Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Date de création : 17-10-2025

Projet de loi 8395B

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

Date de dépôt : Date inconnue

Liste des documents

Date	Description	Nom du document	Page
23-04-2025	Amendements adoptés par la/les commission(s) : Commission de l'Enseignement supérieur, de la Recherche et de la Digitalisation	20250515_AmendementParlementaire	3
29-04-2025	Avis du Syndicat des Villes et Communes Luxembourgeoises (31.3.2025)	20250516_Avis	55
13-06-2025	Amendement gouvernemental	20250821_AmendementGouvernemental	64
24-07-2025	Avis : FEDIL Health Corporations	20250724_Avis	105

20250515_AmendementParlementaire

Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

Dossier suivi par Dan Schmit
Service des Commissions
Tel. : +352 466 966 345
Courriel : dschmit@chd.lu

Monsieur le Président
du Conseil d'État
5, rue Sigefroi
L-2536 Luxembourg

Luxembourg, le 22 avril 2025

Objet : **8395** **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).

Monsieur le Président,

J'ai l'honneur de vous soumettre ci-après une série d'amendements au projet de loi sous rubrique, adoptés par la Commission de l'Enseignement supérieur, de la Recherche et de la Digitalisation (ci-après « Commission ») lors de sa réunion du 22 avril 2025.

Je joins en annexe, à toutes fins utiles, un texte coordonné du projet de loi sous rubrique reprenant les amendements parlementaires exposés *sub* III (**figurant en caractères gras et soulignés**) et les adaptations découlant directement de la scission du projet de loi exposée *sub* I ainsi que les erreurs matérielles que la Commission propose de rectifier exposées *sub* II (figurant en caractères soulignés).

*

I. Scission du projet de loi initial

La Commission décide de scinder le projet de loi n°8385 en deux projets de loi distincts, à savoir :

- le projet de loi n°8395A relative à la désignation des organismes et autorités compétents et au point d'information uniquement prévus aux articles 7, 8, 13 et 23 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;

- le projet de loi n°8395B relative à
  1° la valorisation des données dans un environnement de confiance ;
  2° la mise en œuvre du principe « *once only* » ;
  3° la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ;
  4° la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Le projet de loi n°8395A comprend les articles 4, paragraphe 1er, 7, paragraphe 1er, 39, 40, 44 et 45 du projet de loi n°8395 initial.

En ce qui concerne la structure du projet de loi n°8395A, cette dernière se présente comme suit :

Projet de loi 8395	Projet de loi 8395A
Article 4, paragraphe 1er	Article 1er
Article 7, paragraphe 1er	Article 2
Article 39	Article 3
Article 40	Article 4
Article 44	Article 5
Article 45	Article 6

La renumérotation des articles à la suite de cette scission, nécessite l'adaptation de deux renvois dans le dispositif du projet de loi n°8395A :

1° à l'article 40 du projet de loi n°8395, devenant l'article 4 du projet de loi, il y a lieu de remplacer le renvoi à l'article 39 par un renvoi à l'article 3 ;

2° à l'article 45 du projet de loi n°8395, devenant l'article 6 du projet de loi n°8395A, il y a lieu de remplacer le renvoi à l'article 44 par un renvoi à l'article 5.

Le projet de loi n°8395B comprend les articles du projet de loi n°8395 initial ne faisant pas partie du projet de loi n°8395A.

À toutes fins utiles, un tableau de concordance du projet de loi n°8395B est joint à la présente.

À noter que l'intégration des articles 44 et 45 dans le projet de loi n°8395A a comme conséquence qu'au titre VII du projet de loi n°8395B, la section II ne contient plus d'article. Il y a dès lors lieu de supprimer cette section et de renuméroter les sections suivantes.

Cette scission est motivée par l'urgence de notifier les différents organismes et autorités compétents prévus au règlement (UE) 2022/868 à la Commission européenne. En effet, la Commission a appris que la Commission européenne insiste que ces organismes et autorités,

qui auraient déjà dû lui être notifiés le 24 septembre 2023, seront communiqués dans les meilleurs délais.

La Commission propose dès lors de procéder dans les meilleurs délais au vote des dispositions prévoyant la désignation de ces entités dorénavant prévues au projet de loi n°8395A et laissant le temps nécessaire à tous les acteurs impliqués dans la procédure législative de dûment analyser les autres dispositions du projet de loi n°8395 qui sont dorénavant prévues au projet de loi n°8395B.

*

II. Redressement d'erreurs matérielles

La Commission a procédé au redressement des erreurs matérielles suivantes dans le dispositif du projet de loi n°8395B :

1° à l'article 7, paragraphe 1er (initialement l'article 7, paragraphe 2, du projet de loi n°8395), il convient de rectifier les erreurs matérielles suivantes :
a) à la lettre a), devenant le point 1° en vertu de l'amendement 13 repris ci-dessous, il y a lieu de remplacer les termes « par le » par le terme « au » ;
b) à la lettre c), devenant le point 3° en vertu de l'amendement 13 repris ci-dessous, il y a lieu d'insérer une virgule après les termes « paragraphe 2 » ;

2° à l'article 16, il convient de redresser les erreurs matérielles suivantes :
a) au paragraphe 1er, il y a lieu d'insérer une virgule après les termes « paragraphe 1er » ;
b) au paragraphe 2, il y a lieu d'insérer une virgule après les termes « paragraphe 1er » ;
c) au paragraphe 3, il y a lieu d'insérer des virgules après les termes « paragraphe 1er » et « point 2° » ;

3° à l'article 17, paragraphe 2, il y a lieu d'insérer une virgule après les termes « paragraphe 1er » ;

4° à l'article 22, paragraphe 1er, il convient de redresser les erreurs matérielles suivantes :
a) à la phrase liminaire, il y a lieu d'insérer une virgule après les termes « point 2° » ;
b) à lettre a), il y a lieu d'insérer une virgule après les termes « paragraphe 2 » ;

5° à l'article 23, paragraphe 1er, il convient de redresser les erreurs matérielles suivantes :
a) à la phrase liminaire, il y a lieu d'insérer une virgule après les termes « points 1° à 3° » ;
b) au point 2°, lettre a), il y a lieu d'insérer une virgule après les termes « paragraphe 2 » ;

6° à l'article 27, paragraphe 2, point 4°, il y a lieu d'insérer une virgule après les termes « paragraphe 3 » ;

7° à l'article 28, il convient de redresser les erreurs matérielles suivantes :
a) au paragraphe 1er, point 14°, il y a lieu d'insérer des virgules après les termes « point 2, lettre b) » et « article 23, paragraphe 2 » ;
b) au paragraphe 3, il y a lieu d'insérer une virgule après les termes « paragraphe 3 » ;
c) au paragraphe 4, point 3°, il y a lieu d'insérer une virgule après les termes « paragraphe 3 » ;

8° à l'article 31, il convient de redresser les erreurs matérielles suivantes :
a) au paragraphe 2, point 1°, lettre b), point i, il y a lieu d'insérer une virgule après les termes « paragraphe 2 » ;

b) au paragraphe 5, alinéa 1er, il y a lieu d'insérer des virgules après les termes « point 7 » et « point 10° » ;

*

III. Amendements

Amendements visant le dispositif du projet de loi n°8395A

Amendement 1

L'article 4, paragraphe 1er, du projet de loi n°8395, devenant l'article 1er du projet de loi n°8395A, est amendé comme suit :

« **Art. 4 1er. ~~Autorité des données~~ Organismes compétents**

~~(1)~~ Le Commissariat du Gouvernement à la protection des données auprès de l'État **~~est chargé des missions attribuées à l'Autorité des données par la présente loi. Dans l'exercice de ces missions, le Commissariat du Gouvernement à la protection des données auprès de l'État est désigné ci-après par le terme « Autorité des données »~~ est désigné organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), dénommé ci-après « règlement (UE) 2022/868 », habilité, conformément à l'article 7, paragraphe 2, du même règlement, à octroyer ou à refuser l'accès aux fins de réutilisation des données**.».

Commentaire :

L'amendement sous rubrique modifie l'article 4, paragraphe 1er, du projet de loi initial qui devient l'article 1er du projet de loi n°8395A. Plus précisément, le libellé est amendé pour prévoir que le Commissariat du Gouvernement à la protection des données auprès de l'État est désigné organisme compétent au sens de l'article 7, paragraphe 1er, du règlement sur la gouvernance des données. Par ailleurs, ledit Commissariat sera également habilité à octroyer ou refuser l'accès aux fins de réutilisation des données tel que le prévoit l'article 7, paragraphe 2, du même règlement. Ainsi, le nouveau libellé regroupe la plupart des éléments initialement prévus à l'article 4, paragraphes 1er et 2, du projet de loi initial, et n'apporte dès lors aucun élément nouveau au dispositif en ce qui concerne son fond.

Amendement 2

L'article 7, paragraphe 1er, du projet de loi n°8395, devenant l'article 2 du projet de loi n°8395A, est amendé comme suit :

« **Art. ~~7~~ 2. Point d'information unique**

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

Commentaire :

Étant donné que les articles suivants du projet de loi n°8395A ne renvoient pas au point d'information unique, le bout de phrase prévoyant une forme abrégée pour désigner ce point d'information unique dans la suite du dispositif devient superfétatoire.

Amendement 3

L'article 39 du projet de loi n°8395, devenant l'article 3 du projet de loi n°8395A, est amendé comme suit :

> « **Art. ~~39~~ 3. Autorité compétente en matière d'intermédiation de données**
>
> La Commission nationale pour la protection des données, désignée ci-après **~~par le terme~~** « CNPD », est l'autorité compétente pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données, telle que visée à l'article 13 du règlement (UE) 2022/868. ».

Commentaire :

L'amendement sous rubrique adapte l'intitulé de l'article 39 du projet de loi n°8395, devenant l'article 3 du projet de loi n°8395A, afin de faciliter la distinction entre les articles 3 et 5 du projet de loi n°8395A.

Par ailleurs, cet amendement prévoit la suppression des termes « par le terme » étant donné que ces derniers sont superfétatoires.

Amendement 4

L'intitulé de l'article 40 du projet de loi n°8395, devenant l'article 4 du projet de loi n°8395A, est amendé comme suit :

> « **Art. ~~40~~ 4. Pouvoirs de l'autorité compétente en matière d'intermédiation de données** ».

Commentaire :

Cet amendement vise à faciliter la distinction entre les articles 4 et 6 du projet de loi n°8395A.

Amendement 5

L'intitulé de l'article 44 du projet de loi n°8395, devenant l'article 5 du projet de loi n°8395A, est amendé comme suit :

> « **Art. ~~44~~ 5. Autorité compétente en matière d'altruisme des données** ».

Commentaire :

Cet amendement vise à faciliter la distinction entre les articles 3 et 5 du projet de loi n°8395A.

Amendement 6

L'intitulé de l'article 45 du projet de loi n°8395, devenant l'article 6 du projet de loi n°8395A, est amendé comme suit :

> « **Art. ~~45~~ 6. Pouvoirs de l'autorité compétente en matière d'altruisme des données** ».

Commentaire :

Cet amendement vise à faciliter la distinction entre les articles 4 et 6 du projet de loi n°8395A.

Amendement 7

À la suite de l'article 6 du projet de loi n°8395A est inséré un article 7 nouveau libellé comme suit :

« **Art. 7. Intitulé de citation**

La référence à la présente loi se fait sous la forme suivante : « loi du […] relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 ». ».

Commentaire :

Étant donné que l'article 2 du projet de loi n°8395B tel qu'amendé renvoie au projet de loi n°8395A, la Commission estime qu'il est opportun de prévoir un intitulé de citation.

Amendements visant le dispositif du projet de loi n°8395B

Amendement 8

L'article 1er du projet de loi n°8395, devenant l'article 1er du projet de loi n°8395B, est amendé comme suit :

1° le titre est modifié comme suit :

« **Art. 1er. Objet** » ;

2° le paragraphe 1er, point 4°, est modifié comme suit :

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

Commentaire :

L'amendement sous rubrique vise à apporter deux adaptations d'ordre légistique au dispositif de l'article 1er du projet de loi n°8395B.

Amendement 9

L'article 2 du projet de loi n°8395, devenant l'article 2 du projet de loi n°8395B, est amendé comme suit :

« **Art. 2. Définitions**

(1) **~~Sauf dispositions particulières contraires au paragraphe 2~~ ~~du présent article, les~~ Les** termes et expressions **~~utilisés dans la présente loi ont la signification que leur donnent le~~ définis à l'article 2 du** règlement (UE) 2022/868 et **~~le~~ à l'article 4 du** règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), **dénommé** ci-après **~~désigné par le terme~~** « règlement (UE) 2016/679 »**, ont la même signification dans la présente loi**.

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

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

2° « Autorité des données » : le Commissariat du Gouvernement à la protection des données auprès de l'État ;

~~2°~~ 3° « entité publique » : un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal aux fins d'application des dispositions des titres IV et V. Toutefois, ne sont pas considérées comme entité publique aux fins d'application de la présente loi :

a) **la Chambre des Députés ;**

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

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

4° « point d'information unique » : le point d'information unique visé à l'article 2 de la loi du […] relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 ;

~~3°~~ 5° « tiers de confiance » : toute entité fonctionnellement indépendante des entités publiques visées au titre V, des organismes du secteur public détenant les données et du réutilisateur de données visés au titre VI, qui remplit les conditions prévues à l'article 6. ».

Commentaire :

L'amendement sous rubrique prévoit plusieurs adaptations de l'article 2 du projet de loi n°8395B.

Premièrement, le libellé du paragraphe 1er est adapté dans un souci de cohérence avec d'autres textes renvoyant à des définitions prévues dans un règlement européen. En l'occurrence, la Commission s'est inspirée d'une proposition de texte du Conseil d'État dans son avis relatif au projet de loi relatif à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique.

Deuxièmement, un point 2° nouveau est inséré au paragraphe 2 afin de définir la notion d'« Autorité des données ». Cette notion était définie à l'article 4, paragraphe 1er, du projet de loi initial. En conséquence de la scission du projet de loi, il est proposé d'intégrer la définition à l'article 2 du projet de loi n°8395B.

Troisièmement, le paragraphe 2, point 3°, est complété par une lettre a) nouvelle afin d'exclure explicitement la Chambre des Députés de la notion d'« entité publique ». Dans sa teneur initiale, le point 3° manque de clarté quant à la situation de la Chambre des Députés étant donné qu'elle n'est visée ni par l'énumération des entités visées par cette notion ni par celle des entités exclues de la notion. Après consultation, les organes compétents de la Chambre des Députés ont décidé que l'institution devrait être explicitement exclue de la notion d'« entité publique », de sorte qu'elle ne sera pas visée par les dispositions du projet de loi n°8395B s'appliquant aux entités publiques.

Quatrièmement, en conséquence de la scission du projet de loi n°8395 initial, la Commission insère un point 4° nouveau au paragraphe 2 prévoyant la définition de la notion de « point d'information unique ». Cette définition renvoie au point d'information unique prévu au projet de loi n°8395A.

Ces modifications entraînent la renumérotation de plusieurs points et lettres au paragraphe 2.

Amendement 10

L'article 4, paragraphes 2 à 6, du projet de loi n°8395, devenant l'article 4, paragraphes 1er à 5, du projet de loi n°8395B, est amendé comme suit :

« **Art. 4. Autorité des données**

(**2** **1**) L'Autorité des données **~~est désignée organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868, habilité, conformément à l'article 7, paragraphe 2, du même règlement, à~~** octro~~y~~ie~~r~~ ou refuse~~r~~ l'accès aux fins de réutilisation des données **visées à l'article 3, paragraphe 1er, du règlement (UE) 2022/868** conformément aux dispositions des titres VI et VII.

(**3** **2**) L'Autorité des données est habilitée à autoriser ou refuser le traitement ultérieur de données à caractère personnel par les entités publiques conformément aux dispositions des titres V et VII.

(**4** **3**) L'Autorité des données a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** de collaborer étroitement avec le Centre des technologies de l'information de l'État, **~~dénommé~~** **désigné** ci-après **~~par le terme~~** « Centre », le tiers de confiance mandaté par le Centre et le groupement d'intérêt économique

PNED G.I.E. - Plateforme nationale d'échange de données, désigné ci-après ~~par le terme~~ « LNDS » ;

~~c)~~ **3°** de fonctionner comme organe de réflexion et d'impulsion dans le domaine du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation de données et de formuler des avis et des propositions en la matière au ministre ayant la digitalisation dans ses attributions ;

~~d)~~ **4°** de proposer au ministre ayant la digitalisation dans ses attributions des mesures en matière de politique de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données ;

~~e)~~ **5°** de conseiller, sur demande, le ministre ayant la digitalisation dans ses attributions sur les mesures en matière de traitement ultérieur de données à caractère personnel ;

~~f)~~ **6°** de promouvoir les bonnes pratiques à travers les entités publiques, en matière de traitement ultérieur de données à caractère personnel, et à travers les organismes de droit public en matière d'accès et de réutilisation de données ;

~~g)~~ **7°** de sensibiliser les entités publiques, les organismes de droit public et le public en matière de traitement ultérieur de données à caractère personnel et en matière d'accès et de réutilisation de données.

(~~5~~ **4**) L'Autorité des données dispose des ressources nécessaires pour exercer ses missions. Il peut recourir aux services d'experts.

(~~6~~ **5**) L'Autorité des données veille à ce que son personnel chargé des missions prévues aux paragraphes ~~2 et 3~~ **1er et 2** ne soit pas impliqué dans la préparation des demandes visées ~~à la section II du titre VII~~ **au titre VII, section II,** dans l'exercice de ses missions prévues aux articles 57 et 58 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. ».

Commentaire :

L'amendement sous rubrique apporte plusieurs adaptations au dispositif de l'article 4 du projet de loi n°8395B.

Premièrement, le paragraphe 1er (anciennement le paragraphe 2 du projet de loi n°8395) est adapté pour tenir compte du fait que le projet de loi n°8395A prévoit la désignation du Commissariat du Gouvernement à la protection des données auprès de l'État en tant qu'organisme compétent. Ainsi, il n'est plus nécessaire de réitérer ce point au projet de loi n°8395B. Cependant, comme le projet de loi n°8395B prévoit les procédures applicables aux demandes d'accès à la réutilisation de données, il y a lieu de préciser que les décisions d'octroi et de refus par l'organisme compétent se font en conformité avec les dispositions des titres VI et VII.

Deuxièmement, dans un souci de cohérence à travers l'intégralité du dispositif, la Commission procède à l'uniformisation des énumérations dans le dispositif du projet de loi n°8395B. En l'occurrence, il y a dès lors lieu de remplacer les lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Troisièmement, en raison de la renumérotation des paragraphes en conséquence de la scission du projet de loi initial, il y a lieu d'adapter le renvoi au paragraphe 5.

Enfin, des légères modifications d'ordre légistique sont effectuées.

Amendement 11

À l'article 5, paragraphes 2 à 4, du projet de loi n°8395, devenant l'article 5, paragraphes 2 à 4, du projet de loi n°8395B, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

Dans un souci de cohérence à travers le dispositif du projet de loi n°8395B, il est proposé de procéder à l'uniformisation de la forme des énumérations. En l'occurrence, ceci implique le remplacement des lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Amendement 12

À l'article 6, paragraphes 1er et 2, du projet de loi n°8395, devenant l'article 6, paragraphes 1er et 2, du projet de loi n°8395B, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

Dans un souci de cohérence à travers le dispositif du projet de loi n°8395B, il est proposé de procéder à l'uniformisation de la forme des énumérations. En l'occurrence, ceci implique le remplacement des lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Amendement 13

À l'article 7, paragraphes 2 et 3, du projet de loi n°8395, devenant l'article 7, paragraphes 1er et 2, du projet de loi n°8395B, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

Dans un souci de cohérence à travers le dispositif du projet de loi n°8395B, il est proposé de procéder à l'uniformisation de la forme des énumérations. En l'occurrence, ceci implique le remplacement des lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Amendement 14

L'article 8, paragraphe 1er, du projet de loi n°8395, devenant l'article 8, paragraphe 1er, du projet de loi n°8395B, est amendé comme suit :

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

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 15

À l'article 9, paragraphe 3, du projet de loi n°8395, devenant l'article 9, paragraphe 3, du projet de loi n°8395B, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

Dans un souci de cohérence à travers le dispositif du projet de loi n°8395B, il est proposé de procéder à l'uniformisation de la forme des énumérations. En l'occurrence, ceci implique le remplacement des lettres (a), b), c), …) par des points (1°, 2°, 3°, …).

Amendement 16

L'article 11 du projet de loi n°8395, devenant l'article 11 du projet de loi n°8395B, est amendé comme suit :

1° au paragraphe 2, alinéa 2, les termes « l'alinéa qui précède » sont remplacés par les termes « l'alinéa 1er » ;

2° le paragraphe 4 est modifié comme suit :

a) l'alinéa 1er est modifié comme suit :
   i. aux énumérations, les lettres sont remplacées par des points
   ii. à la fin de la lettre a), devenant le point 1°, le terme « et » est supprimé ;

b) à l'alinéa 2, les termes « l'alinéa qui précède » sont remplacés par les termes « l'alinéa 1er ».

Commentaire :

L'amendement sous rubrique prévoit plusieurs adaptations d'ordre légistique.

Amendement 17

L'article 12 du projet de loi n°8395, devenant l'article 12 du projet de loi n°8395B, est amendé comme suit :

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

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

~~a)~~ **1°** dans le cadre du traitement effectué dans l'exercice de leurs missions des demandes et déclarations présentées par un administré ;

~~b)~~ **2°** pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

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

entités publiques auprès desquelles les informations et données à caractère personnel pourraient être obtenues.

Dans un délai d'un mois à partir de la notification visée à l'alinéa ~~**qui précède**~~ **1er**, les entités publiques notifiées :

~~**a)**~~ **1°** certifient la disponibilité des informations et des données à caractère personnel à l'entité publique demanderesse et confirment que l'échange d'informations et de données à caractère personnel n'est pas impossible ; ou

~~**b)**~~ **2°** informent l'entité publique demanderesse du fait qu'elles ne détiennent pas les informations et les données à caractère personnel sollicitées ou que l'échange d'informations et de données à caractère personnel est impossible.

Une copie de l'information visée ~~**aux points a) et b) du présent paragraphe**~~ **à l'alinéa 2, points 1° et 2°,** est transmise au ministre ayant la digitalisation dans ses attributions.

(3) Dans les cas visés au ~~**point a) du paragraphe qui précède**~~ **au paragraphe 2, alinéa 2, point 2°**, les entités publiques concluent dans les meilleurs délais, et au plus tard après trois mois, le protocole visé à l'article 13. ».

Commentaire :

L'amendement sous rubrique vise plusieurs adaptations d'ordre légistique.

Amendement 18

À l'article 13, paragraphe 2, du projet de loi n°8395, devenant l'article 13, paragraphe 2, du projet de loi n°8395B, les termes « paragraphe qui précède » sont remplacés par les termes « paragraphe 1er ».

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 19

À l'article 14, paragraphe 2, du projet de loi n°8395, devenant l'article 14, paragraphe 2, du projet de loi n°8395, les termes « paragraphes qui précède » sont remplacés par les termes « paragraphe 1er ».

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 20

L'article 20, point 1°, du projet de loi n°8395, devenant l'article 20, point 1°, du projet de loi n°8395B, est amendé comme suit :

« 1° les conditions énoncées à la section II ~~**du présent titre**~~ sont remplies ; ~~**et**~~ ».

Commentaire :

L'amendement sous rubrique vise deux adaptations d'ordre légistique.

Amendement 21

L'article 27 du projet de loi n°8395, devenant l'article 27 du projet de loi n°8395B, est amendé comme suit :

1° au paragraphe 1er, points 13° et 15°, les termes « du présent paragraphe » sont supprimés ;

2° au paragraphe 3°, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

L'amendement sous rubrique vise des adaptations d'ordre légistique.

Amendement 22

L'article 28 du projet de loi n°8395, devenant l'article 28 du projet de loi n°8395B, est amendé comme suit :

1° le paragraphe 1er est modifié comme suit :

a) au point 12°, les termes « du présent paragraphe » sont supprimés ;

b) le point 13° est amendé comme suit :

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

c) au point 14°, les termes « du présent paragraphe » sont supprimés ;

2° au paragraphe 5, aux énumérations, les lettres sont remplacées par des points.

Commentaire :

L'amendement sous rubrique vise des adaptations d'ordre légistique.

Amendement 23

L'article 29, paragraphe 1er, du projet de loi n°8395, devenant l'article 29, paragraphe 1er, du projet de loi n°8395, est amendé comme suit :

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

Commentaire :

L'amendement sous rubrique vise deux adaptations d'ordre légistique.

Amendement 24

L'article 31 du projet de loi n°8395, devenant l'article 31 du projet de loi n°8395, est amendé comme suit :

1° au paragraphe 1er, aux énumérations, les lettres sont remplacées par des points ;

2° le paragraphe 2 est amendé comme suit :

a) au point 1°, lettre b), point ii, les termes « visés au point 2° du présent paragraphe » sont remplacés par le terme « concernés » ;
b) au point 2°, lettre b), point ii, les termes « visés au point 2° du présent paragraphe » sont remplacés par le terme « concernés » ;
c) au point 3°, les termes « du présent paragraphe » sont supprimés ;

3° le paragraphe 5, alinéa 2, est amendé comme suit :

a) au point 1°, lettre d), les termes « au point » sont remplacés par les termes « à la lettre » ;
b) au point 2°, lettre d), les termes « au point » sont remplacés par les termes « à la lettre ».

Commentaire :

L'amendement sous rubrique vise principalement des adaptations d'ordre légistique.

Les modifications opérées au paragraphe 2, points 1° et 2°, visent à tenir compte de renvois erronés. Il est proposé de remplacer ces renvois par des renvois aux organismes du secteur public compétents.

Amendement 25

À l'article 33 du projet de loi n°8395, devenant l'article 33 du projet de loi n°8395B, les termes « du présent titre » sont supprimés.

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 26

L'article 35 du projet de loi n°8395, devenant l'article 35 du projet de loi n°8395B, est amendé comme suit :

1° au paragraphe 2, alinéa 4, à l'énumération, les lettres sont remplacées par des points.

2° le paragraphe 4 est amendé comme suit :

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

~~a)~~ **1°** le Centre, ou le tiers de confiance mandaté par le Centre, s'assure de la mise en œuvre les mesures visées au présent article conformément aux stipulations du plan de confidentialité ;

~~b)~~ **2°** le Centre :

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

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

Commentaire :

L'amendement sous rubrique vise des adaptations d'ordre légistique.

Amendement 27

L'article 36 du projet de loi n°8395, devenant l'article 36 du projet de loi n°8395B, est amendé comme suit :

1° au paragraphe 1er, alinéa 2, à l'énumération, les lettres sont remplacées par des points ;

2° au paragraphe 2, à l'énumération, les lettres sont remplacées par des points ;

3° au paragraphe 3, alinéa 1er, les termes « point b) » sont remplacés par les termes « point 2° » ;

4° au paragraphe 4, à l'énumération, les lettres sont remplacées par des points.

Commentaire :

L'amendement sous rubrique vise des adaptations d'ordre légistique.

Amendement 28

À l'article 43, paragraphe 1er, du projet de loi n°8395, devenant l'article 41, paragraphe 1er, du projet de loi n°8395B, le chiffre « 100.000 » est remplacé par celui de « 100 000 ».

Commentaire :

L'amendement sous rubrique vise une adaptation d'ordre légistique.

Amendement 29

L'article 46 du projet de loi n°8395, devenant l'article 42 du projet du projet de loi n°8395B, est amendé comme suit :

« **Art. ~~46~~ 42. Recours**

Un recours contre les décisions de la CNPD prises en application des **~~sections I et II du présent titre~~ chapitres III et IV du Règlement (UE) 2022/686** est ouvert devant le Tribunal administratif qui statue comme juge du fond. ».

Commentaire :

L'amendement sous rubrique vise à tenir compte de la scission du projet de loi n°8395 qui a comme conséquence que le renvoi aux sections I et II n'est plus possible. Il est dès lors proposé de renvoyer aux décisions prises en vertu des chapitres III et IV du Règlement (UE) 2022/686.

* * *

Au nom de la Commission, je vous saurais gré de bien vouloir faire aviser par le Conseil d'État les amendements exposés ci-dessus.

En ce qui concerne le projet de loi n°8395A, je vous saurais gré de bien vouloir le faire aviser dans les meilleurs délais.

J'envoie copie de la présente à la Ministre déléguée auprès du Premier ministre, chargée des Relations avec le Parlement, avec prière de transmettre les amendements aux instances à consulter.

Veuillez agréer, Monsieur le Président, l'expression de ma considération très distinguée.

(s.) Claude Wiseler
Président de la Chambre des Députés

Annexes :
[1] Tableau de concordance du projet de loi n°8395B
[2] Texte coordonné du projet de loi n°8395A proposé par la Commission
[3] Texte coordonné du projet de loi n°8395B proposé par la Commission

Annexe 1

Tableau de concordance du projet de loi n°8395B

Projet de loi 8395	Projet de loi 8395B
Article 1er	Article 1er
Article 2	Article 2
Article 3	Article 3
Article 4, paragraphes 2 à 6	Article 4, paragraphes 1er à 5
Article 5	Article 5
Article 6	Article 6
Article 7, paragraphes 2 et 3	Article 7, paragraphes 1er et 2
Article 8	Article 8
Article 9	Article 9
Article 10	Article 10
Article 11	Article 11
Article 12	Article 12
Article 13	Article 13
Article 14	Article 14
Article 15	Article 15
Article 16	Article 16
Article 17	Article 17
Article 18	Article 18
Article 19	Article 19
Article 20	Article 20
Article 21	Article 21
Article 22	Article 22
Article 23	Article 23
Article 24	Article 24
Article 25	Article 25
Article 26	Article 26
Article 27	Article 27
Article 28	Article 28
Article 29	Article 29
Article 30	Article 30
Article 31	Article 31
Article 32	Article 32
Article 33	Article 33
Article 34	Article 34
Article 35	Article 35
Article 36	Article 36
Article 37	Article 37
Article 38	Article 38
Article 41	Article 39
Article 42	Article 40
Article 43	Article 41
Article 46	Article 42
Article 47	Article 43

Annexe 2

Texte coordonné du projet de loi n°8395A

Projet de loi relative à la désignation des organismes et autorités compétents et au point d'information uniquement prévus aux articles 7, 8, 13 et 23 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)

Art. 4 1er. ~~Autorité des données~~ Organismes compétents

(1) Le Commissariat du Gouvernement à la protection des données auprès de l'État **~~est chargé des missions attribuées à l'Autorité des données par la présente loi. Dans l'exercice de ces missions, le Commissariat du Gouvernement à la protection des données auprès de l'État est désigné ci-après par le terme « Autorité des données »~~ est désigné organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), dénommé ci-après « règlement (UE) 2022/868 », habilité, conformément à l'article 7, paragraphe 2, du même règlement, à octroyer ou à refuser l'accès aux fins de réutilisation des données**.

Art. ~~7~~ 2. Point d'information unique

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

Art. ~~39~~ 3. Autorité compétente en matière d'intermédiation de données

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

Art. ~~40~~ 4. Pouvoirs de l'autorité compétente en matière d'intermédiation de données

Dans le cadre des tâches qui lui sont assignées à l'article ~~39~~ 3, la CNPD dispose des pouvoirs de contrôle tels que prévus à l'article 14 du règlement (UE) 2022/868.

Art. ~~44~~ 5. Autorité compétente en matière d'altruisme des données

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

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

Art. ~~45~~ 6. Pouvoirs de l'autorité compétente en matière d'altruisme des données

Dans le cadre des missions qui lui sont assignées à l'article 44 5, la CNPD dispose des pouvoirs de contrôle, tels que prévus à l'article 24 du règlement (UE) 2022/868.

Art. 7. Intitulé de citation

La référence à la présente loi se fait sous la forme suivante : « loi du […] relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 ».

Annexe 3

Texte coordonné du projet de loi n°8395B

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

TITRE I^er^ – Dispositions préliminaires

Art. 1^er^. Objet

(1) La présente loi vise :

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

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

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

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

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

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

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

Art. 2. Définitions

(1) ~~**Sauf dispositions particulières contraires au paragraphe 2 du présent article, les**~~ **Les** termes et expressions ~~**utilisés dans la présente loi ont la signification que leur**~~

~~donnent le~~ **définis à l'article 2 du** règlement (UE) 2022/868 et ~~le~~ **à l'article 4 du** règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), **dénommé** ci-après ~~désigné par le terme~~ « règlement (UE) 2016/679 »**, ont la même signification dans la présente loi**.

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

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

2° « Autorité des données » : le Commissariat du Gouvernement à la protection des données auprès de l'État ;

~~2°~~ **3°** « entité publique » : un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal aux fins d'application des dispositions des titres IV et V. Toutefois, ne sont pas considérées comme entité publique aux fins d'application de la présente loi :

a) la Chambre des Députés ;

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

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

4° « point d'information unique » : le point d'information unique visé à l'article 2 de la loi du […] relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 ;

~~3°~~ **5°** « tiers de confiance » : toute entité fonctionnellement indépendante des entités publiques visées au titre V, des organismes du secteur public détenant les données et du réutilisateur de données visés au titre VI, qui remplit les conditions prévues à l'article 6.

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

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

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

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

Art. 4. Autorité des données

(~~2~~ 1) L'Autorité des données ~~est désignée organisme compétent, conformément à l'article 7, paragraphe 1er, du règlement (UE) 2022/868, habilité, conformément à l'article 7, paragraphe 2, du même règlement, à~~ octroyier~~r~~ ou refuse~~r~~ l'accès aux fins de réutilisation des données **visées à l'article 3, paragraphe 1er, du règlement (UE) 2022/868** conformément aux dispositions des titres VI et VII.

(~~3~~ 2) L'Autorité des données est habilitée à autoriser ou refuser le traitement ultérieur de données à caractère personnel par les entités publiques conformément aux dispositions des titres V et VII.

(~~4~~ 3) L'Autorité des données a pour missions :

~~a)~~ 1° de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ 2° de collaborer étroitement avec le Centre des technologies de l'information de l'État, ~~dénommé~~ désigné ci-après ~~par le terme~~ « Centre », le tiers de confiance mandaté par le Centre et le groupement d'intérêt économique PNED G.I.E. - Plateforme nationale d'échange de données, désigné ci-après ~~par le terme~~ « LNDS » ;

~~c)~~ 3° de fonctionner comme organe de réflexion et d'impulsion dans le domaine du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation de données et de formuler des avis et des propositions en la matière au ministre ayant la digitalisation dans ses attributions ;

~~d)~~ 4° de proposer au ministre ayant la digitalisation dans ses attributions des mesures en matière de politique de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données ;

~~e)~~ 5° de conseiller, sur demande, le ministre ayant la digitalisation dans ses attributions sur les mesures en matière de traitement ultérieur de données à caractère personnel ;

~~f)~~ 6° de promouvoir les bonnes pratiques à travers les entités publiques, en matière de traitement ultérieur de données à caractère personnel, et à travers les organismes de droit public en matière d'accès et de réutilisation de données ;

~~g)~~ 7° de sensibiliser les entités publiques, les organismes de droit public et le public en matière de traitement ultérieur de données à caractère personnel et en matière d'accès et de réutilisation de données.

(~~5~~ 4) L'Autorité des données dispose des ressources nécessaires pour exercer ses missions. Il peut recourir aux services d'experts.

(~~6~~ 5) L'Autorité des données veille à ce que son personnel chargé des missions prévues aux paragraphes ~~2 et 3~~ 1er et 2 ne soit pas impliqué dans la préparation des demandes visées ~~à~~

~~la section II du titre VII~~ **au titre VII, section II,** dans l'exercice de ses missions prévues aux articles 57 et 58 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Art. 5. Assistance technique

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

(2) Le Centre a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** de mettre à disposition l'environnement de traitement sécurisé prévu à l'article 36 ;

~~c)~~ **3°** de fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles ;

~~d)~~ **4°** de s'assurer de la mise en œuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou à de modification, d'agrégation, de suppression et de traitement des informations et données selon toute autre méthode de contrôle de la divulgation des données conformément au plan de confidentialité, préalablement à la mise à disposition des données dans l'environnement de traitement sécurisé ;

~~e)~~ **5°** de collaborer étroitement avec l'Autorité des données, le tiers de confiance mandaté par le Centre, et le LNDS ;

~~f)~~ **6°** de proposer, sur décision du ministre ayant le Centre dans ses attributions, des services au LNDS relatifs à la mise en œuvre des dispositions de la présente loi.

(3) Le LNDS a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** d'aider les organismes du secteur public, le cas échéant, à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données conformément à leurs décisions spécifiques, y compris en ce qui concerne le territoire où le traitement des données est prévu et à aider les organismes du secteur public à mettre en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation des réutilisateurs, lorsque cela est réalisable en pratique ;

~~c)~~ **3°** de fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur en vertu de l'article 5, paragraphe 10**,** du règlement (UE) 2022/868 ;

~~d)~~ **4°** de collaborer étroitement avec l'Autorité des données, le Centre et le tiers de confiance mandaté par le Centre ;

~~e)~~ **5°** de fournir, sur demande, une assistance aux entités publiques et aux réutilisateurs de données dans le cadre de la préparation des demandes visées aux articles 27 et 28 et du plan de confidentialité visé à l'article 35.

(4) Le Centre et le LNDS :

~~a)~~ **1°** veillent à ce que le personnel chargé des missions conférées par la présente loi soit fonctionnellement indépendant des entités publiques visées au titre V, des organismes du secteur public détenant les données et des réutilisateurs de données visés au titre VI ;

~~b)~~ **2°** ne divulguent aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données ou permettant la divulgation de données qui sont protégées pour des motifs de protection des données à caractère personnel, de confidentialité commerciale, y compris le secret d'affaire, le secret professionnel, et le secret d'entreprise, de secrets statistique ou de protection de droits de propriété intellectuelle de tiers. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation ;

~~c)~~ **3°** désignent le personnel chargé des missions qui leurs sont conférées par la présente loi. Le personnel est désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données ;

~~d)~~ **4°** veillent à ce que le personnel chargé des missions qui leurs sont conférées par la présente loi ne soit pas chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données visés par la présente loi ;

~~e)~~ **5°** veillent à ce que le personnel chargé des missions qui leurs sont conférées par la présente loi n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui leurs sont conférés par la présente loi ou s'il y a incompatibilité, de fait ou de droit, avec l'exercice des tâches qui leurs sont conférées en application de la présente loi.

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

(6) Sans préjudice de l'article 23 du Code de procédure pénale, le personnel du Centre, du LNDS et du tiers de confiance chargé de l'exécution des missions conférées à ce dernier au

sens de la présente loi est tenu au secret professionnel et passible des peines prévues à l'article 458 du Code pénal.

Art. 6. Tiers de confiance

(1) Le tiers de confiance a pour missions :

~~a)~~ **1°** de mettre en œuvre les missions lui conférées par la présente loi ;

~~b)~~ **2°** d'effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données ;

~~c)~~ **3°** de collaborer étroitement avec l'Autorité des données, le Centre et le LNDS.

(2) Le tiers de confiance :

~~a)~~ **1°** dispose de ressources humaines et techniques suffisantes et de l'expertise adéquate pour s'acquitter efficacement des missions dont il est chargé conformément à la présente loi ;

~~b)~~ **2°** ne divulgue aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données, ou susceptible de porter préjudice aux droits à la protection des données, à la propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation ;

~~c)~~ **3°** désigne le personnel chargé des missions qui lui sont conférées par la présente loi. Le personnel est désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données ;

~~d)~~ **4°** veille à ce que le personnel chargé des missions qui lui sont conférées par la présente loi ne soit pas chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données visés par la présente loi ;

~~e)~~ **5°** veille à ce que le personnel chargé des missions qui lui sont conférées par la présente loi n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui lui sont conférés par la présente loi ou s'il y a incompatibilité, de fait ou de droit, avec l'exercice des tâches qui lui sont conférées en application de la présente loi.

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

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

Art. 7. Point d'information unique

(~~2~~ **1**) Le point d'information unique a pour missions :

~~a)~~ **1°** de recevoir les demandes d'accès et de réutilisation de données visées ~~par le~~ au titre VI, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;

~~b)~~ **2°** de rendre disponibles au public toutes les informations pertinentes concernant l'application des articles 5 et 6 du règlement (UE) 2022/868 ainsi que toute autre information dont la publication est sollicitée par l'Autorité des données ;

~~c)~~ **3°** de mettre à disposition, conformément à l'article 8, paragraphe 2, du règlement (UE) 2022/868, par voie électronique une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données conformément au titre VI, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

(~~3~~ **2**) Pour les cas visés au titre V, le point d'information unique a pour mission :

~~a)~~ **1°** de recevoir les demandes de traitement ultérieur de données à caractère personnel visées par le titre V, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;

~~b)~~ **2°** de mettre à disposition par voie électronique la liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles en vue de leur traitement ultérieur, visée à l'article 18, paragraphe 3 ;

~~c)~~ **3°** de rendre disponibles au public toutes les informations dont la publication est demandée par l'Autorité des données.

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

(1) Il est institué, sous l'autorité du ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions, un Conseil consultatif de la

valorisation des données dans un environnement de confiance, **dénommé** ci-après ~~**désigné par le terme**~~ « Conseil consultatif ».

(2) Le Conseil consultatif a pour mission :

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

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

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

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

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

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

Art. 9. Obligation du « *once only* »

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

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

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

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

~~**a)**~~ **1°** d'assurer la mise à disposition d'informations et de données à caractère personnel aux entités publiques pour l'exécution de leurs obligations et de leurs missions d'intérêt public ;

~~**b)**~~ **2°** d'alléger la charge administrative des administrés dans le cadre de leurs demandes et déclarations ;

~~**c)**~~ **3°** d'éviter aux entités publiques de devoir organiser elles-mêmes la collecte d'informations et de données à caractère personnel auprès des administrés.

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

(1) Lorsque les informations ou données à caractère personnel nécessaires pour traiter la demande présentée par l'administré ou la déclaration présentée par celui-ci doivent être obtenues auprès d'une autre entité publique, dans les conditions prévues aux articles 11 et 12, l'administré ou son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial certifie l'exactitude des informations et des données à caractère personnel ainsi obtenues.

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

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

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

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

L'obligation prévue à l'alinéa ~~**qui précède**~~ **1er** s'applique également dans les cas où l'entité publique se procure des informations ou des données à caractère personnel auprès d'autres entités publiques pour informer les administrés sur leurs droits au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

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

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

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

~~**a)**~~ **1°** les entités publiques ne sont pas tenues de procéder à l'échange d'informations et de données à caractère personnel visé à l'article 9 ; ~~**et**~~

~~b)~~ **2°** l'administré les communique à l'entité publique chargée du traitement de la demande ou de la déclaration.

Dans les cas visés à l'alinéa ~~**qui précède**~~ **1er**, l'entité publique chargée du traitement de la demande ou de la déclaration et l'entité publique détentrice des informations et données à caractère personnel remédient dans les meilleurs délais à l'impossibilité d'échanger les informations et les données à caractère personnel en question.

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

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

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

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

~~a)~~ **1°** dans le cadre du traitement effectué dans l'exercice de leurs missions des demandes et déclarations présentées par un administré ;

~~b)~~ **2°** pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

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

Dans un délai d'un mois à partir de la notification visée à l'alinéa ~~**qui précède**~~ **1er**, les entités publiques notifiées :

~~a)~~ **1°** certifient la disponibilité des informations et des données à caractère personnel à l'entité publique demanderesse et confirment que l'échange d'informations et de données à caractère personnel n'est pas impossible ; ou

~~b)~~ **2°** informent l'entité publique demanderesse du fait qu'elles ne détiennent pas les informations et les données à caractère personnel sollicitées ou que l'échange d'informations et de données à caractère personnel est impossible.

Une copie de l'information visée ~~**aux points a) et b) du présent paragraphe**~~ **à l'alinéa 2, points 1° et 2°,** est transmise au ministre ayant la digitalisation dans ses attributions.

(3) Dans les cas visés au ~~**point a) du paragraphe qui précède**~~ **au paragraphe 2, alinéa 2, point 2°**, les entités publiques concluent dans les meilleurs délais, et au plus tard après trois mois, le protocole visé à l'article 13.

Art. 13. Protocole « *once only* »

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

Le protocole contient, au moins, les éléments suivants :

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

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

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

4° une description détaillée des catégories de personnes concernées ;

5° une description détaillée des finalités du traitement ;

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

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

(2) Tout changement des éléments liés à l'obtention des informations et des données à caractère personnel auprès d'une entité publique doit être formalisé par avenant du protocole visé au paragraphe **~~qui précède~~** **1er**.

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

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

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

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

(2) En vue d'identifier des sources authentiques d'informations et de données à caractère personnel disponibles au sein des entités publiques, le ministre ayant la digitalisation dans ses attributions dispose d'un accès direct au registre des protocoles visés au **~~paragraphe qui précède~~** **1er**.

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

Section I – Dispositions générales

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

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

1° les conditions énoncées au présent titre sont remplies ;

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

a) l'analyse statistique ;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section I – Dispositions générales

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

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

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

2° de secret statistique ;

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

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

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

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

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

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

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

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

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

a) l'analyse statistique ;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) a marqué son accord de principe à la mise à disposition des données à caractère personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en inscrivant

les données disponibles sur la liste des ressources consultable tenue par le point d'information unique conformément à l'article 8, paragraphe 2, du règlement (UE) 2022/868 ; ou

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

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

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

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

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

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

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

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

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

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

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

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

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

a) a marqué son accord de principe à la mise à disposition des données à caractère non personnel aux fins d'accès et de réutilisation par les réutilisateurs de données en inscrivant

les données disponibles sur la liste des ressources consultables tenue par le point d'information unique conformément à l'article 8, paragraphe 2, du règlement (UE) 2022/868 ; ou

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

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

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

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

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

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

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

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

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

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

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

Section I – Dispositions générales

Art. 25. Champ d'application

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

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

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

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

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

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

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

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

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

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

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

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

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

7° la durée du traitement de données à caractère personnel envisagée dans l'environnement de traitement sécurisé visé à l'article 36 et, le cas échéant, la durée de conservation des données dans le système d'archivage intermédiaire du Centre, ainsi que la justification pour laquelle ces durées sont limitées à ce qui est nécessaire ;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

~~**a)**~~ **1°** certifient l'exactitude des informations contenues dans la demande et les pièces jointes visées au présent article ;

~~**b)**~~ **2°** certifient que le plan de confidentialité correspond aux informations contenues dans la demande présentée à l'Autorité des données ;

~~**c)**~~ **3°** s'engagent formellement à respecter les termes de l'autorisation de l'Autorité des données et du plan de confidentialité.

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

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

1° les coordonnées des réutilisateurs des données ;

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

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

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

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

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

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

8° les destinataires de données ;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(5) Les réutilisateurs de données :

~~a)~~ 1° certifient l'exactitude des informations contenues dans la demande et les pièces jointes visées au présent article ;

~~b)~~ 2° certifient que le plan de confidentialité correspond aux informations contenues dans la demande présentée à l'Autorité des données ;

~~c)~~ 3° s'engagent formellement à respecter les termes de l'autorisation de l'Autorité des données et du plan de confidentialité.

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

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

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

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

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

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

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

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

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

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

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

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

Art. 30. Redevances

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

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

Art. 31. Autorisation par l'Autorité des données

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

~~a)~~ **1°** la demande visée à l'article 27 est complète et accompagnée de toutes les pièces visées à l'article 27, paragraphe 2 ;

~~b)~~ **2°** l'entité publique détentrice des données à caractère personnel a donné son accord écrit spécifique au traitement ultérieur de données à caractère personnel, y compris au partage et à la mise à disposition, en contresignant la demande visée à l'article 27 ;

~~c)~~ **3°** le traitement ultérieur de données à caractère personnel est exclusivement effectué pour une ou plusieurs finalités visées à l'article 15, paragraphe 1er, point 2 ;

~~d)~~ **4°** le traitement ultérieur de données à caractère personnel ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(4) Toute modification substantielle du traitement ultérieur de données à caractère personnel visé au titre V ou de l'accès et de la réutilisation des données visés au titre VI couverts par une autorisation de l'Autorité des données conformément au présent article, doit faire l'objet d'une nouvelle demande et d'une nouvelle autorisation par l'Autorité des données, conformément aux dispositions des articles 27 à 31.

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

La demande de modification visée au présent paragraphe contient :

1° dans le cas visé au titre V :

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

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

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

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

2° dans le cas visé au titre VI :

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

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

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

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

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

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

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

Art. 32. Contrôle par l'Autorité des données

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

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

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

Section IV – Publicité par l'Autorité des données

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

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

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

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

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

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

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

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

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

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

Art. 35. Mesures appropriées

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

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

raisonnablement susceptibles d'être utilisés pour réaliser la réidentification ou pour compromettre la confidentialité des informations.

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

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

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

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

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

~~a)~~ **1°** pour les cas visés au titre V, les entités publiques effectuant le traitement ultérieur de données à caractère personnel et les entités publiques détenant les données à caractère personnel ;

~~b)~~ **2°** pour les cas visés au titre VI, les réutilisateurs de données et les organismes du secteur public détenant les données.

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

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

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

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

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

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

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

~~a)~~ **1°** le Centre, ou le tiers de confiance mandaté par le Centre, s'assure de la mise en œuvre les mesures visées au présent article conformément aux stipulations du plan de confidentialité ;

~~b)~~ **2°** le Centre :

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

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

Art. 36. Environnement de traitement sécurisé

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

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

~~a)~~ **1°** restreindre aux personnes physiques autorisées indiquées dans l'autorisation correspondante visée à l'article 31 l'accès à l'environnement de traitement sécurisé ;

~~b)~~ **2°** réduire au minimum le risque de lecture, de copie, de modification ou de suppression non autorisées des données hébergées dans l'environnement de traitement sécurisé par des mesures techniques et organisationnelles de pointe ;

~~c)~~ **3°** restreindre à un nombre limité d'individus identifiables autorisés l'introduction de données et l'inspection, la modification ou la suppression de données hébergées dans l'environnement de traitement sécurisé ;

~~d)~~ **4°** veiller à ce que les personnes visées au point a) n'aient accès qu'aux données couvertes par leur autorisation correspondante visée à l'article 31, au moyen d'identifiants individuelles et uniques et de modes d'accès confidentiels uniquement ;

~~e)~~ **5°** tenir des registres identifiables de l'accès à l'environnement de traitement sécurisé et des activités qui y sont menées pendant la période nécessaire pour vérifier et contrôler toutes les opérations de traitement dans cet environnement. Les registres d'accès devraient être conservés pendant au moins un an ;

~~f)~~ **6°** veiller à la conformité et contrôler les mesures de sécurité énumérées au présent article afin d'atténuer les menaces potentielles pour la sécurité.

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

~~a)~~ **1°** de reproduire les données à l'extérieur de l'environnement et ainsi de les réutiliser dans un autre contexte ou pour des finalités autres qu'autorisées ;

~~b)~~ **2°** d'introduire des solutions technologiques, y compris d'intelligence artificielle, à moins qu'elles aient expressément été inclues dans le plan de confidentialité, ou préalablement été évaluées et certifiées par le Centre, ou par le tiers de confiance mandaté par le Centre, comme ne présentant aucun risque d'atteinte aux exigences visées à l'article 35, paragraphe 1er ;

~~c)~~ **3°** d'introduire des données, à moins que cette introduction ait expressément été demandée conformément à l'article 27, paragraphe 1, point 10°, et à l'article 28, paragraphe 1, point 8°, et autorisée par l'Autorité des données conformément aux dispositions du présent titre ;

~~d)~~ **4°** d'extraire les données de l'environnement de traitement sécurisé, à moins qu'elles aient préalablement été anonymisées.

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

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

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

~~a)~~ **1°** créer un environnement de traitement sécurisé commun, ensemble avec des organismes compétents désignés conformément à l'article 7 du règlement (UE) 2022/868, afin de mettre les données à disposition des entités publiques ou des réutilisateurs de données ;

~~b)~~ **2°** combiner et traiter les données visées au titre VI avec des données provenant d'environnements de traitement sécurisés d'autres États membres gérés par des organismes compétents désignés conformément à l'article 7 du règlement (UE) 2022/868 afin de les mettre à disposition des réutilisateurs de données.

Art. 37. Responsabilité du traitement

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

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

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

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

Section VI – Recours

Art. 38. Recours

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

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

Section I – Services d'intermédiation de données

Art. ~~41~~ 39. Procédure

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

Art. ~~42~~ 40. Redevances

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

Art. ~~43~~ 41. Sanctions

(1) Dans le cadre d'une violation de l'obligation de notification incombant aux prestataires de services d'intermédiation de données en vertu de l'article 11 du règlement (UE) 2022/868 ou des conditions liées à la fourniture de services d'intermédiation de données en vertu de l'article 12 du règlement (UE) 2022/868, la CNPD peut, par voie de décision, imposer des amendes administratives à hauteur de 500 à 100~~.~~ 000 euros aux prestataires de services d'intermédiation de données.

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

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

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

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

Section ~~III~~ II – Recours

Art. ~~46~~ 42. Recours

Un recours contre les décisions de la CNPD prises en application des **~~sections I et II~~ ~~du présent titre~~ chapitres III et IV du Règlement 2022/686** est ouvert devant le Tribunal administratif qui statue comme juge du fond.

TITRE IX – Dispositions finales

Art. ~~47~~ 43. Intitulé de citation

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

20250516_Avis

N° 8395[8]
N° 8395A[2]
N° 8395B[2]

CHAMBRE DES DEPUTES

PROJET DE LOI

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

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

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

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

PROJET DE LOI

relative à la désignation des organismes et autorités compétents et au point d'information uniquement prévus aux articles 7, 8, 13 et 23 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)

PROJET DE LOI

relative à

1° la valorisation des données dans un environnement de confiance ;

2° la mise en oeuvre du principe « once only » ;

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

4° la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil

du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

* * *

AVIS DU SYNDICAT DES VILLES ET COMMUNES LUXEMBOURGEOISES

(31.3.2025)

I. REMARQUES GENERALES

Le SYVICOL a été demandé en son avis par Madame la Ministre de la Digitalisation au sujet du projet de loi sous examen en date du 12 juin 2024. Le syndicat a également été invité à une présentation des grandes lignes du projet de loi au ministère de la Digitalisation en date du 29 novembre 2024 et il souhaite profiter de l'occasion pour remercier Madame la Ministre pour ces démarches.

Le présent avis a été élaboré à l'aide de la commission consultative 1 – volet administratif du SYVICOL. Le SYVICOL tient à remercier les membres de la commission pour leurs contributions importantes.

Le projet de loi n°8395 relatif à la valorisation des données dans un environnement de confiance précise au niveau national luxembourgeois les règles pour l'accès aux données détenues par les entités du secteur public ainsi que les règles concernant la réutilisation de ces données contenues dans le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).

Tout comme le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022, le projet de loi n°8395, qui reprend les dispositions de fond du règlement européen, vise à instaurer une certaine confiance entre les citoyens et les acteurs du secteur public, qui détiennent une panoplie de données à caractère personnel et à caractère non personnel de leurs administrés.

Il complète et précise pour le Luxembourg les dispositions contenues dans le règlement (UE) 2022/868, qui est d'application directe depuis le 24 septembre 2023, concernant en particulier la désignation des organismes compétents au niveau national, la procédure à suivre pour l'octroi des autorisations d'accès et de réutilisation des données, et les conditions applicables à l'accès et à la réutilisation des données.

Les principaux objectifs du projet de loi sont la simplification administrative pour le citoyen, pour les entreprises et pour les administrations publiques ; la valorisation des données détenues par le secteur public pour promouvoir l'économie, la recherche et l'innovation fondées sur les données ; l'habilitation des administrations à proposer des démarches de manière proactive aux citoyens et la facilitation de la prise de décision éclairée basée sur les données, le tout dans un environnement de confiance entre les citoyens et les détenteurs des données du secteur public.

Les dispositions du projet de loi peuvent être divisées en quatre grands piliers, à savoir le traitement primaire de données à caractère personnel (Titre II), le principe du « once only » (Titre IV), les traitements ultérieurs de données personnelles (Titres V et VII) et la réutilisation de données personnelles (Titres VI et VII).

Tandis que le SYVICOL ne veut pas remettre en cause les grands principes du projet de loi ou l'introduction du système « once only », il souhaite néanmoins faire part de ses réflexions ci-dessous concernant surtout la mise en œuvre pratique du texte.

*

II. ELEMENTS-CLES DE L'AVIS

- Le SYVICOL se demande si une commune spécifique ou le Syndicat intercommunal de gestion informatique (SIGI) pourra être désigné « tiers de confiance » au sens de la loi en projet. Dans la négative, il préconise de prévoir cette possibilité. (art. 6)
- Il salue la désignation d'une autorité centrale et l'introduction d'un « point d'information unique » pour le traitement ultérieur et l'accès, ainsi que la réutilisation des données à caractère personnel. ». (art. 7)
- Il note que les membres du conseil consultatif de la valorisation des données dans un environnement de confiance sont uniquement des représentants issus des ministères et administrations de l'État. Il demande que le niveau communal soit représenté par au moins deux membres dans cet organe consultatif. (art. 8)
- De l'avis du syndicat, il ne ressort pas clairement de la formulation actuelle du texte que les communes ne sont pas obligées à informer les administrés qu'ils ont droit à une éventuelle prestation ou un avantage supplémentaire auprès de leur commune de résidence après avoir fait une demande auprès d'une entité étatique. Il recommande de clarifier cette disposition dans le texte du projet de loi. (art. 9)
- Le SYVICOL n'est pas convaincu qu'on puisse parler d'une simplification administrative et d'un gain de temps tels qu'avancés par les auteurs du texte, surtout en relation avec le principe du « once only » et plus spécifiquement dans le contexte de la notification d'un administré relative au droit au bénéfice éventuel d'une prestation ou d'un avantage supplémentaire. Contrairement aux administrés, cette disposition entraînera un surplus de démarches à effectuer par les communes et donc une augmentation de leur charge de travail et une hausse des coûts y afférents. (art. 9 et 11)
- D'une manière plus générale, le SYVICOL demande aux auteurs de clarifier les dispositions sur le principe « once only » afin de préciser les responsabilités et obligations exactes des communes dans la mise en œuvre de ce principe. (art. 9 à 11)
- Il propose de simplifier la tâche de recensement pour les 100 communes, pour les 30 offices sociaux et les autres établissements publics placés sous la surveillance des communes en instituant un groupe de travail composé d'experts du ministère et du niveau communal pour identifier les données à caractère personnel et les informations pour lesquelles les communes devront signer un « protocole once only ». (art.12 et 13)
- Il propose de mettre à disposition des communes des protocoles types pour les échanges qui seront identiques dans les 100 communes du pays ou même d'élaborer des protocoles uniques pour chaque type d'échange de données qui est identique dans le secteur communal. (art.12 et 13)
- De l'avis du syndicat, la complexité des procédures relatives au traitement ultérieur des données à caractère personnel et à l'accès et à la réutilisation des données à caractère personnel ne reflètent pas l'affirmation des auteurs qu'il sera « superflu de recruter un spécialiste disposant des connaissances et de l'expérience pratique auprès de chacune des plus d'une centaine d'entités étatiques, de chacune des plus d'une centaine de communes luxembourgeoises » et que les communes seront, bien au contraire, quasi obligées à engager un spécialiste dans la matière ou de travailler avec un expert externe. (art.15 à 18 et 25 à 38)
- Enfin, le SYVICOL plaide pour l'application rigoureuse du principe de connexité ancré à l'article 123, paragraphe 3 de la Constitution, puisque les nouvelles missions pour les communes contenues dans le projet de loi exigent un grand investissement en termes de finances, de temps et de ressources de la part des communes. (art.15 à 18 et 25 à 38)

*

III. REMARQUES ARTICLE PAR ARTICLE

Titre I^er^ et II – articles 1^er^, 2 et 3

Les articles 1^er^ et 2 énoncent l'objet de la loi en projet ainsi que les définitions de certains termes utilisés dans le texte de la future loi. Les dispositions du projet de loi s'appliquent sans préjudice des dispositions plus spécifiques relatives au traitement de données à caractère personnel, comme celles prévues par exemple dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Les dispositions du projet de loi s'appliquent aux entités publiques, à savoir : les ministères et leurs services, les administrations et les communes, les établissements publics, les groupements d'intérêt économique, les personnes morales d'utilité publique. Le SYVICOL a été informé lors de la réunion avec le ministère de la Digitalisation que la définition d'entité publique n'inclut pas les autres établissements publics placés sous la surveillance des communes, comme les offices sociaux par exemple. Cependant, de l'avis du SYVICOL, l'application du principe « once only » serait certainement utile dans ces entités publiques.

L'article 3 introduit une base légale générale pour le traitement de données à caractère personnel par les entités publiques, la base de licéité générale du traitement de données à caractère personnel se fondant dans le cadre de la future loi sur la condition que les données soient traitées par les entités publiques dans l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont les entités publiques sont investies : « Les entités publiques sont habilitées à traiter les données à caractère personnel nécessaires aux fins relevant de l'exécution de leurs missions d'intérêt public ou relevant de l'exercice de l'autorité publique dont elles sont investies par une disposition de droit de l'Union européenne ou de droit national applicable.»

Titre III – articles 4 à 8

Le titre III du projet de loi définit les acteurs compétents en matière de traitement de données à caractère personnel, ainsi qu'en matière d'accès et de réutilisation de données tel qu'exigé par le règlement (UE) 2022/868.

Le Commissariat du gouvernement à la protection des données auprès de l'État est désigné comme organe centralisé compétent habilité à octroyer ou à refuser les accès et les réutilisations des données, le Commissariat est donc désigné « Autorité des données » au sens du règlement européen.

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

L'autorité des données sera soutenue au niveau technique et dans ses décisions par le Centre des technologies de l'information de l'État (Centre) ainsi que par le groupement d'intérêts économiques Plateforme nationale d'échange de données (LNDS) ainsi que par des « tiers de confiance » (article 6) et le Conseil consultatif de la valorisation des données dans un environnement de confiance (article 8).

Les « tiers de confiance » aideront l'autorité des données, le Centre et le LNDS à « effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données ».

Pour l'accès aux données, un « point d'information unique » est créé sous l'autorité du ministre ayant la digitalisation dans ses attributions. Le point d'information unique recevra, entre autres, les demandes d'accès et de réutilisation de données, les transmettra électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et mettra une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données à disposition du grand public.

Le SYVICOL salue la désignation d'une autorité centrale et l'introduction d'un point d'information unique pour l'accès aux données et pour la réutilisation de données. Il se demande cependant si une commune particulière ou le Syndicat intercommunal de gestion informatique (SIGI) pourra être désigné « tiers de confiance ».

Le Centre, donc le CTIE, a uniquement pour mission de « s'assurer de la mise en oeuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou de modification, d'agrégation, de suppression et de traitement des informations et données selon toute autre méthode de contrôle de la divulgation des données conformément au plan de confidentialité, préalablement à la mise à disposition des données dans l'environnement de traitement sécurisé ». D'après la lecture du texte faite par le SYVICOL, dans la pratique, il incombera donc également aux communes d'anonymiser et de pseudonymiser les données à caractère personnel avant leur introduction dans l'environnement de traitement sécurisé.

Le SIGI s'occupe de la gestion informatique pour 99 des 100 communes du pays et devra constituer un acteur incontournable pour aider les communes à mettre en œuvre les dispositions du projet de loi n°8395. Mais étant donné que la Ville de Luxembourg n'est pas membre du syndicat intercommunal, il est nécessaire, selon l'avis du SYVICOL, de prévoir la possibilité de désigner une commune spécifique ainsi que le syndicat intercommunal en tant que « tiers de confiance ».

Quant au Conseil consultatif de la valorisation des données dans un environnement de confiance, le SYVICOL note que les membres dudit conseil sont des représentants issus des ministères et administrations de l'État. Cet organe n'inclurait donc pas de représentants provenant des communes ou du SYVICOL, un fait qui est regrettable.

Puisque les 100 communes du pays sont des détenteurs d'un grand nombre de données à caractère personnel ou non personnel de leurs administrés et puisqu'elles joueront un rôle important dans l'application du principe du « once only » introduit au titre IV ainsi que dans la mise à disposition des données pour la réutilisation ultérieure, le SYVICOL est d'avis que les communes devraient avoir au moins deux représentants au sein du Conseil consultatif de la valorisation des données dans un environnement de confiance, à nommer ou bien par le SYVICOL ou par le SIGI et la Ville de Luxembourg, tel qu'il est d'ores et déjà le cas pour la Commission du registre national instaurée par la loi du 19 juin 2013 relative à l'identification des personnes physiques, pour laquelle le SYVICOL est habilité à nommer un membre titulaire et un membre suppléant.

Titre IV – articles 9 à 14

L'article 9 introduit le principe du « once only » pour les informations et données à caractère personnel obtenues par les entités publiques auprès d'une autre entité publique. Ce principe comprend la règle générale qu'un « administré présentant une demande ou produisant une déclaration à une entité publique ne peut être tenu de produire des informations ou des données à caractère personnel que celle-ci détient déjà ou qu'elle peut obtenir auprès d'une autre entité publique conformément à l'article 11. » Cette manière de procéder est obligatoire pour toutes les entités publiques.

L'article 9, paragraphe 2, alinéa 2 dispose : « Elles (les entités publiques) échangent entre elles les informations ou les données à caractère personnel nécessaires pour pouvoir informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages. »

Cette situation se présente régulièrement dans les administrations communales, par exemple, si un administré a fait une demande pour une subvention en matière d'énergie auprès de l'Etat, disons pour l'installation de panneaux photovoltaïques, et si une commune offre une subvention pour le même type d'installation fixée à un certain pourcentage du subside de l'Etat sous condition que la subvention étatique ait déjà été accordée à l'administré.

Lors de la réunion du 29 novembre 2024 entre le SYVICOL et les services compétents du ministère de la Digitalisation, il a été expliqué que cette disposition n'est pas obligatoire. De l'avis du syndicat, la formulation actuelle du paragraphe en question ne reflète cependant pas cette subtile différence. Il ne ressort pas clairement de la formulation actuelle du texte que les communes ne sont pas obligées à informer les administrés qu'ils ont droit à une éventuelle prestation supplémentaire auprès de leur commune de résidence après avoir fait une demande auprès d'une entité étatique, surtout si on lit l'article 9, paragraphe 2, alinéa 2 en conjonction avec l'article 11, paragraphe 2, alinéa 2 et l'article 12, paragraphe 1er, lettre b).

Vu ce qui précède, il sera difficile pour les communes de déterminer exactement quelles seront leurs responsabilités et obligations pour l'application du principe « once only ». Dès lors, le SYVICOL demande au gouvernement de clarifier la disposition en question afin d'éviter toute source de confusion et d'insécurité juridique.

L'article 10 place la responsabilité de vérifier l'exactitude des données échangées entre les entités publiques fermement entre les mains de l'administré, son curateur ou son administrateur légal, son administrateur ad hoc ou son mandataire spécial.

D'abord, le SYVICOL note qu'aucune disposition du projet de loi n'explique comment cette vérification sera effectuée. Est-ce que les administrés seront simplement tenus de cocher une case dans un système numérique ?

Dans ce cas, quid des administrés en situation d'illectronisme ? Même de nos jours, un nombre non négligeable de citoyens sont frappés par la fracture numérique, c'est-à-dire par les inégalités dans l'accès aux technologies de l'information et de la communication. Cette fracture peut se présenter à au moins deux niveaux : le niveau de l'accès et le niveau de l'usage.

Surtout au vu de l'affirmation des auteurs du projet de loi dans l'exposé des motifs de vouloir réduire tout particulièrement cette fracture numérique, la vérification devra donc rester possible sous forme de papier : « Afin que l'économie et la recherche fondées sur les données soient inclusives à l'égard de tous les citoyens, il faut veiller tout particulièrement à réduire la fracture numérique et à promouvoir une expertise de pointe nationale dans le secteur des technologies. L'économie des données doit être construite de manière à permettre aux entreprises de prospérer, en garantissant la neutralité de l'accès aux données ainsi que la portabilité et l'interopérabilité des données, et en évitant les effets de verrouillage. »

Ensuite, au cas où les données s'avèrent inexactes, l'administré est tenu de demander une rectification auprès de l'entité publique dont elles proviennent et communiquer la correction à l'entité publique qui traite les données. Le SYVICOL se demande comment les auteurs du texte visent à s'assurer que l'administré soit en mesure d'identifier l'entité publique originaire des données afin de pouvoir demander une rectification ? De l'avis du syndicat, il est en fait non réaliste que tous les administrés sachent quelles entités publiques détiennent quelles données à caractère personnel sur leur personne.

En plus, il se demande si cette manière de procéder n'est pas tout à fait contraire au principe du « once only », un élément clé du projet de loi, vu que l'administré est tenu de communiquer la rectification de ses données à l'entité publique dont elles proviennent et à l'entité publique en charge du traitement. Ne serait-il pas suffisant pour l'administré de communiquer la rectification à l'entité originaire, puisque les entités publiques sont de toute façon soumises à l'obligation d'échanger ces dernières entre elles ?

Puisque le texte du projet de loi reste muet sur les modalités techniques concernant l'échange d'informations pour la vérification de l'exactitude et, le cas échéant, la rectification des données personnelles de l'administré, le SYVICOL part de l'hypothèse que ces démarches seront d'une manière ou d'une autre intégrées dans l'espace individuel « My Guichet » des administrés. Dans cette hypothèse, il est concevable que l'espace personnel de l'administré puisse afficher les entités publiques détentrices des informations et données personnelles, et que l'administré puisse simplement cocher une case pour la vérification de ses données personnelles, demander la rectification de ces dernières et même donner son consentement, le cas échéant quasi généralisé, pour la transmission de ses données à une autre entité publique pour pouvoir bénéficier d'une prestation ou d'un avantage supplémentaire.

L'article 11 explique les conditions applicables au « once only », notamment que « l'entité publique chargée de traiter la demande ou la déclaration fait connaître à l'administré les informations ou données à caractère personnel nécessaires au traitement de la demande ou de la déclaration qu'elle se procure auprès d'autres entités publiques. L'information contient, pour chaque catégorie d'informations et de données à caractère personnel, les coordonnées des entités publiques d'où proviennent les informations […]. »

Dans le cas de figure où un administré aurait droit au bénéfice éventuel d'une prestation ou d'un avantage supplémentaire et se trouverait en situation d'illectronisme, une commune qui souhaiterait faire bénéficier ledit administré de prestations ou d'avantages additionnels devrait d'abord informer ce dernier par lettre recommandée (afin de s'assurer que l'administré reçoive le courriel) qu'il a droit à des aides supplémentaires, puis de quelles données la commune aurait besoin pour traiter le dossier et de quelle(s) entité(s) publique(s) les données ou informations proviendraient, lui demander s'il désire rectifier des données nécessaires et enfin demander à l'administré concerné s'il est d'accord avec le

traitement de ses données pour cette démarche administrative ou s'il veut s'opposer au traitement et par conséquent probablement renoncer à une aide supplémentaire.

Dans ce contexte, on peut se demander si on peut toujours parler d'une simplification administrative et d'un gain de temps, comme avancé par les auteurs du texte dans l'exposé des motifs ? Ceci vaut avant tout pour les administrations communales, pour lesquelles, contrairement aux administrés, ces obligations entraîneront un surplus de démarches à effectuer et donc une augmentation de leur charge administrative et une hausse des coûts y afférents au lieu d'une simplification administrative et d'une réduction des dépenses et du temps de travail.

Afin de pouvoir exécuter les procédures « once only », les entités publiques « sont tenues d'identifier, dans les meilleurs délais, les informations et données à caractère personnel qu'elles peuvent obtenir auprès d'une autre entité publique […] et de notifier, sans délai, les échanges d'informations et de données à caractère personnel identifiées conformément […] aux entités publiques auprès desquelles les informations et données à caractère personnel pourraient être obtenues. » Dans un délai d'un mois à partir de la notification visée, les entités publiques notifiées certifient la disponibilité ou non des informations et des données en question et renseignent l'entité publique demanderesse si ces dernières sont communicables dans un format adéquat. (article 12)

Si les informations et données sont disponibles et techniquement communicables, les entités publiques concluent dans les meilleurs délais, et au plus tard après trois mois, un « protocole once only » (article 13).

Chaque commune devra donc identifier toutes les données à caractère personnel et toutes les informations qu'un ministère ou une administration détient et dont elle aura besoin pour traiter les demandes et les déclarations des administrés et, le cas échéant, pour communiquer à l'administré qu'il a droit à des prestations ou à un avantage supplémentaire, et ceci dans les meilleurs délais.

D'abord, le SYVICOL se demande, vu l'ampleur de la tâche, quel délai exact les auteurs du texte ont envisagé en employant les termes « meilleurs délais » ? Il serait utile de préciser cette disposition afin d'offrir plus de prévisibilité aux administrations communales dans la mise en œuvre du projet de loi sous examen.

Ensuite, puisqu'un grand nombre de démarches sont identiques dans chaque commune du pays, le SYVICOL propose de simplifier cette tâche de recensement pour les 100 communes, et même pour les 30 offices sociaux et les autres établissements publics placés sous la surveillance des communes, en instituant un groupe de travail composé d'experts du ministère de la Digitalisation et du niveau communal pour identifier et recenser les données à caractère personnel et les informations pour lesquelles les communes devront signer un « protocole once only ».

Dans le même ordre d'idées, il se demande s'il serait possible de mettre à disposition des communes des protocoles types pour les échanges qui seront identiques dans chacune des 100 communes du pays ou même d'élaborer des protocoles uniques pour chaque type d'échange de données avec le secteur communal. A titre d'exemple, on peut citer les autorisations à bâtir pour lesquelles les administrés ont besoin d'un extrait cadastral de la parcelle sur laquelle ils planifient leurs travaux.

Pour traiter une telle demande, les communes ont donc besoin du même type de document et du même type d'échange provenant de l'Administration du cadastre et de la topographie (ACT). Ainsi, au lieu de faire signer un « protocole once only » entre l'ACT et les 100 communes individuellement, une vraie simplification administrative, de l'avis du SYVICOL, consisterait en un « protocole once only » entre l'ACT et toutes les communes pour le type d'échange de la transmission de l'extrait du plan cadastral dans le cadre d'une autorisation à bâtir.

Titre V et VII – articles 15 à 18 et 25 à 38

Le Titre V définit le cadre du traitement ultérieur de données à caractère personnel par les entités publiques. Le traitement ultérieur est uniquement possible sous les conditions et pour les finalités énoncées aux articles 15 et 16.

Une entité publique est autorisée à traiter ultérieurement les données à caractère personnel qu'elle détient, le cas échéant après anonymisation ou pseudonymisation (article 17).

Si une entité publique souhaite traiter ultérieurement des données à caractère personnel détenues par une autre entité publique, l'entité détentrice doit marquer son accord de principe pour le traitement ultérieur en inscrivant les données sur la liste des ressources consultables auprès du point d'information

unique et, dans un deuxième temps, en marquant son accord spécifique au traitement ultérieur en contresignant la demande de traitement ultérieur de données à caractère personnel par l'entité publique demanderesse. (article 18)

Le SYVICOL se demande quel organe de la commune sera responsable pour prononcer l'accord de principe et pour donner l'accord spécifique pour le traitement ultérieur des données à caractère personnel. Il propose donc de clarifier cette disposition pour les communes.

En cas de refus par l'entité publique qui détient les données, le Conseil consultatif peut être saisi par la partie demanderesse et émet un avis endéans 3 semaines. La décision finale réside cependant toujours avec l'entité détentrice des données.

Le Titre VII définit les modalités applicables au traitement ultérieur des données à caractère personnel par les entités publiques et à l'accès et à la réutilisation de données par des réutilisateurs de données qui sont soumis à autorisation de l'Autorité des données. (article 25) Toute demande doit être introduite sous forme écrite et de manière précise. (article 26)

Avant chaque traitement ultérieur de données à caractère personnel, des mesures effectives et efficaces d'anonymisation et/ou de pseudonymisation doivent être mises en place et une évaluation spécifique des méthodes et des modalités de mise en oeuvre de ces mesures doit être effectuée et enregistrée dans un plan de confidentialité par l'entité publique qui vise à effectuer le traitement ultérieur des données. Ce plan de confidentialité est uniquement validé au moment où il est signé par le Centre ou par le tiers de confiance mandaté par le Centre et par l'entité publique effectuant le traitement ultérieur de données à caractère personnel.

Dans le cas de figure d'une demande d'accès et de réutilisation des données par un réutilisateur, le plan de confidentialité doit être signé par l'entité publique détentrice des données et par le réutilisateur. Le plan de confidentialité est ensuite transmis au Centre ou à un tiers de confiance mandaté par le Centre, qui certifie alors l'effectivité et l'efficacité des mesures en apposant sa signature.

L'attestation du Centre est jointe à la demande de traitement ultérieur ou à la demande d'accès et de réutilisation selon le cas de figure qui se présente, après quoi les données sont mises à disposition dans l'environnement de traitement sécurisé par le Centre. (article 35)

En lisant les paragraphes précédents, on peut vraiment se demander si une commune ne sera pas obligée d'engager un expert en matière de réutilisation et de traitement ultérieur de données. Il est bien sûr tout à fait compréhensible que les données à caractère personnel de nos citoyens doivent être protégées de manière adéquate et que nous ne pouvons pas traiter ces données à caractère personnel, même ultérieurement, à la légère.

Les procédures décrites ci-dessus sont toutefois si complexes qu'elles ne peuvent pas être mises en œuvre facilement par les communes. L'anonymisation et la pseudonymisation, en particulier, sont des procédures hautement spécialisées qui nécessitent de l'expérience et une formation spécialisée. Les communes seront donc quasi obligées à engager un spécialiste dans la matière ou travailler avec un expert externe.

Partant, tandis que l'exposé des motifs déclare que « en effet, il s'avère excessif de recruter un spécialiste disposant des connaissances et de l'expérience pratique afférente auprès de chacune des plus d'une centaine d'entités étatiques, de chacune des plus d'une centaine de communes luxembourgeoises […] », la complexité du texte et des procédures y comprises ne reflète pas cette affirmation de l'avis du SYVICOL.

Dans ce contexte, il souhaite également renvoyer à l'article 123 de la Constitution, et plus précisément au paragraphe 3 de cet article qui dispose que « les communes ont droit aux ressources financières pour remplir les missions qui leur sont confiées par la loi. » La mise en œuvre du projet de loi n°8395 au niveau communal, notamment le recensement des données, l'application du principe « once only », la rédaction et la gestion des protocoles « once only », la rédaction et la gestion des plans de confidentialité, la gestion des demandes de traitement ultérieur et les demandes d'accès et de réutilisation, peuvent être considérées comme des nouvelles missions pour les communes. Considérant que ces missions exigent un grand investissement en termes de finances, de temps et de ressources de la part des communes, il serait tout à fait justifié que les communes reçoivent des moyens financiers supplémentaires pour exercer ces nouvelles missions.

Adopté unanimement par le comité du SYVICOL, le 31 mars 2025

Impression: CTIE – Division Imprimés et Fournitures de bureau
8395B - Dossier consolidé : 63

20250821_AmendementGouvernemental

N° 8395B[3]

CHAMBRE DES DEPUTES

PROJET DE LOI

relative à

1° la valorisation des données dans un environnement de confiance ;

2° la mise en oeuvre du principe « *once only* » ;

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

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

* * *

AMENDEMENTS GOUVERNEMENTAUX

I. OBSERVATION PRÉLIMINAIRE

La scission des projets de loi n°8395A et n°8395B a été motivée par l'urgence de notifier les différents organismes et autorités compétents prévus au règlement (UE) 2022/868 à la Commission européenne.

Dans le cadre de son examen du projet de loi n°8395A, le Conseil d'État a dans son avis du 3 juin 2025 émis des oppositions formelles auxquelles il n'était pas possible de répondre uniquement en apportant des modifications au projet de loi n°8395A

Les amendements présentés ci-dessous permettent ainsi de répondre à certaines observations du Conseil d'État dans son avis du 3 juin 2025 sur le projet de loi n°8395A.

*

II. AMENDEMENTS

Amendement n°1

Dans l'article 2, paragraphe 2, point 4, les termes « relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868 sont remplacés par les termes « **portant création du Commissariat du Gouvernement à la souveraineté des données** ».

Commentaire

Cet amendement permet de prendre en compte la modification de l'intitulé du projet de loi n°8395A.

Amendement n°2

L'article 8 du projet de loi est modifié comme suit :

1° Le paragraphe 1er, est remplacé pour un nouveau paragraphe 1er qui prend la teneur suivante :

« **(1) Le Conseil consultatif de la valorisation des données dans un environnement de confiance, institué par la loi du […] portant création du Commissariat du Gouvernement à la souveraineté des données, a pour mission de :**

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.»

2° Les paragraphes 2 et 3 sont supprimés.

Commentaire :

Cet amendement vise à modifier le projet de loi n°8395B afin de tenir compte des modifications apportées au projet de loi n°8395A, à savoir l'ajout d'un nouvel article 16, qui institue le Conseil consultatif de la valorisation des données dans un environnement de confiance.

Amendement n°3

L'article 18 du projet de loi est modifié comme suit :

1° Au paragraphe 1er, point 1°, il est inséré les termes « **a marqué son accord par** » après « l'entité publique qui détient les données à caractère personnel ».

2° Au paragraphe 1er, point 1° a), les termes « a marqué son accord de principe au traitement ultérieur, y compris le partage et la mise à disposition en inscrivant les » sont remplacés par les termes « **l'inscription des** ».

3° Au paragraphe 1er, point 1° b), les termes « a marqué son accord spécifique au traitement ultérieur, y compris le partage et la mise à disposition, en contresignant » sont remplacés par les termes « **la contresignature de** ».

4° Au paragraphe 1er, point 3° a), il est inséré les termes «, **après l'accord de l'entité publique qui détient les données à caractère personnel,** » après les termes « l'Autorité des données » et avant les termes « autorise le traitement ultérieur de données à caractère personnel conformément à l'article 31 ».

Commentaire :

Cet amendement permet d'aligner les formulations avec les modifications apportées aux dispositions du projet de loi n°8395A.

Amendement n°4

L'article 20, paragraphe 1er, point 2° est remplacé comme suit :

« **2° l'accès et la réutilisation des données est effectué exclusivement pour une ou plusieurs des finalités visées à l'article 15, paragraphe 3, point 1° loi du […] portant création du Commissariat du Gouvernement à la souveraineté des données.** »

Commentaire :

Cet ajout vise à adapter l'article au regard des modifications apportées au projet de loi n°8395.

Amendement n°5

L'article 22 du projet de loi est modifié comme suit :

1° Au paragraphe 1er, point 3° a), il est inséré les termes «, **après l'accord de l'entité publique qui détient les données à caractère personnel,** » après les termes « l'Autorité des données » et avant les termes « autorise le traitement ultérieur de données à caractère personnel conformément à l'article 31 ».

2° Au paragraphe 1er, point 1°, il est inséré les termes **«, a marqué son accord par** » après « l'organisme du secteur public qui détient les données ».

3° Au paragraphe 1er, point 1° a), les termes « 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 » sont remplacés par les termes « **l'inscription des** ».

4° Au paragraphe 1er, point 1° b), les termes « 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 » sont remplacés par les termes « **la contresignature de** ».

5° Le paragraphe 3 est supprimé.

Commentaire :

Cet amendement permet d'aligner les formulations avec les modifications apportées aux dispositions du projet de loi n°8395A.

Amendement n°6

L'article 23 du projet de loi est modifié comme suit :

1° Au paragraphe 1er, point 1°, il est inséré les termes **«, après l'accord de l'entité publique qui détient les données à caractère personnel,** » après les termes « l'Autorité des données » et avant les termes « autorise le traitement ultérieur de données à caractère personnel conformément à l'article 31 ».

2° Au paragraphe 1er, point 2°, il est inséré les termes « **a marqué son accord par** » après « l'organisme du secteur public qui détient les données ».

3° Au paragraphe 1er, point 2° a), les termes « 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 » sont remplacés par les termes « **l'inscription des** ».

4° Au paragraphe 1er, point 1° b), les termes « 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 » sont remplacés par les termes « **la contresignature de** ».

5° Le paragraphe 2 est supprimé.

Commentaire :

Pour le commentaire, il y a lieu de se référer au commentaire de l'amendement n°2.

Amendement n°7

L'article 31, paragraphe 1er, point 2°, du projet de loi est remplacé comme suit :

« **2° pour les cas visés à l'article 18, paragraphe 3, point 3°, lettre a) :**

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 ;

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

Amendement n°8

La section VI « – Recours » du titre VII et l'article 38 sont supprimés.

Commentaire :

Afin de répondre à l'opposition formelle du Conseil d'État dans son avis du 3 juin 2025, cette disposition a été introduite dans le projet de loi n°8395A.

Amendement n°9

L'article 41 est supprimé.

Commentaire :

Afin de répondre à l'opposition formelle du Conseil d'État dans son avis du 3 juin 2025, cette disposition a été introduite dans le projet de loi n°8395A.

Amendement n°10

La section II « – Recours » du titre VIII et l'article 42 sont supprimés.

Commentaire :

Afin de répondre à l'opposition formelle du Conseil d'État dans son avis du 3 juin 2025, cette disposition a été introduite dans le projet de loi n°8395A.

Amendement n°12

Les numéros des articles 39, 40 et 41 sont modifiées afin de prendre en compte la suppression des articles 38, 41 et 42.

Amendement n°11

Toutes les références à l'« Autorité des données » sont remplacés par les termes « Autorité luxembourgeoise des données ».

Commentaire :

Cet amendement permet de prendre en compte la modification de la désignation de l'Autorité des données apportée au projet de loi n°8395.

*

TEXTE COORDONNE DU PROJET DE LOI N°8395B

PROJET DE LOI

relative à

1° la valorisation des données dans un environnement de confiance ;

2° la mise en œuvre du principe « *once only* » ;

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

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

TITRE I^er^ – Dispositions préliminaires

Art. 1^er^. Objet

(1) La présente loi vise :

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

2° l'échange d'informations et de données à caractère personnel obtenues par une entité publique auprès d'une autre entité publique dans le cadre du traitement d'une demande ou d'une déclaration d'un

administré, ou pour informer l'administré sur ses droits au bénéfice éventuel d'une prestation ou d'un avantage prévu par des dispositions législatives ou réglementaires et pour pouvoir lui attribuer éventuellement lesdits prestations ou avantages ;

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

4° l'accès et la réutilisation de certaines catégories de données collectées par les organismes du secteur public, en application du chapitre II du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), dénommé ci-après « 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) Les termes et expressions définis à l'article 2 du règlement (UE) 2022/868 et à l'article 4 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), dénommé ci-après « règlement (UE) 2016/679 », ont la même signification dans la présente loi.

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

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

2° « Autorité **luxembourgeoise** des données » : le Commissariat du Gouvernement à la protection des données auprès de l'État ;

3° « entité publique » : un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal aux fins d'application des dispositions des titres IV et V. Toutefois, ne sont pas considérées comme entité publique aux fins d'application de la présente loi :

a) la Chambre des Députés ;

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

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

4° « point d'information unique » : le point d'information unique visé à l'article 2 de la loi du […] ~~**relative à la désignation des organismes compétents, autorités compétentes et point d'information unique prévus au règlement (UE) 2022/868**~~ **portant création du Commissariat du Gouvernement à la souveraineté des données** ;

5° « tiers de confiance » : toute entité fonctionnellement indépendante des entités publiques visées au titre V, des organismes du secteur public détenant les données et du réutilisateur de données visés au titre VI, qui remplit les conditions prévues à l'article 6.

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

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

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

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

Art. 4. Autorité luxembourgeoise des données

(1) L'Autorité **luxembourgeoise** des données octroie ou refuse l'accès aux fins de réutilisation des données visées à l'article 3, paragraphe 1er, du règlement (UE) 2022/868 conformément aux dispositions des titres VI et VII.

(2) L'Autorité **luxembourgeoise** 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.

(3) L'Autorité **luxembourgeoise** des données a pour missions :

1° de mettre en œuvre les missions lui conférées par la présente loi ;

2° de collaborer étroitement avec le Centre des technologies de l'information de l'État, désigné ci-après « 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 « LNDS » ;

3° de fonctionner comme organe de réflexion et d'impulsion dans le domaine du traitement ultérieur de données à caractère personnel et de l'accès et de la réutilisation de données et de formuler des avis et des propositions en la matière au ministre ayant la digitalisation dans ses attributions ;

4° de proposer au ministre ayant la digitalisation dans ses attributions des mesures en matière de politique de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données ;

5° de conseiller, sur demande, le ministre ayant la digitalisation dans ses attributions sur les mesures en matière de traitement ultérieur de données à caractère personnel ;

6° de promouvoir les bonnes pratiques à travers les entités publiques, en matière de traitement ultérieur de données à caractère personnel, et à travers les organismes de droit public en matière d'accès et de réutilisation de données ;

7° de sensibiliser les entités publiques, les organismes de droit public et le public en matière de traitement ultérieur de données à caractère personnel et en matière d'accès et de réutilisation de données.

(4) L'Autorité **luxembourgeoise** des données dispose des ressources nécessaires pour exercer ses missions. Il peut recourir aux services d'experts.

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

Art. 5. Assistance technique

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

(2) Le Centre a pour missions :

1° de mettre en œuvre les missions lui conférées par la présente loi ;

2° de mettre à disposition l'environnement de traitement sécurisé prévu à l'article 36 ;

3° de fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles ;

4° de s'assurer de la mise en œuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou à de modification, d'agrégation, de suppression et de traitement des informations et données selon toute autre méthode de contrôle de la divulgation des données conformément au plan de confidentialité, préalablement à la mise à disposition des données dans l'environnement de traitement sécurisé ;

5° de collaborer étroitement avec l'Autorité **luxembourgeoise** des données, le tiers de confiance mandaté par le Centre, et le LNDS ;

6° de proposer, sur décision du ministre ayant le Centre dans ses attributions, des services au LNDS relatifs à la mise en œuvre des dispositions de la présente loi.

(3) Le LNDS a pour missions :

1° de mettre en œuvre les missions lui conférées par la présente loi ;

2° d'aider les organismes du secteur public, le cas échéant, à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données conformément à leurs décisions spécifiques, y compris en ce qui concerne le territoire où le traitement des données est prévu et à aider les organismes du secteur public à mettre en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation des réutilisateurs, lorsque cela est réalisable en pratique ;

3° de fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur en vertu de l'article 5, paragraphe 10, du règlement (UE) 2022/868 ;

4° de collaborer étroitement avec l'Autorité **luxembourgeoise** des données, le Centre et le tiers de confiance mandaté par le Centre ;

5° de fournir, sur demande, une assistance aux entités publiques et aux réutilisateurs de données dans le cadre de la préparation des demandes visées aux articles 27 et 28 et du plan de confidentialité visé à l'article 35.

(4) Le Centre et le LNDS :

1° veillent à ce que le personnel chargé des missions conférées par la présente loi soit fonctionnellement indépendant des entités publiques visées au titre V, des organismes du secteur public détenant les données et des réutilisateurs de données visés au titre VI ;

2° ne divulguent aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données ou permettant la divulgation de données qui sont protégées pour des motifs de protection des données à caractère personnel, de confidentialité commerciale, y compris le secret d'affaire, le secret professionnel, et le secret d'entreprise, de secrets statistique ou de protection de droits de propriété intellectuelle de tiers. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation ;

3° désignent le personnel chargé des missions qui leurs sont conférées par la présente loi. Le personnel est désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de

modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données ;

4° veillent à ce que le personnel chargé des missions qui leurs sont conférées par la présente loi ne soit pas chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données visés par la présente loi ;

5° veillent à ce que le personnel chargé des missions qui leurs sont conférées par la présente loi n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui leurs sont conférés par la présente loi ou s'il y a incompatibilité, de fait ou de droit, avec l'exercice des tâches qui leurs sont conférées en application de la présente loi.

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

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

Art. 6. Tiers de confiance

(1) Le tiers de confiance a pour missions :

1° de mettre en œuvre les missions lui conférées par la présente loi ;

2° d'effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données ;

3° de collaborer étroitement avec l'Autorité **luxembourgeoise** des données, le Centre et le LNDS.

(2) Le tiers de confiance :

1° dispose de ressources humaines et techniques suffisantes et de l'expertise adéquate pour s'acquitter efficacement des missions dont il est chargé conformément à la présente loi ;

2° ne divulgue aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données, ou susceptible de porter préjudice aux droits à la protection des données, à la propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation ;

3° désigne le personnel chargé des missions qui lui sont conférées par la présente loi. Le personnel est désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement selon toute autre méthode de contrôle de la divulgation des données ;

4° veille à ce que le personnel chargé des missions qui lui sont conférées par la présente loi ne soit pas chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données visés par la présente loi ;

5° veille à ce que le personnel chargé des missions qui lui sont conférées par la présente loi n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui lui sont conférés par la présente loi ou s'il y a incompatibilité, de fait ou de droit, avec l'exercice des tâches qui lui sont conférées en application de la présente loi.

(3) Il est interdit au personnel du tiers de confiance chargé de l'exécution des missions conférées à ce dernier par la présente loi d'avoir un intérêt quelconque, par lui-même ou par personne interposée,

et sous quelque forme juridique que ce soit, dans une entité publique, dans un organisme du secteur public détenant les données ou dans un réutilisateur de données visées aux titres V et VI.

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

Art. 7. Point d'information unique

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

1° de recevoir les demandes d'accès et de réutilisation de données visées au titre VI, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité **luxembourgeoise** des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;

2° de rendre disponibles au public toutes les informations pertinentes concernant l'application des articles 5 et 6 du règlement (UE) 2022/868 ainsi que toute autre information dont la publication est sollicitée par l'Autorité **luxembourgeoise** des données ;

3° de mettre à disposition, conformément à l'article 8, paragraphe 2, du règlement (UE) 2022/868, par voie électronique une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données conformément au titre VI, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

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

1° de recevoir les demandes de traitement ultérieur de données à caractère personnel visées par le titre V, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité **luxembourgeoise** des données et d'assurer les échanges et les démarches conformément aux dispositions du titre VII ;

2° de mettre à disposition par voie électronique la liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles en vue de leur traitement ultérieur, visée à l'article 18, paragraphe 3 ;

3° de rendre disponibles au public toutes les informations dont la publication est demandée par l'Autorité **luxembourgeoise** des données.

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

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

(1) Le Conseil consultatif de la valorisation des données dans un environnement de confiance, institué par la loi du […] portant création du Commissariat du Gouvernement à la souveraineté des données, a pour mission de :

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.

~~**(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 :

1° d'assurer la mise à disposition d'informations et de données à caractère personnel aux entités publiques pour l'exécution de leurs obligations et de leurs missions d'intérêt public ;

2° d'alléger la charge administrative des administrés dans le cadre de leurs demandes et déclarations ;

3° d'éviter aux entités publiques de devoir organiser elles-mêmes la collecte d'informations et de données à caractère personnel auprès des administrés.

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

(1) Lorsque les informations ou données à caractère personnel nécessaires pour traiter la demande présentée par l'administré ou la déclaration présentée par celui-ci doivent être obtenues auprès d'une autre entité publique, dans les conditions prévues aux articles 11 et 12, l'administré ou son tuteur, son curateur, son administrateur légal, son administrateur ad hoc ou son mandataire spécial certifie l'exactitude des informations et des données à caractère personnel ainsi obtenues.

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

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

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

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

L'obligation prévue à l'alinéa 1er s'applique également dans les cas où l'entité publique se procure des informations ou des données à caractère personnel auprès d'autres entités publiques pour informer les administrés sur leurs droits au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

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

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

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

1° les entités publiques ne sont pas tenues de procéder à l'échange d'informations et de données à caractère personnel visé à l'article 9 ;

2° l'administré les communique à l'entité publique chargée du traitement de la demande ou de la déclaration.

Dans les cas visés à l'alinéa 1er, l'entité publique chargée du traitement de la demande ou de la déclaration et l'entité publique détentrice des informations et données à caractère personnel remédient dans les meilleurs délais à l'impossibilité d'échanger les informations et les données à caractère personnel en question.

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

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

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

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

1° dans le cadre du traitement effectué dans l'exercice de leurs missions des demandes et déclarations présentées par un administré ;

2° pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

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

Dans un délai d'un mois à partir de la notification visée à l'alinéa 1er, les entités publiques notifiées :

1° certifient la disponibilité des informations et des données à caractère personnel à l'entité publique demanderesse et confirment que l'échange d'informations et de données à caractère personnel n'est pas impossible ; ou

2° informent l'entité publique demanderesse du fait qu'elles ne détiennent pas les informations et les données à caractère personnel sollicitées ou que l'échange d'informations et de données à caractère personnel est impossible.

Une copie de l'information visée à l'alinéa 2, points 1° et 2°, est transmise au ministre ayant la digitalisation dans ses attributions.

(3) Dans les cas visés au au paragraphe 2, alinéa 2, point 2°, les entités publiques concluent dans les meilleurs délais, et au plus tard après trois mois, le protocole visé à l'article 13.

Art. 13. Protocole « *once only* »

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

Le protocole contient, au moins, les éléments suivants :

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

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

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

4° une description détaillée des catégories de personnes concernées ;

5° une description détaillée des finalités du traitement ;

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

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

(2) Tout changement des éléments liés à l'obtention des informations et des données à caractère personnel auprès d'une entité publique doit être formalisé par avenant du protocole visé au paragraphe 1er.

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

Les entités publiques informent sans délai l'Autorité **luxembourgeoise** des données lorsqu'un protocole n'est plus applicable. L'Autorité **luxembourgeoise** 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 **luxembourgeoise** 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 1er.

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

Section I – Dispositions générales

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

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

1° les conditions énoncées au présent titre sont remplies ;

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

a) l'analyse statistique ;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1° l'entité publique qui détient les données à caractère personnel **a marqué son accord par** :

a) ~~**a marqué son accord de principe au traitement ultérieur, y compris le partage et la mise à disposition en inscrivant les**~~ **l'inscription des** 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 contresignature de** 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 **luxembourgeoise** des données**, après l'accord de l'entité publique qui détient les données à caractère personnel,** 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 sont remplies ;

~~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~~

2° l'accès et la réutilisation des données est effectué exclusivement pour une ou plusieurs des finalités visées à l'article 15, paragraphe 3, point 1° loi du […] portant création du Commissariat du Gouvernement à la souveaineté des données.

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 **luxembourgeoise** des données**, après l'accord de l'organisme du secteur public l'entité publique qui détient les données à caractère personnel,** autorise l'accès et la réutilisation conformément à l'article 31 ;

2° l'organisme du secteur public qui détient les données **a marqué son accord par** :

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**~~ **l'inscription des** 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 contresignature de 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 **luxembourgeoise** des données**, après l'accord de l'entité publique qui détient les données à caractère personnel,** autorise l'accès et la réutilisation conformément à l'article 31 ;

2° l'organisme du secteur public qui détient les données **a marqué son accord par** :

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**~~ **l'inscription des** 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 contresignature de** 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 **luxembourgeoise** 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 **luxembourgeoise** 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 **luxembourgeoise** 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° ;

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°.

(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 :

1° certifient l'exactitude des informations contenues dans la demande et les pièces jointes visées au présent article ;

2° certifient que le plan de confidentialité correspond aux informations contenues dans la demande présentée à l'Autorité **luxembourgeoise** des données ;

3° s'engagent formellement à respecter les termes de l'autorisation de l'Autorité **luxembourgeoise** 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° ;

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°.

(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 :

1° certifient l'exactitude des informations contenues dans la demande et les pièces jointes visées au présent article ;

2° certifient que le plan de confidentialité correspond aux informations contenues dans la demande présentée à l'Autorité **luxembourgeoise** des données ;

3° s'engagent formellement à respecter les termes de l'autorisation de l'Autorité **luxembourgeoise** des données et du plan de confidentialité.

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

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

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

(2) L'Autorité **luxembourgeoise** 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 :

1° la demande visée à l'article 27 est complète et accompagnée de toutes les pièces visées à l'article 27, paragraphe 2 ;

2° pour les cas visés à l'article 18, paragraphe 3), point 3°, a) :

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 ;

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

~~**2° l'entité publique détentrice des données à caractère personnel a donné son accord écrit spécifique au traitement ultérieur de données à caractère personnel, y compris au partage et à la mise à disposition, en contresignant la demande visée à l'article 27 ;**~~

3° le traitement ultérieur de données à caractère personnel est exclusivement effectué pour une ou plusieurs finalités visées à l'article 15, paragraphe 1er, point 2 ;

4° le traitement ultérieur de données à caractère personnel ne porte pas une atteinte disproportionnée aux droits et libertés de la personne concernée au regard de la finalité poursuivie.

(2) Dans les cas visés au titre VI, l'Autorité **luxembourgeoise** 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 concernés ;

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

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

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

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

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

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

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

ii. lettre b), la signature de la demande par tous les organismes du secteur public concernés ;

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

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

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

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

(3) La décision d'autorisation ou de refus de l'Autorité **luxembourgeoise** des données est motivée. L'Autorité **luxembourgeoise** 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 **luxembourgeoise** 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 **luxembourgeoise** des données, l'Autorité **luxembourgeoise** 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 à la lettre a).

2° dans le cas visé au titre VI :

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

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

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

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

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

(7) Les entités publiques traitant ultérieurement les données à caractère personnel et les réutilisateurs de données sont tenus de traiter les données uniquement conformément aux termes de l'autorisation de l'Autorité **luxembourgeoise** 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 **luxembourgeoise** 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 **luxembourgeoise** 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 **luxembourgeoise** 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 luxembourgeoise 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 **luxembourgeoise** 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 par l'intermédiaire du point d'information unique.

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

(1) L'Autorité **luxembourgeoise** 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 :

1° pour les cas visés au titre V, les entités publiques effectuant le traitement ultérieur de données à caractère personnel et les entités publiques détenant les données à caractère personnel ;

2° pour les cas visés au titre VI, les réutilisateurs de données et les organismes du secteur public détenant les données.

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

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

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

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

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

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

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

1° le Centre, ou le tiers de confiance mandaté par le Centre, s'assure de la mise en œuvre les mesures visées au présent article conformément aux stipulations du plan de confidentialité ;

2° le Centre :

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

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

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

1° restreindre aux personnes physiques autorisées indiquées dans l'autorisation correspondante visée à l'article 31 l'accès à l'environnement de traitement sécurisé ;

2° réduire au minimum le risque de lecture, de copie, de modification ou de suppression non autorisées des données hébergées dans l'environnement de traitement sécurisé par des mesures techniques et organisationnelles de pointe ;

3° restreindre à un nombre limité d'individus identifiables autorisés l'introduction de données et l'inspection, la modification ou la suppression de données hébergées dans l'environnement de traitement sécurisé ;

4° veiller à ce que les personnes visées au point a) n'aient accès qu'aux données couvertes par leur autorisation correspondante visée à l'article 31, au moyen d'identifiants individuelles et uniques et de modes d'accès confidentiels uniquement ;

5° tenir des registres identifiables de l'accès à l'environnement de traitement sécurisé et des activités qui y sont menées pendant la période nécessaire pour vérifier et contrôler toutes les opérations de traitement dans cet environnement. Les registres d'accès devraient être conservés pendant au moins un an ;

6° veiller à la conformité et contrôler les mesures de sécurité énumérées au présent article afin d'atténuer les menaces potentielles pour la sécurité.

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

1° de reproduire les données à l'extérieur de l'environnement et ainsi de les réutiliser dans un autre contexte ou pour des finalités autres qu'autorisées ;

2° d'introduire des solutions technologiques, y compris d'intelligence artificielle, à moins qu'elles aient expressément été inclues dans le plan de confidentialité, ou préalablement été évaluées et certifiées par le Centre, ou par le tiers de confiance mandaté par le Centre, comme ne présentant aucun risque d'atteinte aux exigences visées à l'article 35, paragraphe 1er ;

3° d'introduire des données, à moins que cette introduction ait expressément été demandée conformément à l'article 27, paragraphe 1, point 10°, et à l'article 28, paragraphe 1, point 8°, et autorisée par l'Autorité **luxembourgeoise** des données conformément aux dispositions du présent titre ;

4° d'extraire les données de l'environnement de traitement sécurisé, à moins qu'elles aient préalablement été anonymisées.

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

1° créer un environnement de traitement sécurisé commun, ensemble avec des organismes compétents désignés conformément à l'article 7 du règlement (UE) 2022/868, afin de mettre les données à disposition des entités publiques ou des réutilisateurs de données ;

2° combiner et traiter les données visées au titre VI avec des données provenant d'environnements de traitement sécurisés d'autres États membres gérés par des organismes compétents désignés conformément à l'article 7 du règlement (UE) 2022/868 afin de les mettre à disposition des réutilisateurs de données.

Art. 37. Responsabilité du traitement

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

(2) L'Autorité **luxembourgeoise** 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 **luxembourgeoise** 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~~38. 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. ~~40~~39. 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. 41. Sanctions**~~

~~**(1) Dans le cadre d'une violation de l'obligation de notification incombant aux prestataires de services d'intermédiation de données en vertu de l'article 11 du règlement (UE) 2022/868 ou des conditions liées à la fourniture de services d'intermédiation de données en vertu de l'article 12 du règlement (UE) 2022/868, la CNPD peut, par voie de décision, imposer des amendes administratives à hauteur de 500 à 100. 000 euros aux prestataires de services d'intermédiation de données.**~~

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

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

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

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

~~***Section II – Recours***~~

~~**Art. 42. Recours**~~

~~**Un recours contre les décisions de la CNPD prises en application des chapitres III et IV du Règlement 2022/686 est ouvert devant le Tribunal administratif qui statue comme juge du fond.**~~

TITRE IX – Dispositions finales

Art. 4340. 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 ».

*

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 à la Digitalisation
Projet de loi ou amendement :	Projet d'amendements au projet de loi n° 8395B 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

Ce projet de loi traite de la valorisation des données du secteur public dans un environnement de confiance et ne contribue donc pas à favoriser une inclusion sociale et une éducation pour tous.

2. Assurer les conditions d'une population en bonne santé. Poins d'orientation / Documentation ☐ Oui ☒ Non

Ce projet de loi a pour objet la valorisation des données du secteur public dans un environnement de confiance et n'a donc pas de lien avec la santé de la population.

3. Promouvoir une consommation et une production durables. Poins d'orientation / Documentation ☐ Oui ☒ Non

Ce projet de loi concerne la valorisation des données du secteur public dans un environnement de confiance et n'a pas d'impact sur la consommation ou la production durables.

4. Diversifier et assurer une économie inclusive et porteuse d'avenir. Poins d'orientation / Documentation ☒ Oui ☐ Non

Ce 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 etre 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 béneficier et stimulant ainsi la société de l'information.

5. Planifier et coordonner l'utilisation du territoire. Poins d'orientation / Documentation ☐ Oui ☒ Non

Ce projet de loi, relatif à la valorisation des données du secteur public dans un environnement de confiance, n'a pas d'impact sur la coordination et la planification de l'utilisation du territoire luxembourgeois.

6. Assurer une mobilité durable. Poins d'orientation / Documentation ☐ Oui ☒ Non

Ce projet de loi n'a pas d'impact sur la mobilité durable.

7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles. Poins d'orientation / Documentation ☐ Oui ☒ Non

Ce projet de loi n'a pas d'effet sur l'environnement ou les ressources naturelles.

8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable. Poins d'orientation / Documentation ☐ Oui ☒ Non

Ce projet de loi n'a pas d'impact direct sur le climat, le changement climatique ou l'énergie durable.

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

Ce projet de loi n'a pas d'impact sur la pauvreté ou sur la cohérence des politiques pour le développement durable.

10. Garantir des finances durables.

Poins d'orientation Documentation ☐ Oui ☒ Non

Ce projet de loi ne contribuera pas financièrement à l'action climatique, ni au développement durable.

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
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
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

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
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	%
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

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
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
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

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
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
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

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
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)
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)

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
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

Impression: CTIE – Division Imprimés et Fournitures de bureau

20250724_Avis

Avis

PROJET DE LOI n°8395

Le 11 juillet 2025

Ce document constitue la position de la FEDIL Health Corporations (ci-après « FHC ») relative au projet de loi n°8395 déposé en date du 12 juin 2024 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).

La FEDIL Health Corporations fédère les entreprises luxembourgeoises opérant dans les secteurs de la santé et des sciences de la vie, en leur offrant une plateforme d'échange ouverte sur les problématiques spécifiques rencontrées par le secteur privé, tout en assurant leur représentation auprès des autorités publiques et institutionnelles.

A. Introduction et commentaires de fond

La digitalisation de la santé figure parmi les priorités stratégiques de la fédération qui entend veiller à accélérer les initiatives et les projets de digitalisation du secteur et à saisir les opportunités offertes pour le secteur, notamment sur le sujet des données de santé. En effet, compte tenu de l'importance croissante de ces données et de leur mise à disposition pour favoriser l'innovation médicale, thérapeutique et technologique visant à offrir une meilleure qualité de soin du patient, la FHC souhaite accompagner le développement de toute initiative stratégique liée à la gestion, l'exploitation et la valorisation des données de santé.

Dès lors, le projet de loi n°8395 relatif à la mise en application de certaines dispositions du règlement (UE) 2022/868 portant sur la gouvernance européenne des données ("Data Governance Act" ou "DGA") et comportant également certaines dispositions relatives à la valorisation des données dans un environnement de confiance et à la mise en œuvre du principe « once only » revêt un enjeu stratégique majeur pour le secteur privé.

Il apparaît essentiel que le projet de loi soit également cohérent et pleinement aligné avec les principes et mécanismes du Règlement (UE) 2025/327 relatif à l'espace européen des données de santé (« European Health Data Space » - ou "EHDS"), particulièrement en matière d'interopérabilité, d'accès sécurisé et de gouvernance des données, afin de garantir une harmonisation réglementaire et opérationnelle à l'échelle européenne.

La FHC souligne également l'opportunité d'une mise en œuvre rapide d'un cadre solide et prévisible afin de positionner le Luxembourg au mieux quant à l'attraction d'entreprises innovantes sur son territoire.

7, rue Alcide de Gasperi · Luxembourg-Kirchberg
P.O. Box 1304 – L-1013 Luxembourg
tél.: (+352) 43 53 66-1 – www.fedilhealthcorporations.lu

Avis

PROJET DE LOI n°8395

Le 11 juillet 2025

La FEDIL Health Corporations soutient favorablement la démarche gouvernementale visant à instaurer une gouvernance efficace et transparente des données publiques, notamment en simplifiant les processus administratifs et en facilitant l'accès aux données publiques. Toutefois, après examen approfondi du texte législatif proposé, plusieurs interrogations et préoccupations subsistent, nécessitant des éclaircissements pour en assurer la pleine effectivité et applicabilité.

La FEDIL Health Corporations prend acte de la décision du 22 avril 2025 de scinder le projet de loi initial en deux textes distincts :

- le projet de loi n°8395A, qui se limite à désigner les autorités compétentes au sens du DGA et à leur conférer les pouvoirs nécessaires à l'exercice de leurs missions ;
- le projet de loi n°8395B, qui contient toutes les autres mesures initialement contenues dans le projet de loi 8395, à savoir, entre autres, les mesures complémentaires nécessaires à la mise en œuvre effective du DGA, ainsi que les autres mesures relatives au principe du "once only", au traitement ultérieur de données par des personnes publiques etc.

Si la FEDIL Health Corporations n'émet pas de commentaires spécifiques sur le contenu du projet de loi n°8395A, elle souhaite néanmoins souligner plusieurs préoccupations quant à la méthode retenue.

1. Une transposition fragmentée source d'insécurité juridique

L'adoption des mesures nécessaires à l'application du DGA en deux projets de loi distincts soulève des interrogations quant à la cohérence des deux textes, et à l'applicabilité en pratique du DGA. En effet, le projet de loi n°8395A, en l'état, désigne les autorités compétentes et leur attribue des pouvoirs, mais sans leur fournir les outils juridiques nécessaires à l'exercice effectif de leurs missions. Cette situation crée un déséquilibre : les autorités sont nommées, mais ne disposent pas encore des procédures ni des bases légales pour traiter les demandes de réutilisation des données.

2. Une mise en œuvre à deux vitesses

Le découplage des textes crée un risque de mise en œuvre à deux vitesses du DGA au Luxembourg. Si les deux projets de loi n'évoluent pas au même rythme dans le processus législatif, cela pourrait retarder l'application complète du règlement européen. Or, une mise en application rapide et efficace du DGA est bénéfique pour le secteur privé car il encourage l'innovation et la compétitivité en permettant un accès sécurisé et réglementé à des ensembles de données auparavant inaccessibles. En pratique, cela signifie que les acteurs économiques, notamment les entreprises souhaitant accéder à des données publiques ou industrielles, ne pourront pas exercer les droits prévus par le DGA tant que le projet de loi n°8395B ne sera pas adopté. Cela porte préjudice aux entreprises luxembourgeoises par rapport aux entreprises des pays voisins, dans lesquels le DGA serait applicable plus rapidement.

7, rue Alcide de Gasperi - Luxembourg-Kirchberg
P.O. Box 1304 – L-1013 Luxembourg
tél.: (+352) 43 53 66-1 – www.fedilhealthcorporations.lu

3. Des difficultés d'articulation entre régimes juridiques

Le projet de loi n°8395B, tel qu'il est rédigé, soulève également des questions d'articulation entre les mesures de mise en œuvre du DGA, les dispositions complémentaires proposées (notamment en matière de réutilisation des données dans le secteur public), et les règles issues d'autres textes européens, comme le RGPD (règlement (UE) 2016/679). Des imprécisions, voire des incohérences terminologiques, sont à relever, ce qui pourrait nuire à la lisibilité et à la sécurité juridique du dispositif.

4. Une complexité accrue pour les praticiens et les usagers

Enfin, la coexistence de deux lois pour transposer un même texte européen complique la tâche des praticiens du droit, qui devront naviguer entre deux régimes pour conseiller leurs clients. Cette complexité risque également de décourager les entreprises et les citoyens souhaitant faire valoir les droits que leur confère le DGA.

À la vue de ce qui est énoncé ici, la FEDIL Health Corporations exhorte à une application rapide et efficace du DGA. Pour cela, la FEDIL Health Corporations recommande de reconsidérer l'opportunité de maintenir deux projets de loi distincts pour la transposition du DGA L'adoption des mesures nécessaires à l'adoption d'un texte ayant un effet direct semble présenter moins de difficultés que la création *ex nihilo* d'un régime d'utilisation ultérieur des données personnelles par les personnes publiques, et d'un système mettant en œuvre le principe "once only". L'adoption d'un texte dédié au DGA faciliterait et accélérerait la mise en œuvre du DGA, qui est importante pour renforcer la compétitivité de l'économie européenne et Luxembourgeoise.

B. Analyse détaillée de cas d'utilisation illustrant les effets de la mise en œuvre du projet de loi

1. Utilisation industrielle et commerciale des données et compatibilité avec le DGA

- Commentaire 1 :

L'article 2, paragraphe 2 du projet de loi définit les "entités publiques" au sens des titres IV (échanges entre administrations – "once only") et V (traitement ultérieur par les entités publiques). En revanche, la notion d'"organismes du secteur public", utilisée au titre VI relatif à la réutilisation des données protégées par des tiers (mettant en œuvre le DGA), n'y est pas définie de manière autonome. Nous comprenons que ce terme est défini à l'article 2(17) du Data Gouvernance Act. Cependant, la superposition des deux cadres juridiques distincts au sein d'un même projet de loi crée une incohérence terminologique et un champ d'application peu lisible, source d'insécurité juridique pour les titulaires des droits. Nous nous référons ici à nos commentaires sur la l'éparpillement des mesures relatives à l'application du DGA, et sur la coexistence de régimes juridiques distincts au sein d'un même projet de loi.

- Proposition 1 :

La FHC recommande dès lors que le projet de loi reprenne ou explicite clairement cette notion, en cohérence avec la définition figurant à l'article 2(17) du règlement (UE) 2022/868[1].

Par ailleurs, en référence à l'article 23, paragraphe 2 du projet de loi 8399B, l'accès aux données publiques est limité lorsqu'il risque de restreindre la concurrence ou d'offrir des avantages économiques disproportionnés. Cette formulation suscite des ambiguïtés significatives quant aux conditions réelles d'accès pour les initiatives commerciales ou semi-commerciales.

Nous nous permettons d'illustrer notre propos par des exemples ci-dessous.

- Exemple 1.1 :

Actuellement, lorsqu'un utilisateur souhaite créer un compte patient sur une plateforme de prise de rendez-vous médical, il doit renseigner manuellement un certain nombre d'informations personnelles. Ces données existent pourtant déjà dans des systèmes tels que MyGuichet ou le Dossier de Soins Partagé (DSP), où elles sont stockées de manière digitale et structurée.

- Exemple 1.2 :

Dans le cadre de la lutte contre le cancer du poumon, ce cas d'usage illustre la valeur ajoutée de l'intégration des données de santé dans un environnement fédéré, sécurisé et conforme au futur règlement EHDS. Il met en lumière l'apport des technologies d'intelligence artificielle (IA) et d'apprentissage automatique (ML) pour améliorer la prévention, le diagnostic, le pronostic et le suivi personnalisé des patients.

L'objectif consiste en développer une solution de surveillance à distance à domicile, intégrant des outils d'IA/ML, pour le profilage des risques, le diagnostic précoce, le suivi pronostique ou encore le bien-être et l'engagement du patient.

Dans le cadre d'un environnement de données fédérées, les données cliniques, imagerie, données de capteurs à domicile, et historiques médicaux sont accessibles via un SPE (espace de partage de données compatible EHDS), garantissant un contrôle d'accès organisationnel et technique.

Afin de gérer les aspects de sécurité et de consentement, l'accès aux données, qu'il soit primaire (soins) ou secondaire (recherche, innovation), est soumis à une authentification forte et à un consentement dynamique du patient. Luxtrust peut être envisagée comme solution d'identification et de gestion du consentement, même si la FHC soutiendrait l'apparition de solutions alternatives qui permettraient de ne pas dépendre d'une solution unique en situation de monopole. Ainsi, le standard européen pourrait se trouver être une option à explorer.

[1] https://eur-lex.europa.eu/eli/reg/2022/868/oj?locale=fr

Grâce à la technologie embarquée, les dispositifs à domicile (capteurs, applications mobiles) collectent des données en continu, analysées localement ou via des modèles IA dans le cloud, pour générer des alertes ou recommandations personnalisées.

- Commentaire Exemple 1.1 et 1.2 :

En raison de la formulation actuelle imprécise du projet de loi, une telle initiative pourrait se heurter à un refus administratif motivé par l'absence de critères clairement définis permettant d'évaluer objectivement l'existence d'un avantage économique disproportionné. Cette incertitude réglementaire constitue un frein réel à l'innovation technologique, à la modernisation des services de santé, ainsi qu'à leur optimisation pour le bénéfice des citoyens.

- Proposition Exemple 1.1 et 1.2 :

Pour simplifier ce processus, la FHC est d'avis qu'une solution pourrait consister à permettre à l'utilisateur de donner son consentement explicite à la plateforme pour accéder directement aux informations nécessaires via une authentification forte et sécurisée. À l'instar de ce qui se fait pour les comptes bancaires en ligne, l'utilisateur autoriserait la plateforme à récupérer automatiquement les données déjà disponibles par le biais d'une validation par une connexion Luxtrust (ou autre solution équivalente), éliminant ainsi la nécessité de ressaisir les informations.

Dans ce modèle, l'entreprise agit comme un intermédiaire entre la source de données et l'utilisateur final, en facilitant l'accès et l'utilisation des données structurées. L'entreprise sera donc enregistrée et validée par Luxtrust (ou autre solution équivalente), offrant ainsi le même type de sécurité que le système bancaire. Le bénéfice principal du principe "once only" revient donc au patient, qui profite d'une expérience simplifiée et fluide.

- Exemple 2 :

Une entreprise souhaite exploiter des données cliniques provenant directement de cabinets médicaux afin d'identifier et cartographier précisément la présence d'allergènes et de perturbateurs endocriniens contenus dans des produits pharmaceutiques et cosmétiques par un processus similaire à du « crowd sourcing ». Bien que cette approche puisse améliorer substantiellement la santé publique, elle offre également à l'entreprise un avantage concurrentiel potentiel, susceptible d'être considéré par l'administration comme disproportionné vis-à-vis d'autres acteurs du secteur.

- Commentaire Exemple 2 :

FHC estime que le texte actuel ne permet pas de clarifier comment ce type d'initiative peut être conforme à l'article 23, tout en évitant une distorsion de concurrence.

- Proposition 2 :

La FEDIL Health Corporations recommande par conséquent l'élaboration de règlements grand-ducaux fixant des critères détaillés et transparents ainsi que des procédures explicites afin de permettre une évaluation objective et équitable des conditions d'exploitation commerciale des données publiques. De plus, il est recommandé de mettre en place une plateforme publiquement accessible où les demandes d'accès faites sont publiées, avec leur statut dans le processus (accordée, refusée, en cours de traitement). En cas de refus, une explication pourrait être fournie pour permettre d'ajuster la demande. Cela éviterait ainsi que des entreprises fassent plusieurs fois les mêmes demandes et elles pourront demander soit le même accès déjà accordée à une autre ou tenter de reformuler leur demande en fonction des explications d'un éventuel refus émis précédemment.

2. Enjeux de standardisation et interopérabilité

L'article 9 du projet de loi introduit une obligation d'échange de données entre entités publiques, dans une logique de simplification administrative, sans détailler toutefois les modalités techniques et organisationnelles nécessaires à la mise en œuvre effective de ces échanges. Si une certaine interopérabilité est implicitement requise pour garantir l'application du principe "Once Only", le texte reste silencieux sur les standards, formats de données ou délais de mise en œuvre. Cette absence de précision pose des défis opérationnels majeurs, notamment illustrés dans l'exemple ci-dessous.

- Exemple :

Dans ce cas concret, une équipe de recherche scientifique spécialisée dans les soins des plaies chroniques se heurte à des difficultés significatives dues à l'absence d'interopérabilité réelle entre les systèmes utilisés par les infirmiers communautaires et les médecins généralistes.

- Commentaire :

La FHC juge que l'absence de normes précises et de formats de données harmonisés conduit à une fragmentation des données, générant ainsi des surcoûts imprévus, une dégradation substantielle de la qualité des résultats scientifiques et un ralentissement notable du processus de recherche.

Par ailleurs, anticipant la mise en œuvre du EHDS, les États membres de l'Union européenne devront garantir que certains types de données de santé, tels que les résumés de patients, les prescriptions électroniques, les images médicales et leurs rapports, les résultats de laboratoire ou encore les comptes rendus de sortie, soient échangés dans un format européen commun. Cet échange devra s'effectuer via une infrastructure numérique transfrontalière, assurant l'interopérabilité, la sécurité et la continuité des soins à l'échelle européenne.

- Proposition :

FHC suggère vivement de prévoir des règlements grand-ducaux techniques détaillant les standards obligatoires, les protocoles précis ainsi que les responsabilités et échéanciers opérationnels clairs pour la mise en œuvre effective de l'interopérabilité. Pour ce faire, une étude de standards déjà existants est à réaliser. Subsidiairement, si une standardisation n'est pas possible au niveau des différentes institutions, la FHC recommande de prévoir que la plateforme centralisée mette en place un système de retraitement des données d'origine pour les mettre à disposition de manière standardisée. Cette approche permettrait aux établissements de santé de conserver leurs systèmes d'information existants, en limitant les adaptations techniques nécessaires. Un tel mécanisme de retraitement centralisé favoriserait l'adhésion des acteurs de terrain, tout en assurant l'interopérabilité requise au niveau européen. Il s'agit d'un compromis réaliste entre ambition réglementaire et faisabilité opérationnelle, qui permettrait de concilier souveraineté numérique, efficacité administrative et continuité des soins transfrontaliers.

3. Sécurité, accessibilité et gestion proactive des échanges de données

L'article 36, paragraphe 1 ne détaille pas les protocoles précis nécessaires pour assurer la sécurité de l'environnement de traitement qui sera mis en place, ce qui posera des défis opérationnels que l'exemple ci-dessous illustre.

- Exemple :

Actuellement, dans le cadre de prestations remboursées par la CNS fournies par un acteur privé de matériel médical, les ordonnances médicales sont reçues au format papier, scannées, puis transmises à la CNS, soit par papier ou courriel, soit dans le meilleur des cas, par le biais de la plateforme sécurisée Healthnet.

Avec l'introduction imminente des prescriptions électroniques, ces ordonnances seront émises par les médecins et probablement déposées dans le **Dossier de Soins Partagé (DSP)** du patient. Par la suite, le patient devra transférer cette ordonnance électronique au fournisseur de matériel médical afin d'établir le lien nécessaire avec la CNS dans le cadre du mécanisme de tiers payant. Le fournisseur sera alors responsable du remboursement auprès de la CNS, hors reste à charge pour le patient.

- Commentaire :

En cas d'incidents techniques, tels que des erreurs d'identification ou des dysfonctionnements non rapidement résolus, ce fournisseur subirait des retards administratifs, impactant négativement tant la fluidité du processus administratif et financier que la satisfaction des patients.

Dans ce contexte, un mécanisme d'accès et de partage sécurisé des données sera indispensable. Si cet accès ou ce partage est limité, le fournisseur ne pourra pas transmettre les informations nécessaires à la CNS, ce qui imposera d'envisager d'autres solutions pour garantir le bon fonctionnement du processus.

- Proposition :

Afin d'éviter ces problèmes opérationnels, FHC est d'avis qu'il serait indispensable de compléter le projet de loi par l'exigence d'un règlement grand-ducal précisant des directives techniques claires portant sur la gestion sécurisée des accès, la procédure détaillée de gestion des identités ainsi que des mécanismes précis et réactifs pour résoudre les incidents techniques et sécuritaires. Ceci pourrait utilement avoir lieu dans le cadre du système Healthnet déjà existant.

4. Demande de traitement ultérieur ou d'accès et de réutilisation

La FEDIL Health Corporations questionne l'opportunité de traiter dans un titre commun des régimes juridiques différents, à savoir le traitement ultérieur de données à caractère personnel par les entités publiques, relevant du Titre V, et l'accès et la réutilisation de données détenues par les organismes du secteur public par les réutilisateurs de données, relevant du Titre VI, et mettant en œuvre le DGA. Les champs d'application respectifs des régimes - qui au demeurant concernent respectivement des entités publiques et privés - ne sont pas suffisamment clairement distincts, entraînant une insécurité juridique pour les utilisateurs, nuisible à l'applicabilité des dispositions du DGA, qui visent à renforcer la compétitivité et l'innovation.

Concernant le Titre VI, la FEDIL Health Corporations note que le terme "réutilisateur de données" n'est pas défini dans le projet de loi, et ne trouve pas d'équivalent dans le DGA (lequel se réfère à "utilisateur de données"). Pour des raisons de cohérence, il serait préférable d'employer les termes du DGA.

Par ailleurs, la FEDIL Health Corporations s'interroge sur la séquence des autorisations à obtenir en vue d'une demande de réutilisation des données, dans la mesure où cette demande doit être adressée à l'Autorité des données, et être accompagnée du plan de confidentialité "signé par toutes les parties visées à l'article 35, paragraphe 2", à savoir , pour ce qui concerne les demande de réutilisation des données, par le réutilisateur de données, les organismes du secteur public et le Centre ou le tiers de confiance mandaté par le Centre. Les modalités de mise en œuvre du DGA ne sont pas claires, privant ainsi les entreprises de la capacité d'exercer leurs droits.

5. Contrôle par l'Autorité des données

Aux termes de l'article 32 du projet de loi, l'Autorité des données soit voit confier le droit de "vérifier le processus, les moyens, et tout résultat" des accès et réutilisation des données effectuées par les utilisateurs de données conformément au Titre VI, et se voit dotée du pouvoir d'interdire "l'utilisation des résultats qui contiennent des informations portant une atteinte disproportionnée aux droits et aux intérêts de tiers".

La FEDIL Health Corporations considère que l'Autorité des données dispose d'un pouvoir discrétionnaire qui implique une insécurité juridique dans le chef des "réutilisateurs de données". Il serait préférable de permettre à l'Autorité de données de vérifier que la réutilisation est effectuée "conformément aux termes de l'autorisation de l'Autorité des données", comme cela est prévu à l'article 31 (7) du projet de loi.

C. Conclusion

La FEDIL Health Corporations considère que le projet de loi n°8395, ultérieurement scindé en deux projets de loi distincts, et visant à favoriser la confiance et l'accès à certaines données auparavant inaccessibles et utiles pour soutenir l'innovation et la compétitivité du pays, constitue une avancée majeure vers une gouvernance moderne et efficace des données au Luxembourg. Néanmoins, l'introduction de clarifications détaillées, de procédures opérationnelles et de critères clairs demeure indispensable pour assurer sa pleine applicabilité et pour favoriser un environnement propice à l'innovation. La FEDIL Health Corporations reste pleinement disponible pour poursuivre ces échanges et contribuer à l'élaboration d'un cadre législatif robuste et pragmatique.

La FHC a également pris note des amendements du 13 juin 2025 et se réserve le droit de prendre position sur ces amendements et/ou tout amendement ultérieur.

-.-.-.-.-.-