395, devenant l'article 11 du projet de loi n°8395B, est amendé comme suit :

1° au paragraphe 2, alinéa 2, les termes « l'alinéa qui précède » sont remplacés par les termes « l'alinéa 1er » ;

2° le paragraphe 4 est modifié comme suit :

a) l'alinéa 1er est modifié comme suit :

i. aux énumérations, les lettres sont remplacées par des points

ii. à la fin de la lettre a), devenant le point 1°, le terme « et » est supprimé ;

b) à l'alinéa 2, les termes « l'alinéa qui précède » sont remplacés par les termes « l'alinéa 1er ».

Commentaire :

L'amendement sous rubrique prévoit plusieurs adaptations d'ordre légistique.

Amendement 17

L'article 12 du projet de loi n°8395, devenant l'article 12 du projet de loi n°8395B, est amendé comme suit :

« **Art. 12. Recensement des informations et des données à caractère personnel disponibles auprès d'une autre entité publique**

(1) Les entités publiques sont tenues d'identifier, dans les meilleurs délais, les informations et données à caractère personnel qu'elles peuvent obtenir auprès d'une autre entité publique :

~~**a)**~~ **1°** dans le cadre du traitement effectué dans l'exercice de leurs missions des demandes et déclarations présentées par un administré ;

~~**b)**~~ **2°** pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

(2) Les entités publiques notifient, sans délai, les échanges d'informations et de données à caractère personnel identifiées conformément au paragraphe 1er aux entités publiques auprès desquelles les informations et données à caractère personnel pourraient être obtenues.

Dans un délai d'un mois à partir de la notification visée à l'alinéa ~~**qui précède**~~ **1er**, les entités publiques notifiées :

~~**a)**~~ **1°** certifient la disponibilité des informations et des données à caractère personnel à l'entité publique demanderesse et confirment que l'échange d'informations et de données à caractère personnel n'est pas impossible ; ou

~~**b)**~~ **2°** informent l'entité publique demanderesse du fait qu'elles ne détiennent pas les informations et les données à caractère personnel sollicitées ou que l'échange d'informations et de données à caractère personnel est impossible.

Une copie de l'information visée ~~**aux points a) et b) du présent paragraphe**~~ **à l'alinéa 2, points 1° et 2°,** est transmise au ministre ayant la digitalisation dans ses attributions.

(3) Dans les cas visés au **~~point a) du paragraphe qui précède~~** **au paragraphe 2, alinéa 2, point 2°**, les entités publiques concluent dans les meilleurs délais, et au plus tard après trois mois, le protocole visé à l'article 13. ».

Commentaire :

L'amendement sous rubrique vise plusieurs adaptations d'ordre légistique.

Amendement 18

À l'article 13, paragraphe 2, du projet de loi n°8395, devenant l'article 13, paragraphe 2, du projet de loi n°8395B, les termes « paragraphe qui précède » sont remplacés par les termes « paragraphe 1er ».

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 19

À l'article 14, paragraphe 2, du projet de loi n°8395, devenant l'article 14, paragraphe 2, du projet de loi n°8395, les termes « paragraphes qui précède » sont remplacés par les termes « paragraphe 1er ».

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 20

L'article 20, point 1°, du projet de loi n°8395, devenant l'article 20, point 1°, du projet de loi n°8395B, est amendé comme suit :

« 1° les conditions énoncées à la section II **~~du présent titre~~** sont remplies ; **~~et~~** ».

Commentaire :

L'amendement sous rubrique vise deux adaptations d'ordre légistique.

Amendement 21

L'article 27 du projet de loi n°8395, devenant l'article 27 du projet de loi n°8395B, est amendé comme suit :

1° au paragraphe 1er, points 13° et 15°, les termes « du présent paragraphe » sont supprimés ;

2° au paragraphe 3°, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

L'amendement sous rubrique vise des adaptations d'ordre légistique.

Amendement 22

L'article 28 du projet de loi n°8395, devenant l'article 28 du projet de loi n°8395B, est amendé comme suit :

1° le paragraphe 1er est modifié comme suit :

a) au point 12°, les termes « du présent paragraphe » sont supprimés ;

b) le point 13° est amendé comme suit :

« 13° pour les cas visés à l'article 22, paragraphe 2, point 2°, lettre a)**,** et à l'article 23, paragraphe **~~(~~**2**~~)~~,** point 2°, lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2**,** du règlement (UE) 2022/868 ; » ;

c) au point 14°, les termes « du présent paragraphe » sont supprimés ;

2° au paragraphe 5, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

L'amendement sous rubrique vise des adaptations d'ordre légistique.

Amendement 23

L'article 29, paragraphe 1er, du projet de loi n°8395, devenant l'article 29, paragraphe 1er, du projet de loi n°8395, est amendé comme suit :

« (1) Le dépôt des demandes visées à la section II ~~**du présent titre**~~, **dénommé** ci-après ~~**désignées**~~ la « demande », se fait auprès de l'Autorité des données. ».

Commentaire :

L'amendement sous rubrique vise deux adaptations d'ordre légistique.

Amendement 24

L'article 31 du projet de loi n°8395, devenant l'article 31 du projet de loi n°8395, est amendé comme suit :

1° au paragraphe 1er, aux énumérations, les lettres sont remplacées par des points ;

2° le paragraphe 2 est amendé comme suit :

a) au point 1°, lettre b), point ii, les termes « visés au point 2° du présent paragraphe » sont remplacés par le terme « concernés » ;

b) au point 2°, lettre b), point ii, les termes « visés au point 2° du présent paragraphe » sont remplacés par le terme « concernés » ;

c) au point 3°, les termes « du présent paragraphe » sont supprimés ;

3° le paragraphe 5, alinéa 2, est amendé comme suit :

a) au point 1°, lettre d), les termes « au point » sont remplacés par les termes « à la lettre » ;

b) au point 2°, lettre d), les termes « au point » sont remplacés par les termes « à la lettre ».

Commentaire :

L'amendement sous rubrique vise principalement des adaptations d'ordre légistique.

Les modifications opérées au paragraphe 2, points 1° et 2°, visent à tenir compte de renvois erronés. Il est proposé de remplacer ces renvois par des renvois aux organismes du secteur public compétents.

Amendement 25

À l'article 33 du projet de loi n°8395, devenant l'article 33 du projet de loi n°8395B, les termes « du présent titre » sont supprimés.

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 26

L'article 35 du projet de loi n°8395, devenant l'article 35 du projet de loi n°8395B, est amendé comme suit :

1° au paragraphe 2, alinéa 4, à l'énumération, les lettres sont remplacées par des points.

2° le paragraphe 4 est amendé comme suit :

« (4) Sous réserve d'autorisation de l'Autorité des données visée à l'article 31 et d'acquittement par le demandeur de la redevance visée à l'article 30 :

~~**a)**~~ **1°** le Centre, ou le tiers de confiance mandaté par le Centre, s'assure de la mise en œuvre les mesures visées au présent article conformément aux stipulations du plan de confidentialité ;

~~**b)**~~ **2°** le Centre :

~~**i.**~~ **a)** combine et traite les données provenant des entités publiques et des organismes du secteur public visés au paragraphe 1er, alinéa 3, pour lesquelles le traitement ultérieur et/ou l'accès et la réutilisation a été autorisé par l'Autorité des données ;

~~**ii.**~~ **b)** procède à la mise à disposition des données à caractère personnel visées au titre V et des données visées au titre VI dans l'environnement de traitement sécurisé, sous réserve des exigences prévues dans le plan de confidentialité et dans l'autorisation de l'Autorité des données. ».

Commentaire :

L'amendement sous rubrique vise des adaptations d'ordre légistique.

Amendement 27

L'article 36 du projet de loi n°8395, devenant l'article 36 du projet de loi n°8395B, est amendé comme suit :

1° au paragraphe 1er, alinéa 2, à l'énumération, les lettres sont remplacées par des points ;

2° au paragraphe 2, à l'énumération, les lettres sont remplacées par des points ;

3° au paragraphe 3, alinéa 1er, les termes « point b) » sont remplacés par les termes « point 2° » ;

4° au paragraphe 4, à l'énumération, les lettres sont remplacées par des points.

Commentaire :

L'amendement sous rubrique vise des adaptations d'ordre légistique.

Amendement 28

À l'article 43, paragraphe 1er, du projet de loi n°8395, devenant l'article 41, paragraphe 1er, du projet de loi n°8395B, le chiffre « 100.000 » est remplacé par celui de « 100 000 ».

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 29

L'article 46 du projet de loi n°8395, devenant l'article 42 du projet du projet de loi n°8395B, est amendé comme suit :

« **Art. ~~46~~ 42. Recours**

Un recours contre les décisions de la CNPD prises en application des ~~**sections I et II du présent titre**~~ **chapitres III et IV du Règlement (UE) 2022/686** est ouvert devant le Tribunal administratif qui statue comme juge du fond. ».

Commentaire :

L'amendement sous rubrique vise à tenir compte de la scission du projet de loi n°8395 qui a comme conséquence que le renvoi aux sections I et II n'est plus possible. Il est dès lors proposé de renvoyer aux décisions prises en vertu des chapitres III et IV du Règlement (UE) 2022/686.

*

Au nom de la Commission, je vous saurais gré de bien vouloir faire aviser par le Conseil d'État les amendements exposés ci-dessus.

En ce qui concerne le projet de loi n°8395A, je vous saurais gré de bien vouloir le faire aviser dans les meilleurs délais.

J'envoie copie de la présente à la Ministre déléguée auprès du Premier ministre, chargée des Relations avec le Parlement, avec prière de transmettre les amendements aux instances à consulter.

Veuillez agréer, Monsieur le Président, l'expression de ma considération très distinguée.

Le Président de la Chambre des Députés
Claude WISELER

Annexes :

[1] Tableau de concordance du projet de loi n°8395B

[2] Texte coordonné du projet de loi n°8395A proposé par la Commission

[3] Texte coordonné du projet de loi n°8395B proposé par la Commission

*

ANNEXE 1

Tableau de concordance du projet de loi n°8395B

Projet de loi 8395	*Projet de loi 8395B*
Article 1er	Article 1er
Article 2	Article 2
Article 3	Article 3
Article 4, paragraphes 2 à 6	Article 4, paragraphes 1er à 5
Article 5	Article 5
Article 6	Article 6
Article 7, paragraphes 2 et 3	Article 7, paragraphes 1er et 2
Article 8	Article 8
Article 9	Article 9
Article 10	Article 10
Article 11	Article 11
Article 12	Article 12
Article 13	Article 13
Article 14	Article 14
Article 15	Article 15
Article 16	Article 16
Article 17	Article 17
Article 18	Article 18
Article 19	Article 19
Article 20	Article 20
Article 21	Article 21
Article 22	Article 22
Article 23	Article 23
Article 24	Article 24
Article 25	Article 25
Article 26	Article 26
Article 27	Article 27
Article 28	Article 28
Article 29	Article 29
Article 30	Article 30
Article 31	Article 31
Article 32	Article 32
Article 33	Article 33
Article 34	Article 34
Article 35	Article 35
Article 36	Article 36
Article 37	Article 37
Article 38	Article 38
Article 41	Article 39
Article 42	Article 40
Article 43	Article 41
Article 46	Article 42
Article 47	Article 43

ANNEXE 2

TEXTE COORDONNE DU PROJET DE LOI N°8395A

PROJET DE LOI

relative à la désignation des organismes et autorités compétents et au point d'information uniquement prévus aux articles 7, 8, 13 et 23 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)

Art. ~~4~~ 1er. ~~Autorité des données~~ Organismes compétents

(1) Le Commissariat du Gouvernement à la protection des données auprès de l'État **~~est chargé des missions attribuées à l'Autorité des données par la présente loi. Dans l'exercice de ces missions, le Commissariat du Gouvernement à la protection des données auprès de l'État est désigné ci-après par le terme « Autorité des données »~~ est désigné organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), dénommé ci-après « règlement (UE) 2022/868 », habilité, conformément à l'article 7, paragraphe 2, du même règlement, à octroyer ou à refuser l'accès aux fins de réutilisation des données**.

Art. ~~7~~ 2. Point d'information unique

~~(1)~~ Sous l'autorité du ministre ayant la digitalisation dans ses attributions est instauré un point d'information unique conformément à l'article 8 du règlement (UE) 2022/868**~~, ci-après désigné par le terme « point d'information unique »~~**.

Art. ~~39~~ 3. Autorité compétente en matière d'intermédiation de données

La Commission nationale pour la protection des données, désignée ci-après **~~par le terme~~** « CNPD », est l'autorité compétente pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données, telle que visée à l'article 13 du règlement (UE) 2022/868.

Art. ~~40~~ 4. Pouvoirs de l'autorité compétente en matière d'intermédiation de données

Dans le cadre des tâches qui lui sont assignées à l'article ~~39~~ 3, la CNPD dispose des pouvoirs de contrôle tels que prévus à l'article 14 du règlement (UE) 2022/868.

Art. ~~44~~ 5. Autorité compétente en matière d'altruisme des données

La CNPD est l'autorité compétente responsable du registre public national des organisations altruistes en matière de données reconnues, tel que visé à l'article 23 du règlement (UE) 2022/868.

La CNPD tient et met à jour régulièrement le registre public national des organisations altruistes en matière de données reconnues, conformément à l'article 17, paragraphe 1er, du règlement (UE) 2022/868.

Art. ~~45~~ 6. Pouvoirs de l'autorité compétente en matière d'altruisme des données

Dans le cadre des missions qui lui sont assignées à l'article 44 5, la CNPD dispose des pouvoirs de contrôle, tels que prévus à l'article 24 du règlement (UE) 2022/868.

Art. 7. Intitulé de citation

La référence à la présente loi se fait sous la forme suivante : « loi du […] relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 ».

*

ANNEXE 3

TEXTE COORDONNE DU PROJET DE LOI N°8395B

PROJET DE LOI

relative à

1° la valorisation des données dans un environnement de confiance ;

2° la mise en œuvre du principe « *once only* » ;

3° la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4° la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

TITRE I^er^ – Dispositions préliminaires

Art. 1^er^. Objet

(1) La présente loi vise :

1° le traitement de données à caractère personnel par les entités publiques dans le cadre de l'exécution des missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies, agissant en leur qualité de responsable du traitement ;

2° l'échange d'informations et de données à caractère personnel obtenues par une entité publique auprès d'une autre entité publique dans le cadre du traitement d'une demande ou d'une déclaration d'un administré, ou pour informer l'administré sur ses droits au bénéfice éventuel d'une prestation ou d'un avantage prévu par des dispositions législatives ou réglementaires et pour pouvoir lui attribuer éventuellement lesdits prestations ou avantages ;

3° le traitement ultérieur de données à caractère personnel par les entités publiques pour les finalités déterminées dans la présente loi ;

4° l'accès et la réutilisation de certaines catégories de données collectées par les organismes du secteur public, en application du chapitre II du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), **~~désigné~~ dénommé** ci-après **~~par le terme~~** « règlement (UE) 2022/868 » ;

5° la fourniture de services d'intermédiation de données, en application du chapitre III du règlement (UE) 2022/868 ; et

6° la mise à disposition de données à des fins altruistes, en application du chapitre IV du règlement (UE) 2022/868.

(2) Les dispositions de la présente loi s'appliquent sans préjudice des dispositions plus spécifiques relatives au traitement de données à caractère personnel.

Art. 2. Définitions

(1) **~~Sauf dispositions particulières contraires au paragraphe 2 du présent article, les~~ Les** termes et expressions **~~utilisés dans la présente loi ont la signification que leur donnent le~~ définis à l'article 2 du** règlement (UE) 2022/868 et **~~le~~ à l'article 4 du** règlement (UE) 2016/679 du Parlement

européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), **dénommé** ci-après ~~**désigné par le terme**~~ « règlement (UE) 2016/679 »**, ont la même signification dans la présente loi**.

(2) Aux fins de la présente loi, on entend par :

1° « anonymisation » : le processus consistant à rendre anonymes des données à caractère personnel de telle sorte que la personne concernée à laquelle celles-ci se rapportent ne soit pas ou plus identifiée ou identifiable, compte tenu de l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique directement ou indirectement ;

2° « Autorité des données » : le Commissariat du Gouvernement à la protection des données auprès de l'État ;

~~**2°**~~ **3°** « entité publique » : un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal aux fins d'application des dispositions des titres IV et V. Toutefois, ne sont pas considérées comme entité publique aux fins d'application de la présente loi :

a) la Chambre des Députés ;

b) ~~**a)**~~ les autorités compétentes visées par l'article 2, point 7°**,** de loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale lorsqu'elles effectuent un traitement de données à caractère personnel relevant du champ d'application ~~**de la loi du 1er août 2018**~~ **de la même loi** ;

c) ~~**b)**~~ les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif, lorsqu'elles effectuent un traitement de données à caractère personnel dans l'exercice de leurs fonctions juridictionnelles ;

4° « point d'information unique » : le point d'information unique visé à l'article 2 de la loi du […] relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 ;

~~**3°**~~ **5°** « tiers de confiance » : toute entité fonctionnellement indépendante des entités publiques visées au titre V, des organismes du secteur public détenant les données et du réutilisateur de données visés au titre VI, qui remplit les conditions prévues à l'article 6.

TITRE II – Traitement de données à caractère personnel par les entités publiques nécessaire à l'exécution de la mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Art. 3. Licéité du traitement de données à caractère personnel par les entités publiques nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Les entités publiques sont habilitées à traiter les données à caractère personnel nécessaires aux fins relevant de l'exécution de leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies par une disposition de droit de l'Union européenne ou de droit national applicable.

TITRE III – Acteurs compétents en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données

Art. 4. Autorité des données

(~~**2**~~ **1**) L'Autorité des données ~~**est désignée organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868, habilité, conformément à l'article 7, paragraphe 2, du même règlement, à**~~ octroyi~~er~~ ou refuse~~r~~ l'accès aux fins de réutilisation des données **visées à l'article 3, paragraphe 1er, du règlement (UE) 2022/868** conformément aux dispositions des titres VI et VII.

(**~~3~~** **2**) L'Autorité des données est habilitée à autoriser ou refuser le traitement ultérieur de données à caractère personnel par les entités publiques conformément aux dispositions des titres V et VII.

(**~~4~~** **3**) L'Autorité des données a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** de collaborer étroitement avec le Centre des technologies de l'information de l'État, **~~dénommé~~** **désigné** ci-après **~~par le terme~~** « Centre », le tiers de confiance mandaté par le Centre et le groupement d'intérêt économique PNED G.I.E.– Plateforme nationale d'échange de données, désigné ci-après **~~par le terme~~** « LNDS » ;

~~c)~~ **3°** de fonctionner comme organe de réflexion et d'impulsion dans le domaine du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation de données et de formuler des avis et des propositions en la matière au ministre ayant la digitalisation dans ses attributions ;

~~d)~~ **4°** de proposer au ministre ayant la digitalisation dans ses attributions des mesures en matière de politique de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données ;

~~e)~~ **5°** de conseiller, sur demande, le ministre ayant la digitalisation dans ses attributions sur les mesures en matière de traitement ultérieur de données à caractère personnel ;

~~f)~~ **6°** de promouvoir les bonnes pratiques à travers les entités publiques, en matière de traitement ultérieur de données à caractère personnel, et à travers les organismes de droit public en matière d'accès et de réutilisation de données ;

~~g)~~ **7°** de sensibiliser les entités publiques, les organismes de droit public et le public en matière de traitement ultérieur de données à caractère personnel et en matière d'accès et de réutilisation de données.

(**~~5~~** **4**) L'Autorité des données dispose des ressources nécessaires pour exercer ses missions. Il peut recourir aux services d'experts.

(**~~6~~** **5**) L'Autorité des données veille à ce que son personnel chargé des missions prévues aux paragraphes **~~2 et 3~~** **1er et 2** ne soit pas impliqué dans la préparation des demandes visées **~~à la section II du titre VII~~** **au titre VII, section II,** dans l'exercice de ses missions prévues aux articles 57 et 58 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Art. 5. Assistance technique

(1) Le Centre et le LNDS, sont désignés organismes compétents au sens de l'article 7, paragraphe 1er, du règlement (UE) 2022/868 pour aider l'Autorité des données dans l'exercice de ses missions conformément aux dispositions de la présente loi.

(2) Le Centre a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** de mettre à disposition l'environnement de traitement sécurisé prévu à l'article 36 ;

~~c)~~ **3°** de fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles ;

~~d)~~ **4°** de s'assurer de la mise en œuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou à de modification, d'agrégation, de suppression et de traitement des informations et données selon toute autre méthode de contrôle de la divulgation des données conformément au plan de confidentialité, préalablement à la mise à disposition des données dans l'environnement de traitement sécurisé ;

~~e)~~ **5°** de collaborer étroitement avec l'Autorité des données, le tiers de confiance mandaté par le Centre, et le LNDS ;

~~f)~~ **6°** de proposer, sur décision du ministre ayant le Centre dans ses attributions, des services au LNDS relatifs à la mise en œuvre des dispositions de la présente loi.

(3) Le LNDS a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** d'aider les organismes du secteur public, le cas échéant, à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données conformément à leurs décisions spécifiques, y compris en ce qui concerne le territoire où le traitement des données est prévu et à aider les organismes du secteur public à mettre en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation des réutilisateurs, lorsque cela est réalisable en pratique ;

~~c)~~ **3°** de fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur en vertu de l'article 5, paragraphe 10**,** du règlement (UE) 2022/868 ;

~~d)~~ **4°** de collaborer étroitement avec l'Autorité des données, le Centre et le tiers de confiance mandaté par le Centre ;

~~e)~~ **5°** de fournir, sur demande, une assistance aux entités publiques et aux réutilisateurs de données dans le cadre de la préparation des demandes visées aux articles 27 et 28 et du plan de confidentialité visé à l'article 35.

(4) Le Centre et le LNDS :

~~a)~~ **1°** veillent à ce que le personnel chargé des missions conférées par la présente loi soit fonctionnellement indépendant des entités publiques visées au titre V, des organismes du secteur public détenant les données et des réutilisateurs de données visés au titre VI ;

~~b)~~ **2°** ne divulguent aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données ou permettant la divulgation de données qui sont protégées pour des motifs de protection des données à caractère personnel, de confidentialité commerciale, y compris le secret d'affaire, le secret professionnel, et le secret d'entreprise, de secrets statistique ou de protection de droits de propriété intellectuelle de tiers. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation ;

~~c)~~ **3°** désignent le personnel chargé des missions qui leurs sont conférées par la présente loi. Le personnel est désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données ;

~~d)~~ **4°** veillent à ce que le personnel chargé des missions qui leurs sont conférées par la présente loi ne soit pas chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données visés par la présente loi ;

~~e)~~ **5°** veillent à ce que le personnel chargé des missions qui leurs sont conférées par la présente loi n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui leurs sont conférés par la présente loi ou s'il y a incompatibilité, de fait ou de droit, avec l'exercice des tâches qui leurs sont conférées en application de la présente loi.

(5) Il est interdit au personnel du Centre et du LNDS chargé de l'exécution des missions qui leurs sont conférées par la présente loi d'avoir un intérêt quelconque, par lui-même ou par personne interposée, et sous quelque forme juridique que ce soit, dans une entité publique, dans un organisme du secteur public détenant les données ou dans un réutilisateur de données visées aux titres V et VI.

(6) Sans préjudice de l'article 23 du Code de procédure pénale, le personnel du Centre, du LNDS et du tiers de confiance chargé de l'exécution des missions conférées à ce dernier au sens de la présente loi est tenu au secret professionnel et passible des peines prévues à l'article 458 du Code pénal.

Art. 6. Tiers de confiance

(1) Le tiers de confiance a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** d'effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation

et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données ;

~~c)~~ **3°** de collaborer étroitement avec l'Autorité des données, le Centre et le LNDS.

(2) Le tiers de confiance :

~~a)~~ **1°** dispose de ressources humaines et techniques suffisantes et de l'expertise adéquate pour s'acquitter efficacement des missions dont il est chargé conformément à la présente loi ;

~~b)~~ **2°** ne divulgue aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données, ou susceptible de porter préjudice aux droits à la protection des données, à la propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation ;

~~c)~~ **3°** désigne le personnel chargé des missions qui lui sont conférées par la présente loi. Le personnel est désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données ;

~~d)~~ **4°** veille à ce que le personnel chargé des missions qui lui sont conférées par la présente loi ne soit pas chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données visés par la présente loi ;

~~e)~~ **5°** veille à ce que le personnel chargé des missions qui lui sont conférées par la présente loi n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui lui sont conférés par la présente loi ou s'il y a incompatibilité, de fait ou de droit, avec l'exercice des tâches qui lui sont conférées en application de la présente loi.

(3) Il est interdit au personnel du tiers de confiance chargé de l'exécution des missions conférées à ce dernier par la présente loi d'avoir un intérêt quelconque, par lui-même ou par personne interposée, et sous quelque forme juridique que ce soit, dans une entité publique, dans un organisme du secteur public détenant les données ou dans un réutilisateur de données visées aux titres V et VI.

(4) Sans préjudice de l'article 23 du Code de procédure pénale, le personnel du tiers de confiance chargé de l'exécution des missions conférées à ce dernier au sens de la présente loi est tenu au secret professionnel et passible des peines prévues à l'article 458 du Code pénal.

Art. 7. Point d'information unique

(~~2~~ **1**) Le point d'information unique a pour missions :

~~a)~~ **1°** de recevoir les demandes d'accès et de réutilisation de données visées ~~par le~~ au titre VI, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;

~~b)~~ **2°** de rendre disponibles au public toutes les informations pertinentes concernant l'application des articles 5 et 6 du règlement (UE) 2022/868 ainsi que toute autre information dont la publication est sollicitée par l'Autorité des données ;

~~c)~~ **3°** de mettre à disposition, conformément à l'article 8, paragraphe 2, du règlement (UE) 2022/868, par voie électronique une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données conformément au titre VI, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

(~~3~~ **2**) Pour les cas visés au titre V, le point d'information unique a pour mission :

~~a)~~ **1°** de recevoir les demandes de traitement ultérieur de données à caractère personnel visées par le titre V, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à

l'Autorité des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;

~~b)~~ **2°** de mettre à disposition par voie électronique la liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles en vue de leur traitement ultérieur, visée à l'article 18, paragraphe 3 ;

~~c)~~ **3°** de rendre disponibles au public toutes les informations dont la publication est demandée par l'Autorité des données.

Art. 8. Conseil consultatif de la valorisation des données dans un environnement de confiance

(1) Il est institué, sous l'autorité du ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions, un Conseil consultatif de la valorisation des données dans un environnement de confiance, **dénommé** ci-après ~~**désigné par le terme**~~ « Conseil consultatif ».

(2) Le Conseil consultatif a pour mission :

1° de fonctionner comme organe consultatif de l'Autorité des données ;

2° de soumettre un avis motivé dans les cas où ce dernier est sollicité conformément aux dispositions de la présente loi ;

3° de se prononcer sur toute question en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données qui lui est soumise par le ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions ;

4° de promouvoir l'accès et la réutilisation des données visés au titre VI.

(3) Le Conseil consultatif est composé de représentants issus des ministères et administrations de l'État. Un règlement grand-ducal précise la composition et le mode de fonctionnement du Conseil consultatif.

TITRE IV – Informations et données à caractère personnel obtenues par les entités publiques auprès d'une autre entité publique (« *once only* »)

Art. 9. Obligation du « *once only* »

(1) Un administré présentant une demande ou produisant une déclaration à une entité publique ne peut être tenu de produire des informations ou des données à caractère personnel que celle-ci détient déjà ou qu'elle peut obtenir auprès d'une autre entité publique conformément à l'article 11.

(2) Les entités publiques échangent entre elles toutes les informations ou les données à caractère personnel nécessaires pour traiter une demande présentée par l'administré ou une déclaration présentée par celui-ci en application d'une disposition législative ou réglementaire.

Elles échangent entre elles les informations ou les données à caractère personnel nécessaires pour pouvoir informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

(3) L'obtention des informations et données à caractère personnel auprès d'une autre entité publique au sens du présent titre a pour finalités :

~~a)~~ **1°** d'assurer la mise à disposition d'informations et de données à caractère personnel aux entités publiques pour l'exécution de leurs obligations et de leurs missions d'intérêt public ;

~~b)~~ **2°** d'alléger la charge administrative des administrés dans le cadre de leurs demandes et déclarations ;

~~c)~~ **3°** d'éviter aux entités publiques de devoir organiser elles-mêmes la collecte d'informations et de données à caractère personnel auprès des administrés.

Art. 10. Certification de l'exactitude des informations et données à caractère personnel

(1) Lorsque les informations ou données à caractère personnel nécessaires pour traiter la demande présentée par l'administré ou la déclaration présentée par celui-ci doivent être obtenues auprès d'une

autre entité publique, dans les conditions prévues aux articles 11 et 12, l'administré ou son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial certifie l'exactitude des informations et des données à caractère personnel ainsi obtenues.

(2) Dans les cas où les informations et les données à caractère personnel s'avèrent inexactes, l'administré est tenu de demander leur rectification auprès de l'entité publique d'où elles proviennent et de communiquer les informations et les données à caractère personnel rectifiées à l'entité publique en charge du traitement de la demande ou de la déclaration présentée par l'administré.

Art. 11. Conditions applicables au « *once only* »

(1) L'entité publique ne sollicite pas l'échange d'informations et de données à caractère personnel auprès d'une autre entité publique s'il est manifeste qu'elle n'est pas compétente pour traiter la demande ou la déclaration présentée par l'administré ou pour l'informer sur ses droits au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir lui attribuer éventuellement lesdits prestations ou avantages.

(2) L'entité publique chargée de traiter la demande ou la déclaration fait connaître à l'administré les informations ou les données à caractère personnel nécessaires au traitement de la demande ou de la déclaration qu'elle se procure auprès d'autres entités publiques. L'information contient, pour chaque catégorie d'informations et de données à caractère personnel, les coordonnées des entités publiques d'où proviennent les informations et les données à caractère personnel.

L'obligation prévue à l'alinéa ~~**qui précède**~~ **1er** s'applique également dans les cas où l'entité publique se procure des informations ou des données à caractère personnel auprès d'autres entités publiques pour informer les administrés sur leurs droits au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

(3) Les informations et les données à caractère personnel collectées et échangées en application du présent titre ne peuvent être utilisées ultérieurement à des fins de détection systématique d'une fraude. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à procéder auxdites détections et ce pour les détections sur lesquelles porte cette habilitation.

Pour les cas visés à l'article 9, paragraphe 2, alinéa 2, au plus tard au moment de la première communication individuelle avec l'administré, celui-ci est avisé de son droit de s'opposer à la poursuite du traitement des données à caractère personnel. En cas d'opposition exprimée par l'administré de poursuivre le traitement, les informations et les données à caractère personnel obtenues à la suite de cet échange sont détruites sans délai.

(4) En cas d'impossibilité dûment motivée pour les entités publiques d'échanger les informations ou les données à caractère personnel nécessaires pour traiter la demande ou la déclaration dans les conditions prévues au présent titre :

~~**a)**~~ **1°** les entités publiques ne sont pas tenues de procéder à l'échange d'informations et de données à caractère personnel visé à l'article 9 ; ~~**et**~~

~~**b)**~~ **2°** l'administré les communique à l'entité publique chargée du traitement de la demande ou de la déclaration.

Dans les cas visés à l'alinéa ~~**qui précède**~~ **1er**, l'entité publique chargée du traitement de la demande ou de la déclaration et l'entité publique détentrice des informations et données à caractère personnel remédient dans les meilleurs délais à l'impossibilité d'échanger les informations et les données à caractère personnel en question.

(5) Les entités publiques destinataires des informations et des données à caractère personnel ne peuvent se voir opposer le secret professionnel dès lors qu'elles sont, dans le cadre de leurs missions légales, habilitées à avoir connaissance des informations ou des données à caractère personnel ainsi échangées.

(6) Un règlement grand-ducal détermine les informations ou données à caractère personnel, qui en raison de leur nature, ne peuvent faire l'objet de ces échanges entre entités publiques.

Art. 12. Recensement des informations et des données à caractère personnel disponibles auprès d'une autre entité publique

(1) Les entités publiques sont tenues d'identifier, dans les meilleurs délais, les informations et données à caractère personnel qu'elles peuvent obtenir auprès d'une autre entité publique :

~~a)~~ **1°** dans le cadre du traitement effectué dans l'exercice de leurs missions des demandes et déclarations présentées par un administré ;

~~b)~~ **2°** pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

(2) Les entités publiques notifient, sans délai, les échanges d'informations et de données à caractère personnel identifiées conformément au paragraphe 1er aux entités publiques auprès desquelles les informations et données à caractère personnel pourraient être obtenues.

Dans un délai d'un mois à partir de la notification visée à l'alinéa ~~**qui précède**~~ **1er**, les entités publiques notifiées :

~~a)~~ **1°** certifient la disponibilité des informations et des données à caractère personnel à l'entité publique demanderesse et confirment que l'échange d'informations et de données à caractère personnel n'est pas impossible ; ou

~~b)~~ **2°** informent l'entité publique demanderesse du fait qu'elles ne détiennent pas les informations et les données à caractère personnel sollicitées ou que l'échange d'informations et de données à caractère personnel est impossible.

Une copie de l'information visée ~~**aux points a) et b) du présent paragraphe**~~ **à l'alinéa 2, points 1° et 2°,** est transmise au ministre ayant la digitalisation dans ses attributions.

(3) Dans les cas visés au ~~**point a) du paragraphe qui précède**~~ **au paragraphe 2, alinéa 2, point 2°**, les entités publiques concluent dans les meilleurs délais, et au plus tard après trois mois, le protocole visé à l'article 13.

Art. 13. Protocole « *once only* »

(1) Chaque type d'échange d'informations et de données à caractère personnel visé à l'article 9 est formalisé dans un protocole signé entre les entités publiques concernées préalablement à l'échange des informations et des données à caractère personnel.

Le protocole contient, au moins, les éléments suivants :

1° les coordonnées des entités publiques d'où proviennent les informations et les données à caractère personnel et des entités publiques destinataires des informations et les données à caractère personnel ;

2° une description détaillée du contexte du traitement des informations et des données à caractère personnel ainsi que les motifs pour lesquels les informations et les données à caractère personnel sont nécessaires pour le respect des obligations prévues à l'article 9 ;

3° une description détaillée des catégories d'informations et de données à caractère personnel visées par l'échange à l'entité publique destinataire ;

4° une description détaillée des catégories de personnes concernées ;

5° une description détaillée des finalités du traitement ;

6° le cas échéant, l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers et les pays tiers à destination desquels des transferts de données à caractère personnel sont envisagés ainsi que l'existence ou l'absence de garanties appropriées conformément au chapitre V du règlement (UE) 2016/679 ;

7° les motifs pour lesquels les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies.

(2) Tout changement des éléments liés à l'obtention des informations et des données à caractère personnel auprès d'une entité publique doit être formalisé par avenant du protocole visé au paragraphe ~~**qui précède**~~ **1er**.

(3) Le protocole ainsi que tout avenant sont transmis sans délai à l'Autorité des données qui les publie par voie électronique. L'Autorité des données n'est pas responsable du contenu du protocole.

Les entités publiques informent sans délai l'Autorité des données lorsqu'un protocole n'est plus applicable. L'Autorité des données maintient la publication des protocoles pendant une durée de deux ans à partir de la réception de l'information visée au présent alinéa. Pendant cette période, elle indique que le protocole n'est plus applicable.

Art. 14. Identification des sources authentiques d'informations et de données à caractère personnel

(1) L'Autorité des données tient un registre de tous les protocoles qui lui sont transmis pour publication conformément à l'article 13, paragraphe 3.

(2) En vue d'identifier des sources authentiques d'informations et de données à caractère personnel disponibles au sein des entités publiques, le ministre ayant la digitalisation dans ses attributions dispose d'un accès direct au registre des protocoles visés au ~~**paragraphe qui précède**~~ **1er**.

TITRE V – Traitement ultérieur de données à caractère personnel par les entités publiques

Section I – Dispositions générales

Art. 15. Finalités du traitement ultérieur autorisées et licéité du traitement

(1) Le traitement ultérieur de données à caractère personnel par des entités publiques est autorisé si :

1° les conditions énoncées au présent titre sont remplies ;

2° que le traitement des données à caractère personnel est effectué exclusivement pour une ou plusieurs des finalités suivantes :

a) l'analyse statistique ;

b) les activités d'éducation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;

c) la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;

d) l'évaluation et la planification des politiques envisagées ou planifiées par le Gouvernement et approuvées par décision du Gouvernement en conseil, ou en ce qui concerne les communes, envisagées ou planifiées par le Conseil communal ;

e) lorsque la mise en œuvre d'un accord international requiert la communication d'informations ou lorsque le traitement ultérieur des données à caractère personnel permet de répondre aux demandes d'informations officielles provenant de gouvernements étrangers ou d'organisations internationales approuvées par décision du Gouvernement en conseil ;

f) les activités de développement, d'évaluation, de démonstration, de sécurité et d'innovation de dispositifs ou de services ;

g) la formation, le test et l'évaluation d'algorithmes, y compris dans les dispositifs, les systèmes d'intelligence artificielle et les applications numériques.

(2) Le traitement ultérieur des données à caractère personnel, y compris leur partage et leur mise à disposition, par les entités publiques conformément au présent titre, est licite au sens de l'article 6, paragraphe 1er, lettre e), et, si applicable, de l'article 9, paragraphe 2, lettre g) ou j) du règlement (UE) 2016/679.

Art. 16. Conditions d'anonymisation et de pseudonymisation des données à caractère personnel

(1) Les données à caractère personnel détenues par des entités publiques doivent être anonymisées préalablement à leur traitement ultérieur aux fins énoncées à l'article 15, paragraphe 1er, point 2°.

(2) Lorsque le traitement de données anonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel doivent être pseudonymisées préalablement à leur traitement ultérieur aux fins énoncées à l'article 15, paragraphe 1er, point 2°.

(3) Lorsque le traitement ultérieur de données à caractère personnel pseudonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel peuvent être traitées ultérieurement

aux fins énoncées à l'article 15, paragraphe 1er, point 2°, de manière non-pseudonymisées dans les limites du strict nécessaire.

(4) Les entités publiques qui détiennent les données à caractère personnel sont tenus d'identifier les informations protégées pour des motifs de protection des données à caractère personnel.

Elles renseignent les motifs pour lesquels les données doivent être protégées dans le plan de confidentialité prévu à l'article 35 et indiquent sur quelles parties des informations porte cette protection.

(5) Les entités publiques effectuant le traitement ultérieur de données à caractère personnel sont tenues d'une obligation de confidentialité interdisant la divulgation de toute information compromettant les droits et intérêts de la personne concernée qu'elles peuvent avoir acquise malgré les garanties mises en place conformément aux dispositions de la présente loi.

Sans préjudice du paragraphe 3, il est interdit aux entités publiques effectuant le traitement ultérieur de données à caractère personnel de rétablir l'identité de toute personne concernée à laquelle se rapportent les données à caractère personnel. Les entités publiques prennent des mesures techniques et opérationnelles pour empêcher toute réidentification.

Section II – Traitement ultérieur de données à caractère personnel par la même entité publique

Art. 17. Conditions spécifiques applicables au traitement ultérieur de données à caractère personnel par la même entité publique

(1) Une entité publique est autorisée à traiter ultérieurement les données à caractère personnel qu'elle détient pour les finalités énoncées à l'article 15, paragraphe 1er, point 2°, sous réserve du respect des dispositions de l'article 16.

(2) Lorsque le traitement ultérieur porte sur des données à caractère personnel visées aux articles 9, paragraphe 1er, et 10 du règlement (UE) 2016/679, les données à caractère personnel ne peuvent pas être traitées ultérieurement de manière non-anonymisées ou non-pseudonymisées.

Section III – Traitement ultérieur de données à caractère personnel par une autre entité publique ou par plusieurs entités publiques

Art. 18. Conditions spécifiques applicables au traitement ultérieur de données à caractère personnel par une autre entité publique ou par plusieurs entités publiques

(1) Une entité publique est autorisée à traiter ultérieurement les données à caractère personnel détenues par une autre entité publique pour les finalités énoncées à l'article 15, paragraphe 1er, point 2°, aux conditions suivantes :

1° l'entité publique qui détient les données à caractère personnel :

a) a marqué son accord de principe au traitement ultérieur, y compris le partage et la mise à disposition en inscrivant les données à caractère personnel disponibles sur la liste des ressources consultables tenues par le point d'information unique, conformément au paragraphe 3 ; ou

b) a marqué son accord spécifique au traitement ultérieur, y compris le partage et la mise à disposition, en contresignant la demande visée à l'article 27 ;

2° le traitement ultérieur de données à caractère personnel ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard des finalités poursuivies ;

3° les données à caractère personnel sont anonymisées préalablement au traitement ultérieur des données à caractère personnel, ou lorsque le traitement de données anonymisées ne permet pas d'atteindre la finalité poursuivie, si :

a) l'Autorité des données autorise le traitement ultérieur de données à caractère personnel conformément à l'article 31 ;

b) les données à caractère personnel sont pseudonymisées préalablement à leur traitement ultérieur ;

c) le traitement ultérieur de données à caractère personnel est effectué dans l'environnement de traitement sécurisé prévu à l'article 36.

(2) L'entité publique sollicitant le traitement ultérieur de données à caractère personnel détenues par une autre entité publique qui se voit opposer un refus de partage par l'entité publique détenant les données à caractère personnel sollicitées peut saisir pour avis le Conseil consultatif. Le Conseil consultatif émet un avis quant à la demande de partage dans un délai de trois semaines. L'avis du Conseil consultatif est communiqué à l'entité publique qui sollicite le partage ainsi qu'à l'entité publique détenant les données à caractère personnel, qui est appelée à considérer à nouveau la demande de partage.

L'entité publique détenant les données à caractère personnel sollicitées acte sa décision finale par écrit dans un délai de trois semaines. Elle transmet une copie de sa décision finale sans délai à l'entité publique qui sollicite le partage et au Conseil consultatif. L'absence de décision finale de l'entité publique détenant les données à caractère personnel sollicitées dans le délai imparti vaut refus.

En cas d'accord, l'entité publique détentrice des données à caractère personnel contresigne la demande visée à l'article 27.

(3) Le point d'information unique met à disposition par voie électronique une liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles en vue de leur traitement ultérieur conformément au présent titre, avec des informations pertinentes décrivant les données à caractère personnel disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur traitement ultérieur.

TITRE VI – Accès et réutilisation des données détenues par des organismes du secteur public par des réutilisateurs de données

Section I – Dispositions générales

Art. 19. Catégories de données protégées disponibles à l'accès et à la réutilisation

(1) Le présent titre s'applique à l'accès et à la réutilisation, par un réutilisateur de données, des données détenues par des organismes du secteur public, conformément au règlement (UE) 2022/868, qui sont protégées pour des motifs :

1° de confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise ;

2° de secret statistique ;

3° de protection des droits de propriété intellectuelle de tiers ; ou

4° de protection des données à caractère personnel, dans la mesure où de telles données ne relèvent pas du champ d'application de la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public.

(2) Le présent titre ne s'applique pas :

1° aux données énoncées à l'article 3, paragraphe 2, du règlement (UE) 2022/868 ;

2° aux cas visés par les autres titres de la présente loi.

Art. 20. Finalités d'accès et réutilisation des données autorisées

L'accès et la réutilisation des données par des réutilisateurs de données sont autorisés si :

1° les conditions énoncées à la section II ~~**du présent titre**~~ sont remplies ; ~~**et**~~

2° l'accès et la réutilisation des données est effectué exclusivement pour une ou plusieurs des finalités suivantes :

a) l'analyse statistique ;

b) les activités d'éducation, de formation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;

c) la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;

d) le développement, l'évaluation, la démonstration, la sécurité et l'innovation de technologies ;

e) le développement, l'évaluation, la démonstration, la sécurité et l'innovation de produits ;

f) l'évaluation des politiques publiques luxembourgeoises ou européennes.

Art. 21. Conditions d'anonymisation, de pseudonymisation et de méthodes de contrôle de divulgation des données

(1) Les données à caractère personnel détenues par des organismes du secteur public doivent être anonymisées préalablement à l'accès et à la réutilisation par le réutilisateur de données.

(2) Lorsque l'accès et la réutilisation de données à caractère personnel anonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel doivent être pseudonymisées préalablement à l'accès et à la réutilisation par le réutilisateur de données.

(3) Les accès et réutilisations effectués conformément au présent titre, par des réutilisateurs de données, de données à caractère personnel détenues par les organismes du secteur public, sous une forme non anonymisée ou non pseudonymisée, sont interdits.

(4) Les données détenues par des organismes du secteur public doivent être modifiées, agrégées, supprimées ou traitées selon toute autre méthode de contrôle de la divulgation préalablement à l'accès et à la réutilisation par le réutilisateur de données, pour éviter toute atteinte disproportionnée aux droits de propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique.

(5) Les organismes du secteur public qui détiennent les données à caractère personnel et les données à caractère non personnel sont tenus d'identifier les données protégées pour les motifs visés à l'article 19, paragraphe 1er.

Ils renseignent les motifs pour lesquels les données doivent être protégées dans le plan de confidentialité prévu à l'article 35 et indiquent sur quelles parties des informations porte cette protection.

(6) Les réutilisateurs de données sont tenus d'une obligation de confidentialité interdisant la divulgation de toute information compromettant les droits et intérêts protégés par la présente loi qu'ils peuvent avoir acquis malgré les garanties mises en place conformément aux dispositions de la présente loi.

Il est interdit aux réutilisateurs de données de rétablir l'identité de toute personne concernée à laquelle se rapportent les données. Les réutilisateurs de données prennent les mesures techniques et opérationnelles nécessaires pour empêcher toute réidentification.

Section II – Conditions applicables à la réutilisation de données à caractère personnel

Art. 22. L'accès et la réutilisation de données à caractère personnel par des réutilisateurs de données

(1) Un réutilisateur de données peut accéder et réutiliser les données à caractère personnel détenues par un organisme du secteur public pour les finalités énoncées à l'article 20, paragraphe 1er, point 2°, aux conditions cumulatives suivantes :

1° l'Autorité des données autorise l'accès et la réutilisation conformément à l'article 31 ;

2° l'organisme du secteur public qui détient les données :

a) a marqué son accord de principe à la mise à disposition des données à caractère personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en inscrivant les données disponibles sur la liste des ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2, du règlement (UE) 2022/868 ; ou

b) a marqué son accord spécifique à la mise à disposition des données à caractère personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en contresignant la demande visée à l'article 28 ;

3° l'accès et la réutilisation ne portent pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ;

4° les données à caractère personnel sont anonymisées ou pseudonymisées préalablement à leur accès et à leur réutilisation ;

5° l'accès et la réutilisation des données à caractère personnel se font dans l'environnement de traitement sécurisé visé à l'article 36.

(2) Le traitement de données à caractère personnel, y compris leur partage et leur mise à disposition, par les organismes du secteur public conformément au présent titre, est licite au sens de l'article 6, paragraphe 1er, lettre e) et, si applicable, de l'article 9, paragraphe 2, lettre g) ou j) du règlement (UE) 2016/679.

(3) Le réutilisateur de données qui se voit opposer un refus d'accès de réutilisation des données par l'organisme du secteur public détenant les données sollicitées peut saisir le Conseil consultatif, qui émet un avis quant à la demande d'accès et de réutilisation dans un délai de trois semaines. L'avis du Conseil consultatif est communiqué au réutilisateur de données et à l'organisme du secteur public détenant les données, qui est appelé à considérer à nouveau la demande d'accès et de réutilisation.

L'organisme du secteur public détenant les données sollicitées acte sa décision finale par écrit dans un délai de trois semaines. Il transmet une copie de sa décision finale sans délai au réutilisateur de données et au Conseil consultatif. L'absence de décision finale de l'organisme du secteur public détenant les données sollicitées dans les délais impartis vaut refus.

En cas d'accord, l'organisme du secteur public détenant les données contresigne la demande visée à l'article 28.

Section III – Conditions applicables à la réutilisation de données à caractère non personnel

Art. 23. L'accès et la réutilisation de données à caractère non personnel détenues par les organismes du secteur public

(1) Un réutilisateur de données peut accéder et réutiliser les données à caractère non personnel détenues par un autre organisme du secteur public et protégées pour les motifs visés à l'article 19, paragraphe 1er, points 1° à 3°, aux conditions cumulatives suivantes :

1° l'Autorité des données autorise l'accès et la réutilisation conformément à l'article 31 ;

2° l'organisme du secteur public qui détient les données :

a) a marqué son accord de principe à la mise à disposition des données à caractère non personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en inscrivant les données disponibles sur la liste des ressources consultables tenue par le point d'information unique conformément à l'article 8, paragraphe 2, du règlement (UE) 2022/868 ; ou

b) a marqué son accord spécifique à la mise à disposition des données à caractère non personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en contresignant la demande visée à l'article 28 ;

3° l'accès et la réutilisation ne portent pas une atteinte disproportionnée aux droits protégés pour les motifs visés à l'article 19, paragraphe 1er, points 1° à 3° ;

4° les données à caractère non personnel sont modifiées, agrégées, supprimées ou traitées selon toute autre méthode de contrôle de la divulgation préalablement à leurs accès et à leur réutilisation ;

5° l'accès et la réutilisation des données à caractère non personnel se font dans l'environnement de traitement sécurisé visé à l'article 36.

(2) Le réutilisateur de données sollicitant l'accès et la réutilisation de données détenues par un organisme du secteur public qui se voit opposer un refus d'accès de réutilisation des données par les organismes du secteur public détenant les données sollicitées peut saisir le Conseil consultatif, qui émet un avis quant à la demande d'accès et de réutilisation dans un délai de trois semaines. L'avis du Conseil consultatif est communiqué au réutilisateur de données et à l'organisme du secteur public détenant les données, qui est appelé à considérer à nouveau la demande d'accès et de réutilisation.

L'organisme du secteur public détenant les données sollicitées acte sa décision finale par écrit dans un délai de trois semaines. Il transmet une copie de sa décision finale sans délai au réutilisateur de données et au Conseil consultatif. L'absence de décision finale de l'organisme du secteur public détenant les données sollicitées dans les délais impartis vaut refus.

En cas d'accord, l'organisme du secteur public détenant les données contresigne la demande visée à l'article 28.

Section IV – Conditions applicables à la réutilisation d'ensembles contenant des données à caractère personnel et des données à caractère non personnel

Art. 24. Conditions applicables à la réutilisation d'ensembles mixtes de données détenus par les organismes du secteur public

Lorsque l'accès et la réutilisation portent sur un ensemble de données détenu par un organisme du secteur public qui contient des données à caractère personnel et des données à caractère non personnel, l'accès et la réutilisation sont soumis aux conditions énoncées aux articles 19 à 23.

TITRE VII – Modalités applicables au traitement ultérieur des données à caractère personnel par les entités publiques et à l'accès et à la réutilisation de données par des réutilisateurs de données

Section I – Dispositions générales

Art. 25. Champ d'application

Les dispositions du présent titre s'appliquent aux traitements ultérieurs de données à caractère personnel visés au titre V et aux accès et réutilisation de données prévus au titre VI, qui sont soumis à autorisation de l'Autorité des données.

Section II – Demande de traitement ultérieur ou d'accès et de réutilisation des données

Art. 26. Forme de la demande de traitement ultérieur ou d'accès et de réutilisation des données

(1) Les demandes de traitement ultérieur de données à caractère personnel visées au titre V ainsi que les demandes d'accès et de réutilisation visées au titre VI à présenter à l'Autorité des données doivent être formulées de façon précise et revêtir une forme écrite.

(2) Toute modification substantielle de la demande intervenant au cours de l'instruction de la demande par l'Autorité des données qui affecte les informations et pièces visées aux articles 27 et 28 nécessite le dépôt d'une nouvelle demande conformément à l'article 29.

Art. 27. Contenu de la demande de traitement ultérieur de données à caractère personnel

(1) Dans les cas visés au titre V, la demande à présenter par les entités publiques effectuant le traitement ultérieur des données à caractère personnel doit contenir les informations suivantes :

1° les coordonnées des entités publiques effectuant le traitement ultérieur des données à caractère personnel ;

2° les coordonnées des entités publiques détentrices des données à caractère personnel ;

3° une description détaillée du contexte du traitement de données à caractère personnel envisagé ;

4° une description détaillée des catégories de données à caractère personnel et des catégories de personnes concernées ;

5° la base de licéité du traitement ainsi qu'une description détaillée des finalités du traitement ;

6° une description détaillée des mesures appropriées qui permettent d'apprécier le respect des exigences en matière d'anonymisation et de pseudonymisation des données à caractère personnel, en particulier la justification du respect des conditions visées à l'article 16 ;

7° la durée du traitement de données à caractère personnel envisagée dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

8° les destinataires de données à caractère personnel et, le cas échéant, l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers et les pays tiers à destination desquels des transferts de données sont envisagés ainsi que l'existence ou l'absence de garanties appropriées conformément au chapitre V du règlement (UE) 2016/679 ;

9° les motifs pour lesquels le traitement ultérieur des données à caractère personnel ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ;

10° les motifs pour lesquels les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies ;

11° le cas échéant, une description détaillée des données à caractère personnel provenant de sources autres que les entités publiques effectuant le traitement ultérieur de données à caractère personnel et les entités publiques détenant les données à caractère personnel, dont l'introduction dans l'environnement de traitement sécurisé est sollicitée ;

12° les obligations respectives des responsables du traitement aux fins d'assurer le respect des exigences du règlement (UE) 2016/679, notamment en ce qui concerne l'exercice des droits de la personne concernée ;

13° la signature de la demande par toutes les entités publiques visées au point 1° ~~**du présent paragraphe**~~ ;

14° pour les cas visés à l'article 18, paragraphe 1er, point 1°, lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 18, paragraphe 3 ;

15° pour les cas visés à l'article 18, paragraphe 1, point 1°, lettre b), la signature de la demande par toutes les entités publiques visées au point 2° ~~**du présent paragraphe**~~.

(2) Les entités publiques effectuant le traitement ultérieur de données à caractère personnel, en leur qualité de responsables du traitement, joignent les documents suivants à leur demande :

1° si applicable, l'analyse d'impact relative à la protection des données à caractère personnel visée par l'article 35 du règlement (UE) 2016/679 ;

2° l'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679 ;

3° le plan de confidentialité signé par toutes les parties visées à l'article 35, paragraphe 2 ;

4° l'attestation de faisabilité visée à l'article 35, paragraphe 3, émise par le Centre ;

5° si applicable, une copie de l'avis du Conseil consultatif visé à l'article 18, paragraphe 2.

(3) Les entités publiques effectuant le traitement ultérieur de données à caractère personnel :

~~**a)**~~ **1°** certifient l'exactitude des informations contenues dans la demande et les pièces jointes visées au présent article ;

~~**b)**~~ **2°** certifient que le plan de confidentialité correspond aux informations contenues dans la demande présentée à l'Autorité des données ;

~~**c)**~~ **3°** s'engagent formellement à respecter les termes de l'autorisation de l'Autorité des données et du plan de confidentialité.

Art. 28. Contenu de la demande d'accès et de réutilisation de données

(1) Dans les cas visés au titre VI, la demande à présenter par les réutilisateurs des données doit contenir les informations suivantes :

1° les coordonnées des réutilisateurs des données ;

2° les coordonnées des organismes du secteur public détenant les données ;

3° une description détaillée du contexte de l'accès et de la réutilisation des données ;

4° une description détaillée des données et des catégories de personnes visées par la demande ;

5° une description détaillée des mesures appropriées qui permettent d'apprécier le respect des exigences en matière d'anonymisation, de pseudonymisation et d'agrégation des données visées à l'article 21, en particulier la justification du respect des conditions visées à l'article 21 ;

6° les motifs pour lesquels les données sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies ;

7° les motifs pour lesquels l'accès et la réutilisation des données ne portent pas une atteinte disproportionnée aux droits protégés pour les motifs visés à l'article 19, paragraphe 1er ;

8° les destinataires de données ;

9° le cas échéant, une description détaillée des données provenant des réutilisateurs de données et/ou de détenteurs de données autres que les organismes du secteur public, dont l'introduction dans l'environnement de traitement sécurisé est sollicitée par le réutilisateur de données ;

10° la durée d'accès et de réutilisation des données dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

11° le cas échéant, l'intention d'effectuer un transfert de données vers un pays tiers et les pays tiers à destination desquels des transferts de données sont envisagés ;

12° la signature de la demande par tous les réutilisateurs des données visés au point 1° ~~**du présent paragraphe**~~ ;

13° pour les cas visés à l'article 22, paragraphe 2, point 2°, lettre a)**,** et à l'article 23, paragraphe ~~**(**~~2~~**)** point 2°, lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2**,** du règlement (UE) 2022/868 ;

14° pour les cas visés à l'article 22, paragraphe 2, point 2°, lettre b)**,** et à l'article 23, paragraphe 2, point 2°, lettre b), la signature de la demande par tous les organismes du secteur public visés au point 2° ~~**du présent paragraphe**~~.

(2) Lorsque la demande porte sur des données à caractère personnel, elle contient également les informations suivantes :

1° la base de licéité du traitement de données à caractère personnel ainsi qu'une description détaillée des finalités du traitement de données à caractère personnel ;

2° les motifs pour lesquels l'accès et la réutilisation des données ne portent pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ;

3° les obligations respectives des responsables du traitement aux fins d'assurer le respect des exigences du règlement (UE) 2016/679, notamment en ce qui concerne l'exercice des droits de la personne concernée ;

4° le cas échéant, l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence de garanties appropriées conformément au chapitre V du règlement (UE) 2016/679.

(3) La demande doit être accompagnée du plan de confidentialité signé par toutes les parties visées à l'article 35, paragraphe 2**,** et de l'attestation de faisabilité visée à l'article 35, paragraphe 3, émise par le Centre.

(4) Les réutilisateurs de données effectuant l'accès et la réutilisation des données à caractère personnel, en leur qualité de responsables du traitement, joignent les documents suivants à leur demande :

1° si applicable, l'analyse d'impact relative à la protection des données visée par l'article 35 du règlement (UE) 2016/679 ;

2° l'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679 ;

3° si applicable, une copie de l'avis du Conseil consultatif visé aux articles 22, paragraphe 3, et 23, paragraphe 2.

(5) Les réutilisateurs de données :

~~**a)**~~ **1°** certifient l'exactitude des informations contenues dans la demande et les pièces jointes visées au présent article ;

~~**b)**~~ **2°** certifient que le plan de confidentialité correspond aux informations contenues dans la demande présentée à l'Autorité des données ;

~~**c)**~~ **3°** s'engagent formellement à respecter les termes de l'autorisation de l'Autorité des données et du plan de confidentialité.

Section III – Instruction de la demande par l'Autorité des données

Art. 29. Dépôt et procédure d'instruction de la demande

(1) Le dépôt des demandes visées à la section II ~~**du présent titre**~~, **dénommé** ci-après ~~**désignées**~~ la « demande », se fait auprès de l'Autorité des données.

(2) L'Autorité des données statue dans un délai de deux mois à compter du dépôt de la demande.

En cas de demande exceptionnellement détaillée et complexe, le délai de deux mois peut être prolongé de trente jours au maximum. L'Autorité des données informe le demandeur dès que possible de la nécessité du délai supplémentaire pour instruire la demande, ainsi que des raisons qui justifient ce délai.

(3) Pour les cas visés à l'article 31, paragraphe 5, l'Autorité des données statue dans un délai d'un mois à compter du dépôt de la demande de modification ponctuelle.

Dans les cas où le délai d'instruction de la demande par l'Autorité des données excède la durée couverte par l'autorisation initiale adoptée par cette dernière, les données disponibles dans l'environnement de traitement sécurisé sont conservées dans un système d'archivage intermédiaire à accès restreint pendant le délai d'instruction de la demande par l'Autorité des données, et ce jusqu'à adoption de la décision finale.

Le système d'archivage intermédiaire et les systèmes informatiques par lesquels le traitement ultérieur des données à caractère personnel ou l'accès et la réutilisation des données sont opérés, doivent être aménagés de sorte que leur accès est sécurisé, moyennant une authentification forte, et que les informations relatives au gestionnaire du dossier ayant initié la requête, les informations demandées, la date et l'heure puissent être retracées.

(4) La demande ne comprenant pas tous les éléments énoncés aux articles 27 ou 28 est déclarée irrecevable.

(5) L'Autorité des données peut demander des renseignements complémentaires aux demandeurs. En pareil cas, les délais visés aux paragraphes 2 et 3 sont suspendus à compter de la transmission de la demande de renseignements complémentaires, et ce jusqu'à réception par l'Autorité des données des renseignements sollicités. Faute de réponse du demandeur dans un délai d'un mois, la demande est rejetée d'office.

(6) Les échanges et démarches visés au présent article se font par voie électronique via le point d'information unique.

(7) L'Autorité des données peut transmettre la demande de traitement ultérieur de données à caractère personnel visée à l'article 27 et la demande d'accès et de réutilisation visée à l'article 28 au Conseil consultatif pour avis. Elle y joint toute autre pièce dont elle dispose qui est sollicitée par le Conseil consultatif. L'absence d'avis du Conseil consultatif dans un délai de trois semaines à compter de la transmission de la demande et de la décision de l'organisme du secteur public détenant les données, vaut avis favorable.

Art. 30. Redevances

Pour chaque demande visée à l'article 28, une redevance est fixée par l'Autorité des données pour couvrir les frais administratifs occasionnés par le traitement de la demande et par la mise à disposition des données dans l'environnement de traitement sécurisé.

Un règlement grand-ducal détermine la procédure applicable à la perception de la redevance.

Art. 31. Autorisation par l'Autorité des données

(1) Dans les cas visés au titre V, l'Autorité des données autorise le traitement ultérieur de données à caractère personnel lorsque :

a) **1°** la demande visée à l'article 27 est complète et accompagnée de toutes les pièces visées à l'article 27, paragraphe 2 ;

b) **2°** l'entité publique détentrice des données à caractère personnel a donné son accord écrit spécifique au traitement ultérieur de données à caractère personnel, y compris au partage et à la mise à disposition, en contresignant la demande visée à l'article 27 ;

~~c)~~ **3°** le traitement ultérieur de données à caractère personnel est exclusivement effectué pour une ou plusieurs finalités visées à l'article 15, paragraphe 1er, point 2 ;

~~d)~~ **4°** le traitement ultérieur de données à caractère personnel ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie.

(2) Dans les cas visés au titre VI, l'Autorité des données autorise l'accès et la réutilisation de données :

1° dans le cas où la demande vise l'accès et la réutilisation de données à caractère personnel, lorsque :

a) la demande visée à l'article 28 est complète et accompagnée de toutes les pièces visées à l'article 28, paragraphes 3 et 4 ;

b) pour les cas visés à l'article 22, paragraphe 2, point 2°:

i. lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2, du règlement (UE) 2022/868 ;

ii. lettre b), la signature de la demande par tous les organismes du secteur public ~~**visés au point 2° du présent paragraphe**~~ **concernés** ;

c) l'accès et la réutilisation de données est exclusivement effectuée pour une ou plusieurs finalités visées à l'article 20, paragraphe 1er, point 2° ;

d) l'accès et la réutilisation ne portent pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie ;

e) la réutilisation des données n'entraine pas un risque pour la défense nationale, la sécurité publique ou l'ordre public.

2° dans les cas où la demande vise l'accès et la réutilisation de données à caractère non personnel, lorsque :

a) la demande visée à l'article 28 est complète et est accompagnée de toutes les pièces visées à l'article 28, paragraphes 3 et 4 ;

b) pour les cas visés à l'article 23, paragraphe 2, point 2° :

i. lettre a), la preuve de l'inscription des données à caractère personnel sur la liste de ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2 du règlement (UE) 2022/868 ;

ii. lettre b), la signature de la demande par tous les organismes du secteur public ~~**visés au point 2° du présent paragraphe**~~ **concernés** ;

c) la réutilisation est exclusivement effectuée pour une ou plusieurs finalités visées à l'article 20, paragraphe 1er, point 2 ;

d) l'accès et la réutilisation ne portent pas une atteinte disproportionnée aux droits protégés pour les motifs visés à l'article 20, paragraphe 1er, points 1° à 3° ;

e) la réutilisation des données n'entraine pas un risque pour la défense nationale, la sécurité publique ou l'ordre public.

3° dans le cas où la demande vise l'accès et la réutilisation d'ensembles mixtes de données, les conditions prévues aux points 1° et 2° ~~**du présent paragraph**~~e s'appliquent.

(3) La décision d'autorisation ou de refus de l'Autorité des données est motivée. L'Autorité des données joint la demande et, si applicable, l'avis du Conseil consultatif à sa décision.

(4) Toute modification substantielle du traitement ultérieur de données à caractère personnel visé au titre V ou de l'accès et de la réutilisation des données visés au titre VI couverts par une autorisation de l'Autorité des données conformément au présent article, doit faire l'objet d'une nouvelle demande et d'une nouvelle autorisation par l'Autorité des données, conformément aux dispositions des articles 27 à 31.

(5) Si la modification sollicitée porte exclusivement sur les éléments visés à l'article 27, paragraphe 1er, point 7°, ou à l'article 28, paragraphe 1er, point 10°, autorisés par l'Autorité des données,

l'Autorité des données statue sur le bien-fondé de la demande de modification dans le cadre de la procédure accélérée visée à l'article 29, paragraphe 3.

La demande de modification visée au présent paragraphe contient :

1° dans le cas visé au titre V :

a) les coordonnées des entités publiques effectuant le traitement ultérieur des données à caractère personnel et des entités publiques détentrices des données à caractère personnel ;

b) la nouvelle durée du traitement de données à caractère personnel envisagée dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

c) l'attestation du Centre, ou du tiers de confiance mandaté par le Centre, que la modification sollicitée ne porte pas préjudice à l'efficacité des mesures consignées dans le plan de confidentialité ;

d) la signature de la demande par toutes les entités publiques visées **~~au point~~ à la lettre** a).

2° dans le cas visé au titre VI :

a) les coordonnées des organismes du secteur public détenant les données et des réutilisateurs des données ;

b) la nouvelle durée d'accès et de réutilisation des données dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

c) l'attestation du Centre, ou du tiers de confiance mandaté par le Centre, que la modification sollicitée ne porte pas préjudice à l'efficacité des mesures consignées dans le plan de confidentialité ;

d) la signature de la demande par tous les organismes du secteur public détenant les données et des réutilisateurs des données visés **~~au point~~ à la lettre** a).

(6) Les entités publiques et les organismes du secteur public mettent les données à caractère personnel et les données à caractère non personnel visées par l'autorisation de l'Autorité des données à disposition de celle-ci en vue de la mise en œuvre des mesures prévues au présent titre et de leur mise à disposition dans l'environnement de traitement sécurisé.

(7) Les entités publiques traitant ultérieurement les données à caractère personnel et les réutilisateurs de données sont tenus de traiter les données uniquement conformément aux termes de l'autorisation de l'Autorité des données.

(8) Chaque fois que les réutilisateurs de données utilisent les données conformément aux titres VI et VII, ils citent les sources de données et mentionnent que les données ont été obtenues dans le cadre de la présente loi.

Art. 32. Contrôle par l'Autorité des données

(1) L'Autorité des données a le droit de vérifier le processus, les moyens et tout résultat du traitement ultérieur de données à caractère personnel effectué par les entités publiques conformément au titre V et des accès et réutilisation des données effectués par les réutilisateurs de données conformément au titre VI, afin de préserver l'intégrité de la protection des données et le respect des conditions prévues par la présente loi, notamment en ce qui concerne les droits de propriété intellectuelle, la confidentialité commerciale et le secret statistique.

(2) L'Autorité des données a le droit d'interdire l'utilisation des résultats qui contiennent des informations portant une atteinte disproportionnée aux droits et aux intérêts de tiers. La décision d'interdire l'utilisation des résultats est transparente et compréhensible pour le réutilisateur de données.

(3) L'Autorité des données peut demander tous renseignements et informations nécessaires pour l'accomplissement des missions prévues par la présente loi au Centre, au tiers de confiance mandaté par le Centre, au LNDS, aux entités publiques, aux organismes du secteur public qui détiennent les données, aux réutilisateurs ainsi qu'à tout autre entité impliquée dans la mise en œuvre de la loi.

Section IV – Publicité par l'Autorité des données

Art. 33. Publicité des conditions d'accès et de réutilisation de données détenues par les organismes du secteur public et procédure applicable

Pour les cas visés au titre VI, l'Autorité des données rend publiques les conditions d'autorisation d'accès et de réutilisation de données détenues par les organismes du secteur public et la procédure prévue à la section III du ~~**présent titre**~~ par l'intermédiaire du point d'information unique.

Art. 34. Publicité des autorisations adoptées par l'Autorité des données

(1) L'Autorité des données tient un registre public des traitements ultérieurs de données à caractère personnel et des accès et réutilisations de données autorisées.

Le registre contient pour chaque autorisation accordée par l'Autorité des données conformément au titre VII les informations suivantes :

1° une copie de la décision adoptée par l'Autorité des données conformément à l'article 31 ;

2° si applicable, l'avis du Conseil consultatif ;

3° dans le cas de données à caractère personnel, l'information à destination des personnes concernées visée aux articles 12 à 14 du règlement (UE) 2016/679, communiquée par le demandeur.

(2) La publication par l'Autorité des données des éléments d'information à destination des personnes concernées, telle que visée au paragraphe 1er, alinéa 2, point 3°, vaut information de la personne concernée au sens des articles 12 à 14 du règlement (UE) 2016/679 pour les traitements ultérieurs de données visés au titre V et les accès et réutilisations visés au titre VI.

Section V – Mesures appropriées et mise à disposition des données dans un environnement de traitement sécurisé

Art. 35. Mesures appropriées

(1) Les mesures d'anonymisation et/ou de pseudonymisation des données à caractère personnel et/ou de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données requises par les dispositions de la présente loi et par les dispositions du règlement (UE) 2022/868 doivent être mises en œuvre préalablement au traitement ultérieur de données à caractère personnel et à l'accès et la réutilisation de données visés aux titres V et VI.

Ces mesures doivent être effectives et efficaces pour éviter toute réidentification des personnes concernées ainsi que toute atteinte aux droits d'autrui, tels que la confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise, le secret statistique et de propriété intellectuelle, compte tenu de l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour réaliser la réidentification ou pour compromettre la confidentialité des informations.

La mise en œuvre des mesures visées au présent paragraphe doit être opérée de sorte que nul autre que l'entité publique ou l'organisme du secteur public duquel proviennent les données n'ait accès aux données dans un format non anonymisé, non pseudonymisé ou non agrégé.

(2) Pour chaque demande visée aux articles 27 et 28, il est établi une évaluation spécifique des méthodes et des modalités de mise en œuvre des mesures visées au paragraphe qui précède.

L'évaluation est initiée, dans les cas visés au titre V, par les entités publiques effectuant le traitement ultérieur de données à caractère personnel et, dans les cas visés au titre VI, par les réutilisateurs de données. Elle est consignée dans un plan de confidentialité.

Le plan de confidentialité est préparé par les parties visées à l'alinéa qui précède. Il précise les conditions et les modalités, y compris les opérations et procédures de mise en œuvre, des mesures visées au paragraphe 1er.

Le projet de plan de confidentialité est amendé jusqu'à validation finale et signature commune par le Centre, ou par le tiers de confiance mandaté par le Centre, et :

~~**a)**~~ **1°** pour les cas visés au titre V, les entités publiques effectuant le traitement ultérieur de données à caractère personnel et les entités publiques détenant les données à caractère personnel ;

~~**b)**~~ **2°** pour les cas visés au titre VI, les réutilisateurs de données et les organismes du secteur public détenant les données.

Toutes les parties visées au présent paragraphe fournissent au Centre, ou au tiers de confiance mandaté par le Centre, et, dans les cas visés à l'article 5, paragraphe 3, point d) au LNDS, toute information nécessaire pour la mise en place du plan de confidentialité, qui les traitent pour les seules finalités visées au présent article ou à des fins de preuve. Le tiers de confiance et le Centre se concertent étroitement.

En signant le plan de confidentialité, le Centre, ou le tiers de confiance mandaté par le Centre, certifie que les mesures prévues au paragraphe 1er consignées dans le plan de confidentialité sont effectives et efficaces pour éviter toute réidentification des personnes concernées ainsi que toute atteinte aux droits d'autrui, tels que la confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise, le secret statistique et de propriété intellectuelle, compte tenu de l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour réaliser la réidentification ou pour compromettre la confidentialité des informations.

(3) Sur présentation du plan de confidentialité signé par toutes les parties, le Centre atteste de la faisabilité :

a) de la mise en œuvre des mesures énoncées dans le plan de confidentialité ;

b) de la mise à disposition des données dans l'environnement de traitement sécurisé.

L'attestation du Centre est jointe à la demande visée aux articles 27 et 28.

(4) Sous réserve d'autorisation de l'Autorité des données visée à l'article 31 et d'acquittement par le demandeur de la redevance visée à l'article 30 :

~~a)~~ **1°** le Centre, ou le tiers de confiance mandaté par le Centre, s'assure de la mise en œuvre les mesures visées au présent article conformément aux stipulations du plan de confidentialité ;

~~b)~~ **2°** le Centre :

~~i.~~ **a)** combine et traite les données provenant des entités publiques et des organismes du secteur public visés au paragraphe 1er, alinéa 3, pour lesquelles le traitement ultérieur et/ou l'accès et la réutilisation a été autorisé par l'Autorité des données ;

~~ii.~~ **b)** procède à la mise à disposition des données à caractère personnel visées au titre V et des données visées au titre VI dans l'environnement de traitement sécurisé, sous réserve des exigences prévues dans le plan de confidentialité et dans l'autorisation de l'Autorité des données.

Art. 36. Environnement de traitement sécurisé

(1) Le traitement ultérieur de données à caractère personnel visé au titre V et l'accès et la réutilisation de données visés au titre VI se font dans un environnement de traitement sécurisé mis à disposition par l'Autorité des données et géré par le Centre.

L'environnement de traitement sécurisé respecte notamment les mesures de sécurité suivantes:

~~a)~~ **1°** restreindre aux personnes physiques autorisées indiquées dans l'autorisation correspondante visée à l'article 31 l'accès à l'environnement de traitement sécurisé ;

~~b)~~ **2°** réduire au minimum le risque de lecture, de copie, de modification ou de suppression non autorisées des données hébergées dans l'environnement de traitement sécurisé par des mesures techniques et organisationnelles de pointe ;

~~c)~~ **3°** restreindre à un nombre limité d'individus identifiables autorisés l'introduction de données et l'inspection, la modification ou la suppression de données hébergées dans l'environnement de traitement sécurisé ;

~~d)~~ **4°** veiller à ce que les personnes visées au point a) n'aient accès qu'aux données couvertes par leur autorisation correspondante visée à l'article 31, au moyen d'identifiants individuelles et uniques et de modes d'accès confidentiels uniquement ;

~~e)~~ **5°** tenir des registres identifiables de l'accès à l'environnement de traitement sécurisé et des activités qui y sont menées pendant la période nécessaire pour vérifier et contrôler toutes les opérations de traitement dans cet environnement. Les registres d'accès devraient être conservés pendant au moins un an ;

~~f)~~ **6°** veiller à la conformité et contrôler les mesures de sécurité énumérées au présent article afin d'atténuer les menaces potentielles pour la sécurité.

(2) L'environnement de traitement sécurisé doit être aménagé de sorte à ce qu'il ne permet pas :

~~a)~~ **1°** de reproduire les données à l'extérieur de l'environnement et ainsi de les réutiliser dans un autre contexte ou pour des finalités autres qu'autorisées ;

~~b)~~ **2°** d'introduire des solutions technologiques, y compris d'intelligence artificielle, à moins qu'elles aient expressément été inclues dans le plan de confidentialité, ou préalablement été évaluées et certifiées par le Centre, ou par le tiers de confiance mandaté par le Centre, comme ne présentant aucun risque d'atteinte aux exigences visées à l'article 35, paragraphe 1er ;

~~c)~~ **3°** d'introduire des données, à moins que cette introduction ait expressément été demandée conformément à l'article 27, paragraphe 1, point 10°**,** et à l'article 28, paragraphe 1, point 8°**,** et autorisée par l'Autorité des données conformément aux dispositions du présent titre ;

~~d)~~ **4°** d'extraire les données de l'environnement de traitement sécurisé, à moins qu'elles aient préalablement été anonymisées.

(3) Dans les cas visés au paragraphe 2, point ~~b)~~ **2°**, la certification établie par le Centre, ou par le tiers de confiance mandaté par le Centre, est jointe au plan de confidentialité. Une copie est transmise sans délai à l'Autorité des données.

Pour établir la certification, le Centre, ou le tiers de confiance mandaté par le Centre, peut exiger une évaluation préalable, le cas échéant, sous forme d'audit, établie par un organisme spécialisé, à présenter, dans les cas visés au titre V, par les entités publiques effectuant le traitement de données à caractère personnel ou dans les cas visés au titre VI par les réutilisateurs de données.

(4) Sous réserve de l'autorisation de l'Autorité des données et du respect des conditions prévues par le présent titre, le Centre peut, dans le cadre d'une demande spécifique visée aux articles 27 ou 28 :

~~a)~~ **1°** créer un environnement de traitement sécurisé commun, ensemble avec des organismes compétents désignés conformément à l'article 7 du règlement (UE) 2022/868, afin de mettre les données à disposition des entités publiques ou des réutilisateurs de données ;

~~b)~~ **2°** combiner et traiter les données visées au titre VI avec des données provenant d'environnements de traitement sécurisés d'autres États membres gérés par des organismes compétents désignés conformément à l'article 7 du règlement (UE) 2022/868 afin de les mettre à disposition des réutilisateurs de données.

Art. 37. Responsabilité du traitement

(1) Les entités publiques détenant les données à caractère personnel et les organismes du secteur public détenant les données ont la qualité de responsable du traitement pour la mise à disposition des données à caractère personnel sollicitées à l'Autorité des données conformément à l'article 31, paragraphe 6.

(2) L'Autorité des données a la qualité de responsable du traitement pour le traitement de données à caractère personnel pour l'accomplissement des missions conformément à la présente loi.

(3) Les entités publiques qui traitent ultérieurement les données à caractère personnel et les réutilisateurs de données ont la qualité de responsable du traitement pour les traitements de données à caractère personnel dans l'environnement de traitement sécurisé.

(4) Dans les cas visés aux articles 35 et 36, le Centre agit comme sous-traitant de l'Autorité des données. Le Centre peut sous-traiter ultérieurement les tâches et missions lui attribués conformément à la présente loi.

Section VI – Recours

Art. 38. Recours

Un recours contre les décisions de l'Autorité des données peut être exercé devant le Tribunal administratif qui statue comme juge du fond.

TITRE VIII – Gouvernance en matière de services d'intermédiation de données et d'altruisme des données

Section I – Services d'intermédiation de données

Art. ~~41~~ 39. Procédure

Un règlement interne de la CNPD définit la procédure en matière de notification pour les services d'intermédiation de données, conformément à l'article 11 du règlement (UE) 2022/868.

Art. ~~42~~ 40. Redevances

La CNPD peut imposer des redevances proportionnées et objectives pour la notification des services d'intermédiation, conformément à l'article 11, paragraphe 11, du règlement (UE) 2022/868. Un règlement de la CNPD détermine le montant et les modalités de paiement des redevances.

Art. ~~43~~ 41. Sanctions

(1) Dans le cadre d'une violation de l'obligation de notification incombant aux prestataires de services d'intermédiation de données en vertu de l'article 11 du règlement (UE) 2022/868 ou des conditions liées à la fourniture de services d'intermédiation de données en vertu de l'article 12 du règlement (UE) 2022/868, la CNPD peut, par voie de décision, imposer des amendes administratives à hauteur de 500 à 100~~.~~ 000 euros aux prestataires de services d'intermédiation de données.

(2) La CNPD peut, par voie de décision, infliger au prestataire de services d'intermédiation de données des astreintes jusqu'à concurrence de 250 euros par jour de retard à compter de la date qu'elle fixe dans sa décision, pour le contraindre :

1° à communiquer toute information demandée par la CNPD en vertu de l'article 14, paragraphe 2, du règlement (UE) 2022/868 ;

2° à respecter une demande de cessation prononcée en vertu de l'article 14, paragraphe 4, du règlement (UE) 2022/868.

(3) Le recouvrement des amendes ou astreintes est confié à l'Administration de l'enregistrement, des domaines et de la TVA. Il se fait comme en matière d'enregistrement.

Section ~~III~~ II – Recours

Art. ~~46~~ 42. Recours

Un recours contre les décisions de la CNPD prises en application des **~~sections I et II du présent titre~~ chapitres III et IV du Règlement 2022/686** est ouvert devant le Tribunal administratif qui statue comme juge du fond.

TITRE IX – Dispositions finales

Art. ~~47~~ 43. Intitulé de citation

La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : « loi du […] relative à la valorisation des données dans un environnement de confiance ».

Impression: CTIE – Division Imprimés et Fournitures de bureau

20250516_Avis

N° 8395[8]
N° 8395A[2]
N° 8395B[2]

CHAMBRE DES DEPUTES

PROJET DE LOI

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en oeuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

PROJET DE LOI

relative à la désignation des organismes et autorités compétents et au point d'information uniquement prévus aux articles 7, 8, 13 et 23 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)

PROJET DE LOI

relative à

1° la valorisation des données dans un environnement de confiance ;

2° la mise en oeuvre du principe « once only » ;

3° la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

4° la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil

du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AVIS DU SYNDICAT DES VILLES ET COMMUNES LUXEMBOURGEOISES

(31.3.2025)

I. REMARQUES GENERALES

Le SYVICOL a été demandé en son avis par Madame la Ministre de la Digitalisation au sujet du projet de loi sous examen en date du 12 juin 2024. Le syndicat a également été invité à une présentation des grandes lignes du projet de loi au ministère de la Digitalisation en date du 29 novembre 2024 et il souhaite profiter de l'occasion pour remercier Madame la Ministre pour ces démarches.

Le présent avis a été élaboré à l'aide de la commission consultative 1 – volet administratif du SYVICOL. Le SYVICOL tient à remercier les membres de la commission pour leurs contributions importantes.

Le projet de loi n°8395 relatif à la valorisation des données dans un environnement de confiance précise au niveau national luxembourgeois les règles pour l'accès aux données détenues par les entités du secteur public ainsi que les règles concernant la réutilisation de ces données contenues dans le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).

Tout comme le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022, le projet de loi n°8395, qui reprend les dispositions de fond du règlement européen, vise à instaurer une certaine confiance entre les citoyens et les acteurs du secteur public, qui détiennent une panoplie de données à caractère personnel et à caractère non personnel de leurs administrés.

Il complète et précise pour le Luxembourg les dispositions contenues dans le règlement (UE) 2022/868, qui est d'application directe depuis le 24 septembre 2023, concernant en particulier la désignation des organismes compétents au niveau national, la procédure à suivre pour l'octroi des autorisations d'accès et de réutilisation des données, et les conditions applicables à l'accès et à la réutilisation des données.

Les principaux objectifs du projet de loi sont la simplification administrative pour le citoyen, pour les entreprises et pour les administrations publiques ; la valorisation des données détenues par le secteur public pour promouvoir l'économie, la recherche et l'innovation fondées sur les données ; l'habilitation des administrations à proposer des démarches de manière proactive aux citoyens et la facilitation de la prise de décision éclairée basée sur les données, le tout dans un environnement de confiance entre les citoyens et les détenteurs des données du secteur public.

Les dispositions du projet de loi peuvent être divisées en quatre grands piliers, à savoir le traitement primaire de données à caractère personnel (Titre II), le principe du « once only » (Titre IV), les traitements ultérieurs de données personnelles (Titres V et VII) et la réutilisation de données personnelles (Titres VI et VII).

Tandis que le SYVICOL ne veut pas remettre en cause les grands principes du projet de loi ou l'introduction du système « once only », il souhaite néanmoins faire part de ses réflexions ci-dessous concernant surtout la mise en œuvre pratique du texte.

*

II. ELEMENTS-CLES DE L'AVIS

- Le SYVICOL se demande si une commune spécifique ou le Syndicat intercommunal de gestion informatique (SIGI) pourra être désigné « tiers de confiance » au sens de la loi en projet. Dans la négative, il préconise de prévoir cette possibilité. (art. 6)
- Il salue la désignation d'une autorité centrale et l'introduction d'un « point d'information unique » pour le traitement ultérieur et l'accès, ainsi que la réutilisation des données à caractère personnel. ». (art. 7)
- Il note que les membres du conseil consultatif de la valorisation des données dans un environnement de confiance sont uniquement des représentants issus des ministères et administrations de l'État. Il demande que le niveau communal soit représenté par au moins deux membres dans cet organe consultatif. (art. 8)
- De l'avis du syndicat, il ne ressort pas clairement de la formulation actuelle du texte que les communes ne sont pas obligées à informer les administrés qu'ils ont droit à une éventuelle prestation ou un avantage supplémentaire auprès de leur commune de résidence après avoir fait une demande auprès d'une entité étatique. Il recommande de clarifier cette disposition dans le texte du projet de loi. (art. 9)
- Le SYVICOL n'est pas convaincu qu'on puisse parler d'une simplification administrative et d'un gain de temps tels qu'avancés par les auteurs du texte, surtout en relation avec le principe du « once only » et plus spécifiquement dans le contexte de la notification d'un administré relative au droit au bénéfice éventuel d'une prestation ou d'un avantage supplémentaire. Contrairement aux administrés, cette disposition entraînera un surplus de démarches à effectuer par les communes et donc une augmentation de leur charge de travail et une hausse des coûts y afférents. (art. 9 et 11)
- D'une manière plus générale, le SYVICOL demande aux auteurs de clarifier les dispositions sur le principe « once only » afin de préciser les responsabilités et obligations exactes des communes dans la mise en œuvre de ce principe. (art. 9 à 11)
- Il propose de simplifier la tâche de recensement pour les 100 communes, pour les 30 offices sociaux et les autres établissements publics placés sous la surveillance des communes en instituant un groupe de travail composé d'experts du ministère et du niveau communal pour identifier les données à caractère personnel et les informations pour lesquelles les communes devront signer un « protocole once only ». (art.12 et 13)
- Il propose de mettre à disposition des communes des protocoles types pour les échanges qui seront identiques dans les 100 communes du pays ou même d'élaborer des protocoles uniques pour chaque type d'échange de données qui est identique dans le secteur communal. (art.12 et 13)
- De l'avis du syndicat, la complexité des procédures relatives au traitement ultérieur des données à caractère personnel et à l'accès et à la réutilisation des données à caractère personnel ne reflètent pas l'affirmation des auteurs qu'il sera « superflu de recruter un spécialiste disposant des connaissances et de l'expérience pratique auprès de chacune des plus d'une centaine d'entités étatiques, de chacune des plus d'une centaine de communes luxembourgeoises » et que les communes seront, bien au contraire, quasi obligées à engager un spécialiste dans la matière ou de travailler avec un expert externe. (art.15 à 18 et 25 à 38)
- Enfin, le SYVICOL plaide pour l'application rigoureuse du principe de connexité ancré à l'article 123, paragraphe 3 de la Constitution, puisque les nouvelles missions pour les communes contenues dans le projet de loi exigent un grand investissement en termes de finances, de temps et de ressources de la part des communes. (art.15 à 18 et 25 à 38)

*

III. REMARQUES ARTICLE PAR ARTICLE

Titre I^er^ et II – articles 1^er^, 2 et 3

Les articles 1^er^ et 2 énoncent l'objet de la loi en projet ainsi que les définitions de certains termes utilisés dans le texte de la future loi. Les dispositions du projet de loi s'appliquent sans préjudice des dispositions plus spécifiques relatives au traitement de données à caractère personnel, comme celles prévues par exemple dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Les dispositions du projet de loi s'appliquent aux entités publiques, à savoir : les ministères et leurs services, les administrations et les communes, les établissements publics, les groupements d'intérêt économique, les personnes morales d'utilité publique. Le SYVICOL a été informé lors de la réunion avec le ministère de la Digitalisation que la définition d'entité publique n'inclut pas les autres établissements publics placés sous la surveillance des communes, comme les offices sociaux par exemple. Cependant, de l'avis du SYVICOL, l'application du principe « once only » serait certainement utile dans ces entités publiques.

L'article 3 introduit une base légale générale pour le traitement de données à caractère personnel par les entités publiques, la base de licéité générale du traitement de données à caractère personnel se fondant dans le cadre de la future loi sur la condition que les données soient traitées par les entités publiques dans l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont les entités publiques sont investies : « Les entités publiques sont habilitées à traiter les données à caractère personnel nécessaires aux fins relevant de l'exécution de leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies par une disposition de droit de l'Union européenne ou de droit national applicable.»

Titre III – articles 4 à 8

Le titre III du projet de loi définit les acteurs compétents en matière de traitement de données à caractère personnel, ainsi qu'en matière d'accès et de réutilisation de données tel qu'exigé par le règlement (UE) 2022/868.

Le Commissariat du gouvernement à la protection des données auprès de l'État est désigné comme organe centralisé compétent habilité à octroyer ou à refuser les accès et les réutilisations des données, le Commissariat est donc désigné « Autorité des données » au sens du règlement européen.

Le commentaire des articles explique que « pour des raisons de cohérence et d'économie budgétaire, cette option est mise en oeuvre par la création d'une Autorité des données centralisée. En effet, il s'avère excessif de recruter un spécialiste disposant des connaissances et de l'expérience pratique afférente auprès de chacune des plus d'une centaine d'entités étatiques ainsi qu'auprès de chacune des plus d'une centaine de communes luxembourgeoises et des autres organismes de droit public relevant du champ d'application du règlement (UE) 2022/868. »

L'autorité des données sera soutenue au niveau technique et dans ses décisions par le Centre des technologies de l'information de l'État (Centre) ainsi que par le groupement d'intérêts économiques Plateforme nationale d'échange de données (LNDS) ainsi que par des « tiers de confiance » (article 6) et le Conseil consultatif de la valorisation des données dans un environnement de confiance (article 8).

Les « tiers de confiance » aideront l'autorité des données, le Centre et le LNDS à « effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données ».

Pour l'accès aux données, un « point d'information unique » est créé sous l'autorité du ministre ayant la digitalisation dans ses attributions. Le point d'information unique recevra, entre autres, les demandes d'accès et de réutilisation de données, les transmettra électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et mettra une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données à disposition du grand public.

Le SYVICOL salue la désignation d'une autorité centrale et l'introduction d'un point d'information unique pour l'accès aux données et pour la réutilisation de données. Il se demande cependant si une commune particulière ou le Syndicat intercommunal de gestion informatique (SIGI) pourra être désigné « tiers de confiance ».

Le Centre, donc le CTIE, a uniquement pour mission de « s'assurer de la mise en oeuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou de modification, d'agrégation, de suppression et de traitement des informations et données selon toute autre méthode de contrôle de la divulgation des données conformément au plan de confidentialité, préalablement à la mise à disposition des données dans l'environnement de traitement sécurisé ». D'après la lecture du texte faite par le SYVICOL, dans la pratique, il incombera donc également aux communes d'anonymiser et de pseudonymiser les données à caractère personnel avant leur introduction dans l'environnement de traitement sécurisé.

Le SIGI s'occupe de la gestion informatique pour 99 des 100 communes du pays et devra constituer un acteur incontournable pour aider les communes à mettre en œuvre les dispositions du projet de loi n°8395. Mais étant donné que la Ville de Luxembourg n'est pas membre du syndicat intercommunal, il est nécessaire, selon l'avis du SYVICOL, de prévoir la possibilité de désigner une commune spécifique ainsi que le syndicat intercommunal en tant que « tiers de confiance ».

Quant au Conseil consultatif de la valorisation des données dans un environnement de confiance, le SYVICOL note que les membres dudit conseil sont des représentants issus des ministères et administrations de l'État. Cet organe n'inclurait donc pas de représentants provenant des communes ou du SYVICOL, un fait qui est regrettable.

Puisque les 100 communes du pays sont des détenteurs d'un grand nombre de données à caractère personnel ou non personnel de leurs administrés et puisqu'elles joueront un rôle important dans l'application du principe du « once only » introduit au titre IV ainsi que dans la mise à disposition des données pour la réutilisation ultérieure, le SYVICOL est d'avis que les communes devraient avoir au moins deux représentants au sein du Conseil consultatif de la valorisation des données dans un environnement de confiance, à nommer ou bien par le SYVICOL ou par le SIGI et la Ville de Luxembourg, tel qu'il est d'ores et déjà le cas pour la Commission du registre national instaurée par la loi du 19 juin 2013 relative à l'identification des personnes physiques, pour laquelle le SYVICOL est habilité à nommer un membre titulaire et un membre suppléant.

Titre IV – articles 9 à 14

L'article 9 introduit le principe du « once only » pour les informations et données à caractère personnel obtenues par les entités publiques auprès d'une autre entité publique. Ce principe comprend la règle générale qu'un « administré présentant une demande ou produisant une déclaration à une entité publique ne peut être tenu de produire des informations ou des données à caractère personnel que celle-ci détient déjà ou qu'elle peut obtenir auprès d'une autre entité publique conformément à l'article 11. » Cette manière de procéder est obligatoire pour toutes les entités publiques.

L'article 9, paragraphe 2, alinéa 2 dispose : « Elles (les entités publiques) échangent entre elles les informations ou les données à caractère personnel nécessaires pour pouvoir informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages. »

Cette situation se présente régulièrement dans les administrations communales, par exemple, si un administré a fait une demande pour une subvention en matière d'énergie auprès de l'Etat, disons pour l'installation de panneaux photovoltaïques, et si une commune offre une subvention pour le même type d'installation fixée à un certain pourcentage du subside de l'Etat sous condition que la subvention étatique ait déjà été accordée à l'administré.

Lors de la réunion du 29 novembre 2024 entre le SYVICOL et les services compétents du ministère de la Digitalisation, il a été expliqué que cette disposition n'est pas obligatoire. De l'avis du syndicat, la formulation actuelle du paragraphe en question ne reflète cependant pas cette subtile différence. Il ne ressort pas clairement de la formulation actuelle du texte que les communes ne sont pas obligées à informer les administrés qu'ils ont droit à une éventuelle prestation supplémentaire auprès de leur commune de résidence après avoir fait une demande auprès d'une entité étatique, surtout si on lit l'article 9, paragraphe 2, alinéa 2 en conjonction avec l'article 11, paragraphe 2, alinéa 2 et l'article 12, paragraphe 1er, lettre b).

Vu ce qui précède, il sera difficile pour les communes de déterminer exactement quelles seront leurs responsabilités et obligations pour l'application du principe « once only ». Dès lors, le SYVICOL demande au gouvernement de clarifier la disposition en question afin d'éviter toute source de confusion et d'insécurité juridique.

L'article 10 place la responsabilité de vérifier l'exactitude des données échangées entre les entités publiques fermement entre les mains de l'administré, son curateur ou son administrateur légal, son administrateur ad hoc ou son mandataire spécial.

D'abord, le SYVICOL note qu'aucune disposition du projet de loi n'explique comment cette vérification sera effectuée. Est-ce que les administrés seront simplement tenus de cocher une case dans un système numérique ?

Dans ce cas, quid des administrés en situation d'illectronisme ? Même de nos jours, un nombre non négligeable de citoyens sont frappés par la fracture numérique, c'est-à-dire par les inégalités dans l'accès aux technologies de l'information et de la communication. Cette fracture peut se présenter à au moins deux niveaux : le niveau de l'accès et le niveau de l'usage.

Surtout au vu de l'affirmation des auteurs du projet de loi dans l'exposé des motifs de vouloir réduire tout particulièrement cette fracture numérique, la vérification devra donc rester possible sous forme de papier : « Afin que l'économie et la recherche fondées sur les données soient inclusives à l'égard de tous les citoyens, il faut veiller tout particulièrement à réduire la fracture numérique et à promouvoir une expertise de pointe nationale dans le secteur des technologies. L'économie des données doit être construite de manière à permettre aux entreprises de prospérer, en garantissant la neutralité de l'accès aux données ainsi que la portabilité et l'interopérabilité des données, et en évitant les effets de verrouillage. »

Ensuite, au cas où les données s'avèrent inexactes, l'administré est tenu de demander une rectification auprès de l'entité publique dont elles proviennent et communiquer la correction à l'entité publique qui traite les données. Le SYVICOL se demande comment les auteurs du texte visent à s'assurer que l'administré soit en mesure d'identifier l'entité publique originaire des données afin de pouvoir demander une rectification ? De l'avis du syndicat, il est en fait non réaliste que tous les administrés sachent quelles entités publiques détiennent quelles données à caractère personnel sur leur personne.

En plus, il se demande si cette manière de procéder n'est pas tout à fait contraire au principe du « once only », un élément clé du projet de loi, vu que l'administré est tenu de communiquer la rectification de ses données à l'entité publique dont elles proviennent et à l'entité publique en charge du traitement. Ne serait-il pas suffisant pour l'administré de communiquer la rectification à l'entité originaire, puisque les entités publiques sont de toute façon soumises à l'obligation d'échanger ces dernières entre elles ?

Puisque le texte du projet de loi reste muet sur les modalités techniques concernant l'échange d'informations pour la vérification de l'exactitude et, le cas échéant, la rectification des données personnelles de l'administré, le SYVICOL part de l'hypothèse que ces démarches seront d'une manière ou d'une autre intégrées dans l'espace individuel « My Guichet » des administrés. Dans cette hypothèse, il est concevable que l'espace personnel de l'administré puisse afficher les entités publiques détentrices des informations et données personnelles, et que l'administré puisse simplement cocher une case pour la vérification de ses données personnelles, demander la rectification de ces dernières et même donner son consentement, le cas échéant quasi généralisé, pour la transmission de ses données à une autre entité publique pour pouvoir bénéficier d'une prestation ou d'un avantage supplémentaire.

L'article 11 explique les conditions applicables au « once only », notamment que « l'entité publique chargée de traiter la demande ou la déclaration fait connaître à l'administré les informations ou données à caractère personnel nécessaires au traitement de la demande ou de la déclaration qu'elle se procure auprès d'autres entités publiques. L'information contient, pour chaque catégorie d'informations et de données à caractère personnel, les coordonnées des entités publiques d'où proviennent les informations […]. »

Dans le cas de figure où un administré aurait droit au bénéfice éventuel d'une prestation ou d'un avantage supplémentaire et se trouverait en situation d'illectronisme, une commune qui souhaiterait faire bénéficier ledit administré de prestations ou d'avantages additionnels devrait d'abord informer ce dernier par lettre recommandée (afin de s'assurer que l'administré reçoive le courriel) qu'il a droit à des aides supplémentaires, puis de quelles données la commune aurait besoin pour traiter le dossier et de quelle(s) entité(s) publique(s) les données ou informations proviendraient, lui demander s'il désire rectifier des données nécessaires et enfin demander à l'administré concerné s'il est d'accord avec le

traitement de ses données pour cette démarche administrative ou s'il veut s'opposer au traitement et par conséquent probablement renoncer à une aide supplémentaire.

Dans ce contexte, on peut se demander si on peut toujours parler d'une simplification administrative et d'un gain de temps, comme avancé par les auteurs du texte dans l'exposé des motifs ? Ceci vaut avant tout pour les administrations communales, pour lesquelles, contrairement aux administrés, ces obligations entraîneront un surplus de démarches à effectuer et donc une augmentation de leur charge administrative et une hausse des coûts y afférents au lieu d'une simplification administrative et d'une réduction des dépenses et du temps de travail.

Afin de pouvoir exécuter les procédures « once only », les entités publiques « sont tenues d'identifier, dans les meilleurs délais, les informations et données à caractère personnel qu'elles peuvent obtenir auprès d'une autre entité publique […] et de notifier, sans délai, les échanges d'informations et de données à caractère personnel identifiées conformément […] aux entités publiques auprès desquelles les informations et données à caractère personnel pourraient être obtenues. » Dans un délai d'un mois à partir de la notification visée, les entités publiques notifiées certifient la disponibilité ou non des informations et des données en question et renseignent l'entité publique demanderesse si ces dernières sont communicables dans un format adéquat. (article 12)

Si les informations et données sont disponibles et techniquement communicables, les entités publiques concluent dans les meilleurs délais, et au plus tard après trois mois, un « protocole once only » (article 13).

Chaque commune devra donc identifier toutes les données à caractère personnel et toutes les informations qu'un ministère ou une administration détient et dont elle aura besoin pour traiter les demandes et les déclarations des administrés et, le cas échéant, pour communiquer à l'administré qu'il a droit à des prestations ou à un avantage supplémentaire, et ceci dans les meilleurs délais.

D'abord, le SYVICOL se demande, vu l'ampleur de la tâche, quel délai exact les auteurs du texte ont envisagé en employant les termes « meilleurs délais » ? Il serait utile de préciser cette disposition afin d'offrir plus de prévisibilité aux administrations communales dans la mise en œuvre du projet de loi sous examen.

Ensuite, puisqu'un grand nombre de démarches sont identiques dans chaque commune du pays, le SYVICOL propose de simplifier cette tâche de recensement pour les 100 communes, et même pour les 30 offices sociaux et les autres établissements publics placés sous la surveillance des communes, en instituant un groupe de travail composé d'experts du ministère de la Digitalisation et du niveau communal pour identifier et recenser les données à caractère personnel et les informations pour lesquelles les communes devront signer un « protocole once only ».

Dans le même ordre d'idées, il se demande s'il serait possible de mettre à disposition des communes des protocoles types pour les échanges qui seront identiques dans chacune des 100 communes du pays ou même d'élaborer des protocoles uniques pour chaque type d'échange de données avec le secteur communal. A titre d'exemple, on peut citer les autorisations à bâtir pour lesquelles les administrés ont besoin d'un extrait cadastral de la parcelle sur laquelle ils planifient leurs travaux.

Pour traiter une telle demande, les communes ont donc besoin du même type de document et du même type d'échange provenant de l'Administration du cadastre et de la topographie (ACT). Ainsi, au lieu de faire signer un « protocole once only » entre l'ACT et les 100 communes individuellement, une vraie simplification administrative, de l'avis du SYVICOL, consisterait en un « protocole once only » entre l'ACT et toutes les communes pour le type d'échange de la transmission de l'extrait du plan cadastral dans le cadre d'une autorisation à bâtir.

Titre V et VII – articles 15 à 18 et 25 à 38

Le Titre V définit le cadre du traitement ultérieur de données à caractère personnel par les entités publiques. Le traitement ultérieur est uniquement possible sous les conditions et pour les finalités énoncées aux articles 15 et 16.

Une entité publique est autorisée à traiter ultérieurement les données à caractère personnel qu'elle détient, le cas échéant après anonymisation ou pseudonymisation (article 17).

Si une entité publique souhaite traiter ultérieurement des données à caractère personnel détenues par une autre entité publique, l'entité détentrice doit marquer son accord de principe pour le traitement ultérieur en inscrivant les données sur la liste des ressources consultables auprès du point d'information

unique et, dans un deuxième temps, en marquant son accord spécifique au traitement ultérieur en contresignant la demande de traitement ultérieur de données à caractère personnel par l'entité publique demanderesse. (article 18)

Le SYVICOL se demande quel organe de la commune sera responsable pour prononcer l'accord de principe et pour donner l'accord spécifique pour le traitement ultérieur des données à caractère personnel. Il propose donc de clarifier cette disposition pour les communes.

En cas de refus par l'entité publique qui détient les données, le Conseil consultatif peut être saisi par la partie demanderesse et émet un avis endéans 3 semaines. La décision finale réside cependant toujours avec l'entité détentrice des données.

Le Titre VII définit les modalités applicables au traitement ultérieur des données à caractère personnel par les entités publiques et à l'accès et à la réutilisation de données par des réutilisateurs de données qui sont soumis à autorisation de l'Autorité des données. (article 25) Toute demande doit être introduite sous forme écrite et de manière précise. (article 26)

Avant chaque traitement ultérieur de données à caractère personnel, des mesures effectives et efficaces d'anonymisation et/ou de pseudonymisation doivent être mises en place et une évaluation spécifique des méthodes et des modalités de mise en oeuvre de ces mesures doit être effectuée et enregistrée dans un plan de confidentialité par l'entité publique qui vise à effectuer le traitement ultérieur des données. Ce plan de confidentialité est uniquement validé au moment où il est signé par le Centre ou par le tiers de confiance mandaté par le Centre et par l'entité publique effectuant le traitement ultérieur de données à caractère personnel.

Dans le cas de figure d'une demande d'accès et de réutilisation des données par un réutilisateur, le plan de confidentialité doit être signé par l'entité publique détentrice des données et par le réutilisateur. Le plan de confidentialité est ensuite transmis au Centre ou à un tiers de confiance mandaté par le Centre, qui certifie alors l'effectivité et l'efficacité des mesures en apposant sa signature.

L'attestation du Centre est jointe à la demande de traitement ultérieur ou à la demande d'accès et de réutilisation selon le cas de figure qui se présente, après quoi les données sont mises à disposition dans l'environnement de traitement sécurisé par le Centre. (article 35)

En lisant les paragraphes précédents, on peut vraiment se demander si une commune ne sera pas obligée d'engager un expert en matière de réutilisation et de traitement ultérieur de données. Il est bien sûr tout à fait compréhensible que les données à caractère personnel de nos citoyens doivent être protégées de manière adéquate et que nous ne pouvons pas traiter ces données à caractère personnel, même ultérieurement, à la légère.

Les procédures décrites ci-dessus sont toutefois si complexes qu'elles ne peuvent pas être mises en œuvre facilement par les communes. L'anonymisation et la pseudonymisation, en particulier, sont des procédures hautement spécialisées qui nécessitent de l'expérience et une formation spécialisée. Les communes seront donc quasi obligées à engager un spécialiste dans la matière ou travailler avec un expert externe.

Partant, tandis que l'exposé des motifs déclare que « en effet, il s'avère excessif de recruter un spécialiste disposant des connaissances et de l'expérience pratique afférente auprès de chacune des plus d'une centaine d'entités étatiques, de chacune des plus d'une centaine de communes luxembourgeoises […] », la complexité du texte et des procédures y comprises ne reflète pas cette affirmation de l'avis du SYVICOL.

Dans ce contexte, il souhaite également renvoyer à l'article 123 de la Constitution, et plus précisément au paragraphe 3 de cet article qui dispose que « les communes ont droit aux ressources financières pour remplir les missions qui leur sont confiées par la loi. » La mise en œuvre du projet de loi n°8395 au niveau communal, notamment le recensement des données, l'application du principe « once only », la rédaction et la gestion des protocoles « once only », la rédaction et la gestion des plans de confidentialité, la gestion des demandes de traitement ultérieur et les demandes d'accès et de réutilisation, peuvent être considérées comme des nouvelles missions pour les communes. Considérant que ces missions exigent un grand investissement en termes de finances, de temps et de ressources de la part des communes, il serait tout à fait justifié que les communes reçoivent des moyens financiers supplémentaires pour exercer ces nouvelles missions.

Adopté unanimement par le comité du SYVICOL, le 31 mars 2025

Impression: CTIE – Division Imprimés et Fournitures de bureau
8395 - Dossier consolidé : 211

20250515_Avis_3

N°8395/09
Entrée le 15.05.2025
Chambre des Députés

à Madame la Ministre de la Digitalisation

Strassen, le 12 mai 2025

Avis

sur le projet de loi n° 8395

1) relatif à la valorisation des données dans un environnement de confiance ;

2) relatif à la mise en œuvre du principe « once only » ;

3) relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données);

4) relatif à la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Par sa lettre du 12 juin 2024, vous avez bien voulu demander l'avis de la Chambre de l'Agriculture au sujet du projet de loi repris sous rubrique.

I. Considérations générales

Ce projet de loi a pour objet :

- d'autoriser les entités publiques à traiter des données à caractère personnel dès lors que leur traitement est nécessaire aux fins de l'exécution de leur mission d'intérêt public ;
- de mettre en œuvre le principe de simplification administrative dit « once only » ;
- de mettre en application pour les organismes du secteur public certaines dispositions du règlement européen (UE) 2022/868 sur la gouvernance européenne des données, et
- de mettre en application certaines dispositions du règlement général sur la protection des données (règlement (UE) 2016/679).

La Chambre d'Agriculture se félicite que l'utilisation et la réutilisation des données (personnelles ou non) soit encadrée afin de garantir un environnement de confiance pour les citoyens ainsi que les entreprises.

Elle salue également la mise en œuvre du principe « once only », qui a pour objectif la simplification administrative, objectif cher au monde agricole qui croûle sous les obligations de déclaration et de paperasses administratives.

II. <u>Commentaires concernant la définition des « entités publiques » :</u>

La Chambre d'Agriculture partage l'avis des Chambre de Commerce et Chambre des Métiers concernant la définition de la notion « d'entité publique » et donc du champ d'application exact de la loi.

Le règlement sur la gouvernance européenne des données définit les notions d'« organisme de du secteur public » et d'« organisme de droit public ».

Le projet de loi sous avis ajoute la notion d'entité publique et fournit une définition qui renvoie néanmoins à une liste prévue par un règlement grand-ducal qui n'a pas été soumis pour avis à la Chambre d'Agriculture.

Il en résulte une certaine confusion et insécurité juridique, ainsi que notamment une impossibilité pour la Chambre d'Agriculture de savoir précisément si les chambres professionnelles sont à considérer comme des entités publiques au regard du projet de loi sous avis ou pas.

La Chambre d'Agriculture plaide en faveur d'une clarification de cette notion ainsi que pour la qualification des chambres professionnelles en tant qu'entités publiques.

Il est en effet incontestable qu'elles remplissent des missions d'intérêt public qui leur sont dévolues de par la loi et qu'elles ont un grand intérêt à avoir accès aux données de leurs secteurs respectifs qu'elles accompagnent et dont elles défendent les intérêts.

Pour le surplus, le projet de loi sous avis ne soulève pas de commentaires particuliers de la part de la Chambre d'Agriculture.

III. <u>Conclusion :</u>

La Chambre d'Agriculture approuve le projet de loi sous avis à condition que toutes ses remarques, formulées dans le présent avis, soient prises en compte.

Veuillez agréer, Madame la Ministre, l'expression de notre plus haute considération.

Paul MARCEUL

Directeur