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)

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 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. 1er. 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. ~~43~~40. 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 ».