Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Date de création : 30-10-2024

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	8395/00	3
18-06-2024	Commission de l'Enseignement supérieur, de la Recherche et de la Digitalisation Procès verbal (09) de la reunion du 18 juin 2024	09	80
23-10-2024	Avis de la Chambre des Fonctionnaires et Employés publics (21.10.2024)	8395/01	98
25-10-2024	Avis de la Chambre des Salariés (23.10.2024)	8395/02	104
30-10-2024	Avis de l'Ordre des Architectes et des Ingénieurs-Conseils (28.10.2024)	8395/03	116

8395/00

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

09

Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

DS/LW P.V. ESRD 09

Commission de l'Enseignement supérieur, de la Recherche et de la Digitalisation

Procès-verbal de la réunion du 18 juin 2024

Ordre du jour :

1. **Approbation du projet de procès-verbal de la réunion du 21 mai 2024**

2. 8371 **Projet de loi portant modification de la loi modifiée du 28 octobre 2016 relative à la reconnaissance des qualifications professionnelles**
   - Rapporteur : Monsieur Gérard Schockmel

   - Présentation et approbation d'un projet de rapport

3. 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)

   - Désignation d'un rapporteur
   - Présentation des grandes lignes du projet de loi

4. **Divers**

*

Présents : Mme Barbara Agostino, M. Guy Arendt, M. André Bauler, M. François Bausch, Mme Taina Bofferding, Mme Liz Braz, M. Sven Clement, M. Franz Fayot, M. Max Hengel remplaçant M. Laurent Zeimet, Mme Françoise Kemp, Mme Octavie Modert, Mme Nathalie Morgenthaler remplaçant M. Christophe Hansen, M. Gérard Schockmel, M. David Wagner, Mme Joëlle Welfring

Mme Stéphanie Obertin, Ministre de la Recherche et de l'Enseignement supérieur, Ministre de la Digitalisation

Mme Anne Glesener, du groupe politique DP

M. Patrick Houtsch, Directeur du Centre des Technologies de l'Information de l'Etat (CTIE)

Mme Christiane Huberty, M. Pierre Misteri, du Ministère de la Recherche et de l'Enseignement supérieur

M. Gaston Schmit, du Ministère de la Digitalisation

M. Maximilien Spielmann, Commissaire du Gouvernement à la protection des données auprès de l'État

M. Dan Schmit, de l'Administration parlementaire

Excusés : M. Christophe Hansen, M. Tom Weidig, M. Laurent Zeimet

*

Présidence : M. Gérard Schockmel, Président de la Commission

*

1. Approbation du projet de procès-verbal de la réunion du 21 mai 2024

Le projet de procès-verbal sous rubrique est adopté à l'unanimité.

2. 8371 Projet de loi portant modification de la loi modifiée du 28 octobre 2016 relative à la reconnaissance des qualifications professionnelles

Le rapporteur du projet de loi sous rubrique présente les grandes lignes de son projet de rapport.

Ce projet ne suscitant aucun commentaire de la part des membres de la Commission, il est ensuite procédé au vote.

- *La Commission adopte le projet de rapport à l'unanimité.*

Pour la séance plénière, la Commission propose de ne pas prévoir de débat à l'issue de la présentation du rapport. M. David Wagner (déi Lénk) se prononce en faveur du modèle de base.

3. 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)

La Commission entame les travaux parlementaires sur le projet de loi sous rubrique pour procéder à (1) la désignation d'un rapporteur, (2) la présentation des grandes lignes du projet de loi par la Ministre de la Digitalisation ainsi qu'un (3) premier échange de vues.

❖ **Désignation d'un rapporteur**

M. Gérard Schockmel (DP) est désigné comme rapporteur du projet de loi sous rubrique.

❖ **Présentation du projet de loi**

La Ministre de la Digitalisation, Mme Stéphanie Obertin, présente les grandes lignes du projet de loi qui vise une optimisation de l'utilisation des données à caractère personnel dont dispose l'État en vue d'améliorer le service public. Ceci implique la définition d'un cadre légal qui garantit la sécurité des données à caractère personnel en conformité avec la législation européenne afférente dont notamment le règlement général sur la protection des données (ci-après le « RGPD ») ainsi que le règlement sur la gouvernance des données.

Le projet de loi comporte des dispositions prévoyant les éléments suivants :

- l'autorisation pour les entités publiques de traiter des données dans le cadre de leurs missions en conformité avec les principes du RGPD. Ainsi, le projet de loi instaure une autorisation globale pour les acteurs publics de traiter des données à caractère personnel à condition que ce traitement soit effectué dans le cadre de l'accomplissement de leurs missions prévues par la loi ;

- l'introduction du principe du « *once only* ». Ce principe prévoit l'échange de données déjà à disposition d'une administration publique afin d'éviter qu'un administré doive fournir une même donnée à plusieurs reprises à une entité étatique. Ces échanges se réalisent selon des protocoles définis visant à garantir la protection des données et notamment le principe de la minimisation des données ;

- le traitement ultérieur de données à caractère personnel par des acteurs publics au-delà de la fin du traitement initial. Les finalités licites de réutilisation sont énumérées, de façon exhaustive, à l'article 15 du projet de loi. En outre, le titre correspondant du projet de loi prévoit des dispositions visant à garantir la protection des données à caractère personnel traitées ;

- la réutilisation des données à caractère personnel détenues par l'État par des acteurs privés. Cette réutilisation n'est possible qu'à des fins définies par le projet de loi et en respect d'une série de dispositions visant à garantir la protection des données.

Pour des informations complémentaires, il est renvoyé au document parlementaire n° 8395/00 ainsi qu'à la présentation annexée au présent procès-verbal.

❖ **Échange de vues**

Lors de l'échange de vues qui suit la présentation du projet de loi, les membres de la Commission abordent plusieurs sujets dont il y a lieu de retenir les éléments suivants :

À une question afférente de M. Franz Fayot (LSAP), M. le Commissaire du Gouvernement à la protection des données auprès de l'État explique que le dispositif du projet de loi s'inspire notamment de la loi française pour l'implémentation du principe du « *once only* », de la loi finlandaise pour les dispositions relatives à l'utilisation ultérieure de données par les entités

publiques et de la législation européenne existante et en cours de finalisation pour la dernière partie du projet de loi.

Mme Octavie Modert (CSV) s'interroge sur l'applicabilité du projet de loi au vu de secrets tels que le secret fiscal pouvant empêcher l'échange de données.

À ce titre, M. Franz Fayot (LSAP) renvoie aux difficultés du STATEC d'obtenir certaines données d'administrations publiques qui invoquent des secrets et aimerait savoir dans quelle mesure le projet de loi affecte cet accès aux informations.

M. Gérard Schockmel (DP) ajoute qu'il serait opportun de connaître les raisons d'un refus.

Mme la Ministre de la Digitalisation indique que le projet de loi prévoit en effet un droit d'opposition à un traitement ultérieur des données. Dans cette hypothèse, il reste cependant la possibilité de faire appel au Conseil consultatif pour trancher sur le bien-fondé du refus.

M. le Commissaire du Gouvernement à la protection des données auprès de l'État rappelle que le projet de loi rappelle le principe selon lequel un refus d'une autorité administrative doit être dûment motivé. Par ailleurs, il y a lieu de retenir que l'article 18 du projet de loi précise les conditions devant être remplies afin que des données puissent être échangées. Ainsi, le projet de loi prévoit des critères objectifs sur lesquels une décision de refus peut être fondée.

M. Franz Fayot (LSAP) relève encore que la faisabilité technique résultant de l'incompatibilité des systèmes informatiques empruntés par l'État est susceptible de constituer un frein à la mise en place du principe du « *once only* » et souhaite dès lors savoir dans quels délais le Gouvernement entend remédier à ces obstacles.

À ce titre, Mme Taina Bofferding (LSAP) cite l'exemple des communes qui peuvent utiliser des systèmes informatiques différents augmentant le défi pour la mise en place du nouveau principe.

Mme Stéphanie Obertin indique qu'il est prévu de résoudre de tels problèmes techniques dans les meilleurs délais afin de garantir une application large du principe du « *once only* ». En ce qui concerne le secteur communal, des premiers échanges ont été organisés.

Mme la Ministre de la Digitalisation confirme, suite à une question afférente de Mme Joëlle Welfring (déi gréng), que le personnel du Commissariat du Gouvernement à la protection des données sera revu à la hausse afin de pouvoir accomplir ses nouvelles missions.

M. Sven Clement (Piraten) et Mme Octavie Modert (CSV) renvoient à des procédures qui ne sont pas initiées par l'administré, mais par l'administration ou qui se reproduisent à des intervalles définis. À ce titre, les orateurs aimeraient savoir dans quelle mesure ces procédures sont visées par le projet de loi.

M. Sven Clement (Piraten) s'interroge sur le droit d'opposition à l'utilisation des données à caractère personnel.

En réponse à ces observations, Mme Stéphanie Obertin revient sur les différences entre le principe du « *once only* » visé au Titre VI du projet de loi et le traitement ultérieur de données à caractère personnel visé au Titre V. Le principe du « *once only* » vise un échange obligatoire d'informations dans le cadre de démarches administratives et ne concerne que les données strictement nécessaires pour compléter une procédure. Des démarches non initiées par un administré, mais qui requièrent certaines actions de la part de l'administré tombent également dans le champ d'application dudit principe. Le traitement ultérieur vise le traitement de données au-delà de certaines démarches administratives à des fins très précises telles que

des analyses ou une approche proactive de la part des communes. Ce traitement est strictement encadré par le projet de loi. En ce qui concerne le droit d'opposition, ce dernier n'existe que pour le traitement ultérieur des données.

Répondant à une question complémentaire afférente de Mme Liz Braz (LSAP) qui s'intéresse notamment à l'utilité du règlement grand-ducal prévu à l'article 11, paragraphe 6, du projet de loi, Mme la Ministre de la Digitalisation précise que le principe du « *once only* » ne créera pas de nouvelles procédures, mais qu'il s'agit de faciliter des procédures existantes. Le règlement grand-ducal précité prévoit une liste de données exclues du principe « *once only* » en raison de leur nature sensible. Cette sensibilité est déterminée par le Ministère en fonction de leur nature.

Mme Taina Bofferding (LSAP) aimerait connaître les conséquences de la non-validation des données par l'administré provenant d'un échange entre les administrations dans le cadre d'une démarche administrative.

Mme Stéphanie Obertin explique que l'échange de données vise à obtenir les données déjà à disposition de l'État, mais qu'il appartient au citoyen de vérifier la véracité des données avant de soumettre une demande ou démarche administrative. Ainsi, la vérification fait partie intégrante de la soumission d'une demande, de sorte qu'une démarche non vérifiée ne constitue par une demande adressée à une autorité administrative sur laquelle cette dernière peut se prononcer.

À une question afférente de Mme Liz Braz (LSAP), M. le Commissaire du Gouvernement à la protection des données auprès de l'État explique que les juridictions de l'ordre judiciaire et de l'ordre administratif sont uniquement visées par le projet de loi lorsqu'elles effectuent des missions administratives telles que des recrutements. En revanche, elles ne sont pas visées dans l'exercice de leurs fonctions juridictionnelles.

Mme Liz Braz (LSAP) et M. Sven Clement (Piraten) souhaite savoir si le registre des accès centralisé pour l'accès aux données à caractère personnel dans l'application du principe du « *once only* » à l'instar de celui prévu pour le Registre national des personnes physiques (ci-après « RNPP ») est un registre similaire à celui de l'Espagne.

Mme la Ministre de la Digitalisation explique que tout échange de données dans le cadre du principe du « *once only* » doit d'abord être prévu dans des protocoles expliquant le détail de ces échanges. En outre, l'article 11 du projet de loi prévoit que les administrés sont informés des données procurées ainsi que de leur origine.

Au vu du renvoi auRNPP , M. le directeur du CTIE précise que le projet de loi n'effectue aucune modification à la législation dudit registre, de sorte que toute utilisation de données issues du RNPP dans le cadre du principe « *once only* » sera enregistrée.

À une question complémentaire de Mme Liz Braz (LSAP), Mme Stéphanie Obertin précise que les protocoles précités seront publiquement consultables.

M. André Bauler (DP) aimerait savoir dans quelle mesure le principe du « *once only* » pourrait être applicable dans le cas d'études du STATEC.

Mme Stéphanie Obertin explique que ce cas de figure correspondrait davantage à une réutilisation de données par une autre administration publique et que la finalité de traitement devrait dès lors correspondre à une des finalités prévues à l'article 15 pour pouvoir être effectuée.

À une question afférente de Mme Françoise Kemp (CSV), Mme la Ministre de la Digitalisation confirme que des chercheurs ne pourront pas télécharger des données sur leurs ordinateurs, mais qu'ils auront la possibilité de les consulter dans des environnements sécurisés. Seuls les résultats de leurs analyses pourront être sauvegardés sur leurs propres appareils.

❖ **Prochaines étapes de l'instruction parlementaire**

Suite à une proposition afférente de M. Sven Clement (Piraten), les membres de la Commission sont invités à soumettre leurs questions relatives au projet de loi par écrit.

La Commission procèdera probablement à l'examen des différents articles du projet de loi après la réception des avis afférents.

4. Divers

Mme la Ministre de la Digitalisation informe qu'elle proposera au Gouvernement le retrait du projet de loi n° 8168. Ce projet de loi avait comme vocation de tester le portefeuille numérique avant l'introduction d'un cadre légal au niveau européen à travers une refonte du règlement européen dit « eIDAS ». Cependant, le Conseil d'État a soulevé plusieurs réflexions fondamentales. En outre, la version modifiée du règlement « eIDAS » vient d'entrer en vigueur. Au vu de ces éléments, il est proposé de procéder à l'élaboration d'une nouvelle initiative législative pour mettre en œuvre le portefeuille numérique en conformité avec le règlement « eIDAS ».

Annexe
Présentation relative au projet de loi n°8395 préparée par le Ministère de la Digitalisation

Procès-verbal approuvé et certifié exact

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation

Projet de loi relatif à la valorisation des données dans un environnement de confiance

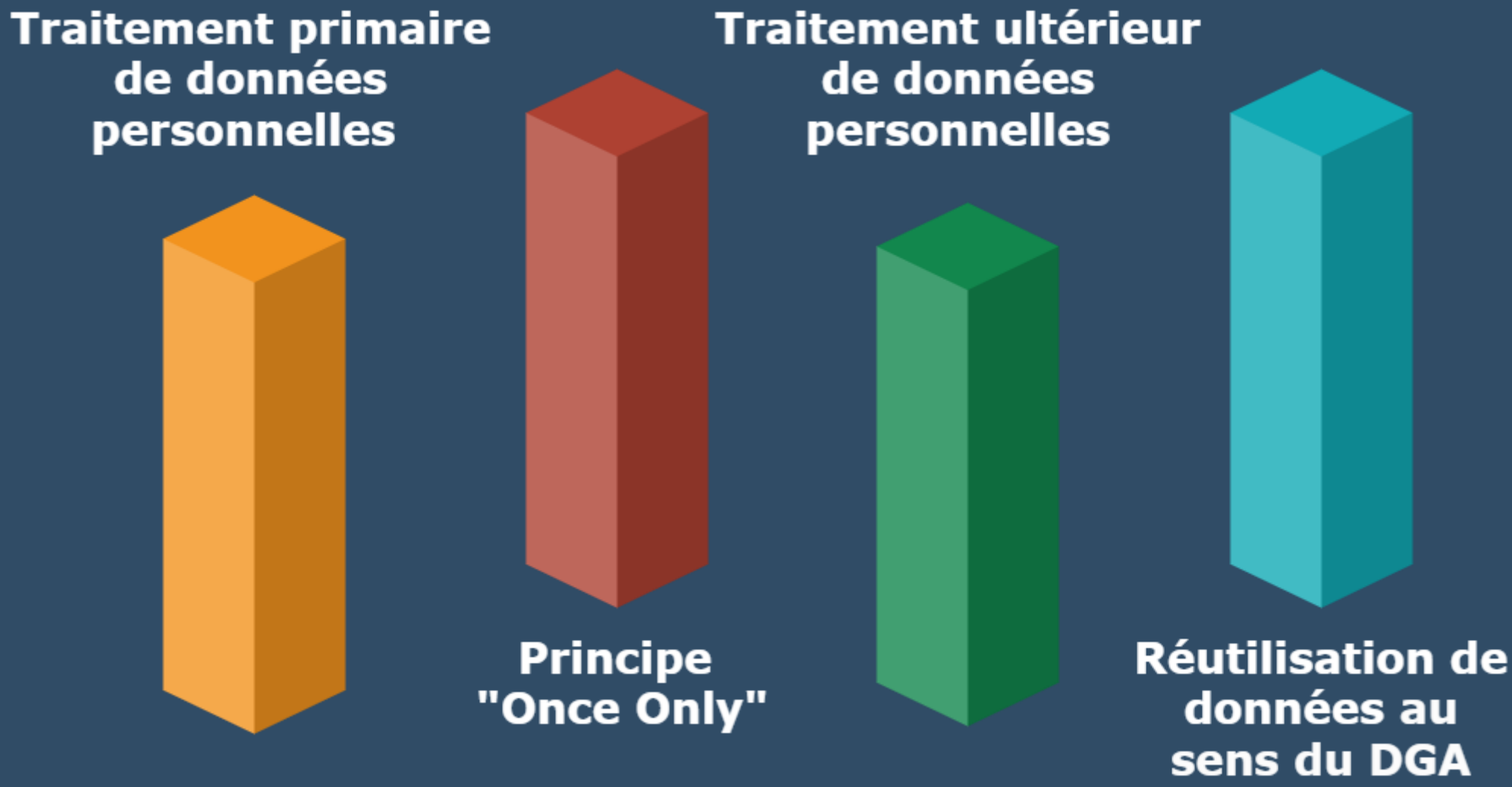
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation

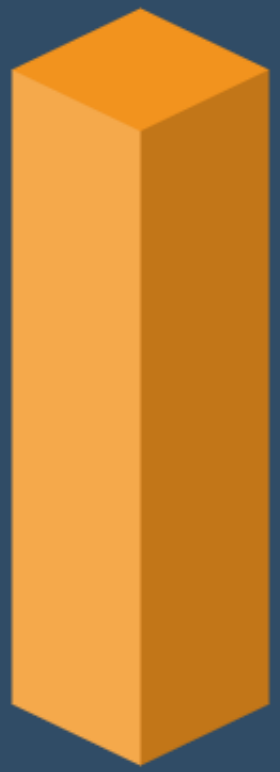
Transformation de l'État en secteur public axé sur les données et proactif

Objectifs

- **Simplification administrative pour le citoyen, les entreprises et les administrations**
- **Donner une valeur ajoutée aux données détenues par l'État**
- **Permettre aux administrations de proposer des démarches de manière proactive**
- **Faciliter la prise de décision éclairée basée sur les données**

4 piliers


Traitement primaire de données personnelles
Principe "Once Only"
Traitement ultérieur de données personnelles
Réutilisation de données au sens du DGA



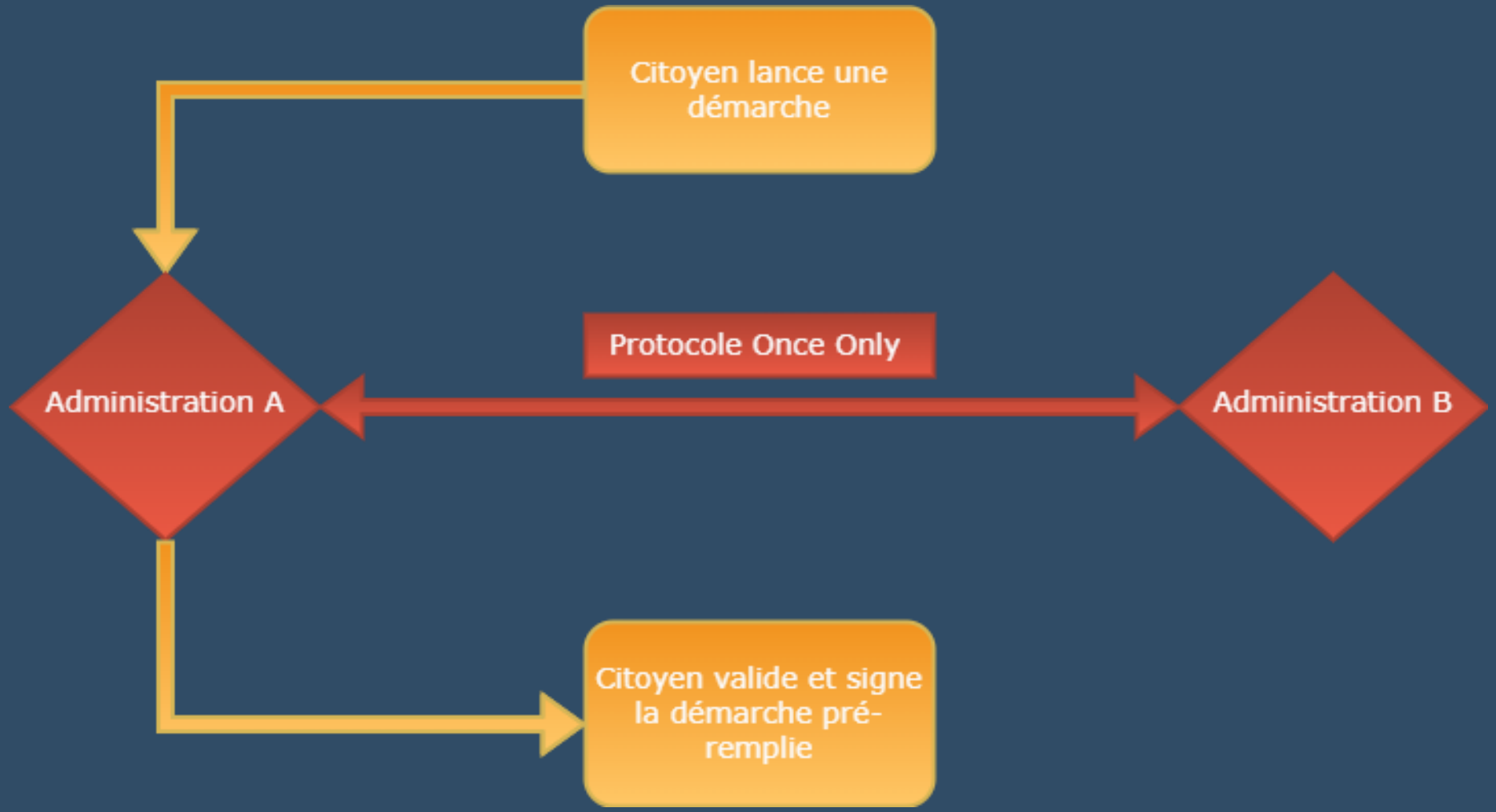
Traitement primaire de données personnelles

Les entités publiques sont, dans le respect du RGPD, habilitées à traiter les données personnelles nécessaires aux fins relevant de l'exécution de leurs missions d'intérêt public, dont elles sont investies par une disposition de droit de l'UE ou de droit national.

Principe « Once Only »

- Collecte des données disponibles auprès d'autres administrations et non pas auprès de l'administré
- Établissement de protocoles « Once Only » entre les administrations concernées
- Information du public concernant les protocoles établis

Dans la pratique



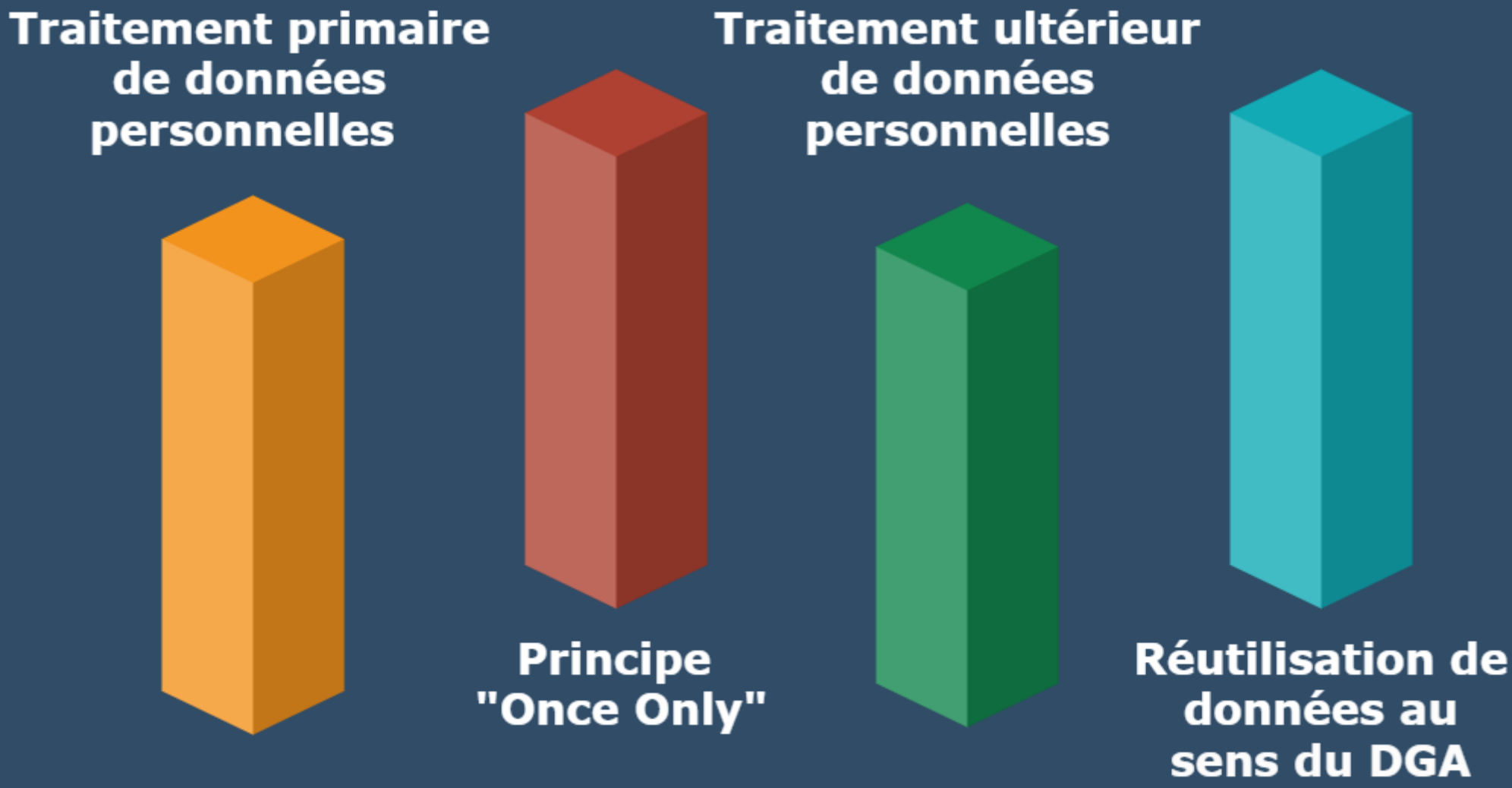
Traitements ultérieurs de données personnelles

Traitement ultérieur de données par les entités publiques à des fins autorisées par le projet de loi (recherche scientifique, statistiques, planification des politiques,…).

Réutilisation de données personnelles au sens du DGA

Réutilisation de données détenues par le secteur public par les acteurs du secteur privé à des fins autorisées par le projet de loi (recherche scientifique, statistiques, développement de produits et de technologies…).

4 piliers


Traitement primaire de données personnelles
Principe "Once Only"
Traitement ultérieur de données personnelles
Réutilisation de données au sens du DGA

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation
4, rue de la Congrégation
L-1352 Luxembourg

info@digital.etat.lu
www.digitalisation.lu

8395/01

A-4088/24-25

Doc. parl. n° 8395

CHFEP
Chambre des fonctionnaires et employés publics

AVIS

du 21 octobre 2024

sur

le projet de loi relatif à la valorisation des données dans un environnement de confiance

et sur

le projet de règlement grand-ducal relatif à la valorisation des données dans un environnement de confiance

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

8395/02

N°8395/2
Entrée le 25.10.2024
Chambre des Députés

CHAMBRE DES SALARIÉS
LUXEMBOURG

AVIS

Avis III/32/2024 23 octobre 2024

Valorisation des données dans un environnement de confiance

relatif aux

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).

Projet de règlement grand-ducal fixant certaines modalités d'application de la loi du […] relative à la valorisation des données dans un environnement de confiance

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 ;*
- *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.

[1]Source : https://eur-lex.europa.eu/FR/legal-content/summary/european-data-governance.html

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,

Sylvain HOFFMANN
Directeur

Nora BACK
Présidente

L'avis a été adopté à l'unanimité.

8395/03

N°8395/3
Entrée le 30.10.2024
Chambre des Députés

OAI
ORDRE DES ARCHITECTES ET DES INGENIEURS-CONSEILS

Avis OAI 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).

Sommaire **Page**

1. Considérations générales 2
2. Méthodologie 3
3. Avis article par article sur le projet de loi n°8395 relatif à la valorisation des données dans un environnement de confiance 3
4. Conclusion 4

1. Considérations générales

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 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, 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 transversales 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. Méthodologie

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 à la valorisation des données 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
Présidente

Patrick NOSBUSCH
Vice-Président

Pierre HURT
Directeur