N°8395/2
Entrée le 25.10.2024
Chambre des Députés

CHAMBRE DES SALARIÉS
LUXEMBOURG

AVIS

Avis III/32/2024 23 octobre 2024

Valorisation des données dans un environnement de confiance

relatif aux

Projet de loi

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

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

Par lettres du 12 juin 2024, Madame Stéphanie Obertin, ministre de la Digitalisation a soumis le projet de loi et le projet de règlement grand-ducal sous rubrique à l'avis de la Chambre des salariés (CSL).

1. Le présent projet a pour objet de compléter le règlement (UE) 2022/868 sur la gouvernance des données (Data Governance Act,ci-après aussi AGD) qui a pour objectif d'instaurer la confiance entre les citoyens et les acteurs impliqués dans l'accès et la réutilisation des données, en particulier en concevant des mécanismes appropriés permettant le respect des droits individuels dans le contexte de l'accès et de la réutilisation des données à caractère personnel et à caractère non personnel détenues par les organismes du secteur public.

2. Le règlement (UE) 2022/868 est applicable depuis le 24 septembre 2023 et il détermine la majorité des dispositions de fond.

Résumé du règlement (UE) 2022/868 [1]

Il vise à rendre davantage de données disponibles pour la réutilisation et à faciliter le partage des données dans des domaines tels que la santé, l'environnement, l'énergie, l'agriculture, la mobilité, la finance, l'industrie manufacturière, l'administration publique et les compétences, au profit des citoyens et des entreprises, en créant des emplois et en stimulant l'innovation.

Le règlement européen énonce :

- *les **conditions de réutilisation de certaines données protégées** détenues par des organismes du secteur public ;*
- *des **règles** pour les entreprises fournissant des services d'intermédiation de données ;*
- ***un cadre pour l'altruisme en matière de données** (le partage des données de manière volontaire et sans contrepartie) ;*
- ***un cadre pour le Comité européen de l'innovation dans le domaine des données (EDIB)** ; et*
- *des mesures permettant le **flux sécurisé de données à caractère non personnel** en dehors de l'UE.*

Réutilisation de certaines catégories de données publiques

Les organismes du secteur public détiennent de grandes quantités de données protégées par les droits de tiers (tels que les secrets commerciaux, les données personnelles ou la propriété intellectuelle) qui ne peuvent pas être utilisées en tant que données ouvertes, mais qui pourraient être réutilisées en vertu de règles européennes ou nationales spécifiques. Lorsqu'une telle réutilisation est autorisée, les organismes du secteur public devront respecter les conditions de réutilisation fixées par l'AGD. Les conditions de réutilisation doivent être non discriminatoires, transparentes, proportionnées, justifiées et rendues publiques.

Transfert de données vers des pays tiers

Un réutilisateur ayant l'intention de transférer des données protégées et à caractère non personnel vers un pays tiers devra se conformer aux règles spécifiques de l'AGD.

Redevances

Les redevances de réutilisation que les Etats membres peuvent fixer, doivent être transparentes, proportionnées, non discriminatoires et objectivement justifiées. Les organismes du secteur public qui accordent des permis de réutilisation peuvent appliquer des frais réduits ou nuls, par exemple pour les petites et moyennes entreprises, les jeunes entreprises, les organisations de la société civile et les établissements d'enseignement.

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

Point d'information unique

Pour garantir que les données puissent être trouvées («trouvabilité»), les États membres de l'UE devront veiller à ce que toutes les informations pertinentes sur les conditions de réutilisation et sur les redevances soient disponibles et facilement accessibles via un point d'information unique. La Commission européenne rassemblera à son tour ces informations sur data.europa.eu.

Services d'intermédiation de données

L'AGD réglemente en outre les fournisseurs de services d'intermédiation de données, qui sont des tiers neutres qui mettent en relation les personnes et les entreprises qui détiennent des données avec d'autres qui souhaitent les utiliser. Les exigences relatives à ces services visent à garantir que ces intermédiaires de données fonctionneront comme des organisateurs dignes de confiance du partage des données. Afin de renforcer la confiance dans le partage des données, cette approche établit un modèle basé sur la neutralité et la transparence des intermédiaires de données tout en donnant aux personnes et aux entreprises le contrôle de leurs données.

Les entités souhaitant fournir des services d'intermédiation de données doivent :

- *respecter des exigences strictes pour garantir la neutralité et éviter les conflits d'intérêts ;*
- *être structurellement séparées de tout autre service à valeur ajoutée fourni ;*
- *avoir des conditions tarifaires indépendantes du fait que le détenteur de données* ou l'utilisateur de données* potentiel utilise d'autres services; et*
- *s'enregistrer auprès d'une autorité compétente.*

Altruisme en matière de données

Il y a altruisme en matière de données lorsque des personnes et des entreprises donnent leur consentement ou leur autorisation pour mettre à disposition les données qu'elles génèrent en vue de leur utilisation dans l'intérêt public, volontairement et sans contrepartie. Ces données ont un énorme potentiel pour faire avancer la recherche et développer de meilleurs produits et services, notamment dans les domaines de la santé, de l'action climatique et de la mobilité. Les États membres peuvent développer des politiques nationales pour encourager l'altruisme en matière de données, et une entité engagée dans l'altruisme en matière de données peut demander à être enregistrée comme «organisation altruiste en matière de données reconnue dans l'Union». La Commission tiendra un registre de ces organisations au niveau de l'UE.

Comité européen de l'innovation dans le domaine des données

La Commission mettra en place l'EDIB, qui sera composé de représentants :

- *des autorités nationales désignées dans le cadre de l'AGD ;*
- *du Comité européen de la protection des données;*
- *du Contrôleur européen de la protection des données;*
- *de l'Agence de l'Union européenne pour la cybersécurité;*
- *du Représentant de l'UE pour les PME; et*
- *d'autres secteurs et organismes spécifiques disposant d'une expertise particulière.*

Les tâches de l'EDIB consistent notamment à conseiller et à assister la Commission dans les domaines suivants :

- *le développement d'une pratique cohérente dans le traitement des demandes de réutilisation des données ;*
- *l'amélioration de l'interopérabilité des données et des services de partage de données ;*

- *le développement d'une pratique cohérente des autorités compétentes dans la mise en vigueur des exigences applicables aux prestataires de services d'intermédiation de données*.*

Flux de données internationaux

Les données à caractère non personnel pouvant avoir une valeur économique considérable, l'AGD introduit des garanties pour protéger ces données contre tout accès illicite par les autorités des pays tiers.

3. Au niveau national les conditions applicables à l'accès et à la réutilisation des données détenues par les organismes du secteur public doivent être précisées.

Ces conditions doivent être non discriminatoires, transparentes, proportionnées et objectivement justifiées en ce qui concerne les catégories de données et les finalités de la réutilisation, ainsi que la nature des données pour lesquelles la réutilisation est autorisée.

Le présent projet de loi, qui doit ainsi se lire conjointement avec le règlement (UE) 2022/868, complète par conséquent ce cadre européen par les dispositions nationales qui s'imposent, en particulier concernant :

- la désignation des organismes compétents,
- la procédure à suivre pour l'octroi des autorisations d'accès et de réutilisation des données, et
- les conditions applicables à l'accès et à la réutilisation des données.

4. Le **Commissariat du gouvernement à la protection des données auprès de l'État** est désigné comme **« Autorité des données »** centralisée conformément au règlement (UE) 2022/868.

Il sera l'organisme compétent pour octroyer ou refuser les accès et les réutilisations des données détenues par les organismes du secteur public.

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

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

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

Le Centre a ainsi notamment pour missions :

- de mettre à disposition un environnement de traitement sécurisé tel p.ex. restreindre le nombre de personnes pouvant accéder aux données, tenir un registre des accès etc.
- de fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles ;
- de s'assurer de la mise en œuvre des mesures d'anonymisation et de pseudonymisation des données à caractère personnel et/ou à de modification, d'agrégation, de suppression et de traitement des informations et données.

Le **LNDS** a notamment pour missions :

- d'aider les organismes du secteur public à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données ;
- de fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur.

Le Centre et le LNDS veillent notamment à ce que leur personnel soit fonctionnellement indépendant des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données. Ils doivent désigner leur personnel sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel. Ils doivent aussi veiller à ce que ce personnel n'exerce aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui leurs sont conférés par la future loi. Il est interdit au personnel du Centre et du LNDS chargé de l'exécution des missions qui leurs sont conférées par la future loi d'avoir un intérêt quelconque, par lui-même ou par personne interposée, et sous quelque forme juridique que ce soit, dans une entité publique, dans un organisme du secteur public détenant les données ou dans un réutilisateur de données.

6. Pour éviter d'éventuels conflits d'intérêts et pour maintenir la confiance des citoyens dans une gestion prudente de leurs données par les acteurs publics, la loi prévoit la possibilité pour le Centre des technologies de l'information de l'État de recourir aux services d'un **tiers de confiance** qui doit être une **entité fonctionnellement indépendante des entités publiques, des organismes du secteur public détenant les données et du réutilisateur de données.**

Le tiers de confiance a notamment pour missions

- d'effectuer des opérations de sécurité d'authentification, de transmission et de stockage d'informations permettant la réidentification, y compris, le cas échéant, l'anonymisation, la pseudonymisation et l'agrégation des données, ainsi que la gestion des clés d'anonymisation, de pseudonymisation et d'agrégation des données ;
- de collaborer étroitement avec l'Autorité des données, le Centre et le LNDS.

Le tiers de confiance doit disposer de ressources humaines et techniques suffisantes et de l'expertise adéquate pour s'acquitter efficacement des missions dont il est chargé.

Il ne doit divulguer aucune information à un tiers permettant l'identification des personnes concernées, des personnes physiques ou morales, des entités publiques, des organismes du secteur public détenant les données et des réutilisateurs de données, ou susceptible de porter préjudice aux droits à la protection des données, à la propriété intellectuelle, à la confidentialité commerciale, y compris le secret d'affaires, au secret professionnel, au secret d'entreprise et au secret statistique.

Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles informations et ce pour les informations sur lesquelles porte cette habilitation.

Son personnel doit être désigné sur la base des qualités professionnelles et, en particulier, des connaissances spécialisées en matière d'anonymisation et de pseudonymisation de données à caractère personnel et de modification, d'agrégation, de suppression et de traitement.

Ce personnel ne doit pas être chargé ou impliqué, de manière directe ou indirecte, dans le traitement ultérieur de données à caractère personnel ainsi que dans l'accès et la réutilisation de données. Et ce personnel ne doit exercer aucune activité qui ne se concilie pas avec l'accomplissement consciencieux et intégral des devoirs qui lui sont conférés.

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

7. En complément du règlement (UE) 2022/868, et afin de faciliter la mise en œuvre de traitements ultérieurs de données dans le secteur public, le projet de loi énonce les **finalités pour lesquelles le traitement ultérieur de données à caractère personnel est autorisé** et précise que les traitements de données opérés par les **entités publiques en lien avec l'exécution des missions d'intérêt public** ou relevant de l'exercice de l'autorité publique leurs conférées sont fondés sur **l'article 6, paragraphes 1, point e) et 3 du règlement (UE) 2016/679.**

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

Selon le projet de loi, est une **« entité publique »** : un Ministère, y compris ses services, une administration ou une commune luxembourgeoise, ainsi que les établissements publics luxembourgeois, les groupements d'intérêt économique et les personnes morales d'utilité publique listés expressément par règlement grand-ducal.

La CSL regrette que le règlement grand-ducal ne soit pas encore disponible afin de pouvoir être analysé en même temps que le projet de loi.

8. Sous l'autorité du ministre ayant la digitalisation dans ses attributions est instauré un **point d'information unique** conformément à l'article 8 du règlement (UE) 2022/868.
Le point d'information unique a pour missions :

- de recevoir les demandes d'accès et de réutilisation de données, de les transmettre électroniquement, le cas échéant par des moyens automatisés, à l'Autorité des données et d'assurer les échanges et les démarches nécessaires;
- de rendre disponibles au public toutes les informations pertinentes concernant la mise à disposition des données par les entités publiques (en application des articles 5 et 6 du règlement (UE) 2022/868) ainsi que toute autre information dont la publication est sollicitée par l'Autorité des données ;
- de mettre à disposition par voie électronique une liste des ressources consultable contenant un aperçu de toutes les ressources en données disponibles à l'accès et à la réutilisation de données, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

9. Il est en outre institué, sous l'autorité du ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions, un **Conseil consultatif de la valorisation des données dans un environnement de confiance, appelé le « Conseil consultatif** ».

Il a pour mission :

- de fonctionner comme organe consultatif de l'Autorité des données ;
- de soumettre un avis motivé dans les cas où ce dernier est sollicité ;
- de se prononcer sur toute question en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données qui lui est soumise par le ministre ayant le Commissariat du Gouvernement à la protection des données auprès de l'État dans ses attributions ;
- de promouvoir l'accès et la réutilisation des données.

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

10. Dans un objectif de rendre plus rapides et plus efficaces les procédures pour les citoyens et les entreprises, le projet de loi instaure également le **principe du « once only »**, qui constitue une priorité du Gouvernement, et selon lequel **une personne fournit une seule fois des données aux autorités, au lieu de devoir le faire à plusieurs reprises.**

Le système proposé a pour but de faire économiser du temps, des ressources et de l'argent à tous les acteurs concernés, qu'il s'agisse des citoyens, des entreprises ou de l'administration publique.

Le système « once only » constitue ainsi selon les auteurs du projet, une vraie mesure de simplification administrative qui permettra de diminuer les dépenses et favorisera une gestion plus efficace des ressources des entités publiques.

Ce principe du « once only » impliquera qu'un administré présentant une demande ou produisant une déclaration à une entité publique ne peut être tenu de produire des informations ou des données à caractère personnel que celle-ci détient déjà ou qu'elle peut obtenir auprès d'une autre entité publique.

Les entités publiques échangent entre elles toutes les informations ou les données à caractère personnel nécessaires pour traiter une demande présentée par l'administré ou une déclaration présentée par celui-ci en application d'une disposition législative ou réglementaire. Elles échangent aussi entre elles les informations ou les données à caractère personnel nécessaires pour pouvoir informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévu par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

Lorsque les informations ou données à caractère personnel nécessaires pour traiter la demande présentée par l'administré ou la déclaration présentée par celui-ci doivent être obtenues auprès d'une autre entité publique, l'administré certifie l'exactitude des informations et des données à caractère personnel ainsi obtenues.

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

L'entité publique ne sollicite pas l'échange d'informations et de données à caractère personnel auprès d'une autre entité publique s'il est manifeste qu'elle n'est pas compétente pour traiter la demande de l'administré.

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

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

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

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

Le projet de loi prévoit qu'un règlement grand-ducal détermine les informations ou données à caractère personnel, qui en raison de leur nature, ne peuvent faire l'objet de ces échanges entre entités publiques.

La CSL constate et regrette que ce projet de règlement grand-ducal fait malheureusement encore défaut.

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

- dans le cadre du traitement effectué dans l'exercice de leurs missions des demandes et déclarations présentées par un administré ;
- pour informer les administrés sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou réglementaires et pour pouvoir leur attribuer éventuellement lesdits prestations ou avantages.

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

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

- certifient la disponibilité des informations et des données à caractère personnel à l'entité publique demanderesse et confirment que l'échange d'informations et de données à caractère personnel n'est pas impossible
- ou informent l'entité publique demanderesse du fait qu'elles ne détiennent pas les informations et les données à caractère personnel sollicitées ou que l'échange d'informations et de données à caractère personnel est impossible.

Une copie de l'information visée ci-avant est transmise au ministre ayant la digitalisation dans ses attributions.

11. Chaque type d'échange d'informations et de données à caractère personnel est formalisé dans un **protocole signé entre les entités publiques concernées préalablement à l'échange des informations et des données à caractère personnel**.

Le protocole contient, au moins, les éléments suivants :

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

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

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

4° 4° une description détaillée des catégories de personnes concernées ;

5° 5° une description détaillée des finalités du traitement ;

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

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

Tout changement des éléments liés à l'obtention des informations et des données à caractère personnel auprès d'une entité publique doit être formalisé par avenant du protocole.

Le protocole ainsi que tout avenant sont transmis sans délai à l'Autorité des données qui les publie par voie électronique pour une durée de 2 ans. Les entités publiques informent sans délai l'Autorité des données lorsqu'un protocole n'est plus applicable.

12. L'Autorité des données tient un **registre de tous les protocoles** qui lui sont transmis pour publication.

13. Le **traitement ultérieur de données à caractère personnel** par des entités publiques est autorisé si le traitement des données à caractère personnel est effectué exclusivement pour une ou plusieurs des finalités suivantes :

- **l'analyse statistique ;**
- **les activités d'éducation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;**
- **la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;**
- **l'évaluation et la planification des politiques envisagées ou planifiées par le Gouvernement et approuvées par décision du Gouvernement en conseil, ou en ce qui concerne les communes, envisagées ou planifiées par le Conseil communal ;**
- **lorsque la mise en œuvre d'un accord international requiert la communication d'informations ou lorsque le traitement ultérieur des données à caractère personnel permet de répondre aux demandes d'informations officielles provenant de gouvernements étrangers ou d'organisations internationales approuvées par décision du Gouvernement en conseil ;**
- **les activités de développement, d'évaluation, de démonstration, de sécurité et d'innovation de dispositifs ou de services ;**
- **la formation, le test et l'évaluation d'algorithmes, y compris dans les dispositifs, les systèmes d'intelligence artificielle et les applications numériques.**

Le traitement ultérieur des données à caractère personnel, y compris leur partage et leur mise à disposition, par les entités publiques doit en outre être licite au sens de l'article 6, paragraphe 1er, lettre e) (mission d'intérêt public) et, si applicable, de l'article 9 (données sensibles), paragraphe 2, lettre g) (mission d'intérêt public) ou j) (santé publique) du règlement (UE) 2016/679.

14. Les données à caractère personnel détenues par des entités publiques doivent être **anonymisées préalablement à leur traitement ultérieur** aux fins énoncées ci-avant.

Lorsque le traitement de données anonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel doivent être **pseudonymisées préalablement à leur traitement ultérieur.**

Et lorsque le traitement ultérieur de données à caractère personnel pseudonymisées ne permet pas d'atteindre la finalité poursuivie, les données à caractère personnel peuvent être traitées ultérieurement de manière nonpseudonymisées dans les limites du strict nécessaire.

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

16. L'**accès et la réutilisation, par un réutilisateur, des données détenues par des organismes du secteur public**, **vise,** conformément au règlement (UE) 2022/868, les **données qui sont protégées pour des motifs :**

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

2° de secret statistique ;

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

4° **de protection des données à caractère personnel**.

L'accès et la réutilisation des données par des réutilisateurs sont autorisés si l'accès et la réutilisation des données est effectué exclusivement pour une ou plusieurs des **finalités suivantes** :

- **l'analyse statistique ;**
- **les activités d'éducation, de formation ou d'enseignement, y compris au niveau de l'enseignement professionnel ou supérieur ;**
- **la recherche scientifique dans l'intérêt public ou dans l'intérêt général ;**
- **le développement, l'évaluation, la démonstration, la sécurité et l'innovation de technologies ;**
- **le développement, l'évaluation, la démonstration, la sécurité et l'innovation de produits ;**
- **l'évaluation des politiques publiques luxembourgeoises ou européennes**

17. Le projet de loi précise également les conditions endéans lesquelles la réutilisation est possible. Ainsi les données à caractère personnel détenues par des organismes du secteur public doivent notamment être **anonymisées, sinon pseudonymisées,** préalablement à l'accès et à la réutilisation par le réutilisateur de données.

18. La réutilisation de données nécessite en outre l'**accord de l'Autorité des données**.
Les demandes de traitement ultérieur de données à caractère personnel ainsi que les demandes d'accès et de réutilisation à présenter à l'Autorité des données doivent être formulées de façon précise et revêtir une **forme écrite**. Le projet de loi précise les informations qui doivent être fournies par le demandeur dans sa demande.
L'Autorité des données statue ensuite dans un délai de 2 mois à compter du dépôt de la demande.

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

20. En ce qui concerne les **services d'intermédiation de données** (Chapitre III du règlement (UE) 2022/868), la **Commission nationale pour la protection des données (CNPD)** est l'autorité compétente pour effectuer les tâches liées à la procédure de notification, telle que visée à l'article 13 du règlement (UE) 2022/868. Un règlement interne de la CNPD définira la procédure en matière de notification pour les services d'intermédiation de données.

La CNPD pourra imposer des **redevances proportionnées et objectives** pour la notification des services d'intermédiation. Un règlement de la CNPD déterminera le montant et les modalités de paiement de ces redevances.

Dans le cadre d'une violation de l'obligation de notification incombant aux prestataires de services d'intermédiation de données ou des conditions liées à la fourniture de services d'intermédiation de données, la CNPD peut, par voie de décision, imposer des amendes administratives à hauteur de 500 à 100.000 euros aux prestataires de services d'intermédiation de données.

La CNPD pourra aussi infliger au prestataire de services d'intermédiation de données des astreintes jusqu'à concurrence de 250 euros par jour de retard à compter de la date qu'elle fixe dans sa décision, pour le contraindre à communiquer toute information demandée par la CNPD ou à respecter une demande de cessation prononcée.

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

22. Un **projet de règlement grand-ducal** complète le projet de loi. Il prévoit la composition, le mode de fonctionnement et les attributions du Conseil consultatif de la valorisation des données dans un environnement de confiance et il précise les règles relatives au calcul et à la perception des redevances lesquelles ne doivent pas dépasser le montant des coûts réels liés au mécanisme de réutilisation des données.

***

23. La CSL marque son accord au présent projet de loi et de règlement grand-ducal.

Luxembourg, le 23 octobre 2024

Pour la Chambre des salariés,

Sylvain HOFFMANN
Directeur

Nora BACK
Présidente

L'avis a été adopté à l'unanimité.