Avis

Mise en œuvre de certaines dispositions du Data Act

Luxembourg, le 28 juillet 2025

Ce document présente les recommandations de la FEDIL, The Voice of Luxembourg's Industry, en vue de la mise en œuvre de certaines dispositions du règlement (UE) 2023/2854[1] du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données, ci-après « Data Act »)

A. Introduction et commentaires de fond

Le Data Act constitue un texte majeur de la stratégie européenne pour les données, visant à stimuler une économie des données équitable et dynamique en Europe. Il établit des règles harmonisées sur l'accès, le partage et l'utilisation des données générées par les objets connectés dans l'Union européenne, afin de lever les potentielles barrières et d'encourager l'innovation tout en protégeant les intérêts légitimes des entreprises (secrets des affaires, protection des données à caractère personnel, etc.). Entré en vigueur en janvier 2024, il sera pleinement applicable à partir de septembre 2025.

Le Data Act part du postulat qu'une meilleure circulation des données libèrera le potentiel de l'économie des données. En permettant aux utilisateurs et aux entreprises tierces d'accéder aux données générées par les objets connectés, l'émergence de nouveaux services à valeur ajoutée est facilitée et l'innovation stimulée. Pour le Luxembourg, positionné comme une « data -driven economy », cela peut se traduire par l'attraction de nouvelles activités basées sur les données et la mise en place de nouveaux modèles économiques. Des secteurs comme la FinTech, la logistique, la mobilité intelligente ou l'IoT industriel pourraient particulièrement bénéficier d'un accès facilité aux données parfois enfermées dans des silos propriétaires.

La mise en œuvre de certaines dispositions du Data Act ne se limite pas à une question réglementaire. Elle entraînera des répercussions économiques significatives pour le Luxembourg, tant positives que sous forme de défis à relever. À ce titre, la FEDIL estime qu'il est nécessaire de situer la gouvernance proposée dans une perspective plus large de compétitivité et d'innovation du pays.

Exécuté avec succès, le Data Act détient le potentiel de renforcer la compétitivité de l'économie luxembourgeoise en favorisant l'innovation, en abaissant certaines barrières potentielles à l'entrée pour les petites entreprises et en ouvrant la voie à de nouvelles opportunités de marché. Toutefois, un accompagnement soutenu et collaboratif ainsi qu'une mise en œuvre intelligente seront nécessaires pour éviter des effets négatifs transitoires (coûts, complexité, incertitudes sur les secrets des affaires). En d'autres termes, la gouvernance nationale proposée ne servira son propos que si elle intègre ce double impératif : appliquer la loi tout en éduquant et soutenant les acteurs économiques dans cette transition vers une économie plus ouverte des données. La FEDIL insiste donc pour que l'autorité compétente joue également un rôle de facilitateur économique, par exemple en consultant régulièrement les organisations professionnelles sur les difficultés rencontrées, en calibrant finement les sanctions, et en valorisant les « success stories » d'innovation permises par le Data Act au Luxembourg.

[1] https://eur-lex.europa.eu/eli/reg/2023/2854/oj?locale=fr

7, rue Alcide de Gasperi - Luxembourg-Kirchberg
P.O. Box 1304 – L-1013 Luxembourg
fedil@fedil.lu – tél. : (+352) 43 53 66-1 - www.fedil.lu

B. Analyse préliminaire

1) Exigences en matière de gouvernance

Parmi ses dispositions, l'article 37 du Data Act revêt une importance particulière, car il oblige chaque État membre à désigner une ou plusieurs autorités nationales compétentes chargées de veiller au respect du règlement sur son territoire. Cet article fixe les principes directeurs du cadre que chaque pays doit mettre en place pour l'application nationale du règlement. En outre, il stipule que si plusieurs autorités sont désignées, un coordinateur national des données doit être nommé pour servir de point de contact unique et assurer la coopération entre elles. Cet article impose donc la mise en place d'une architecture de gouvernance nationale claire, efficace et coordonnée. Ses principales exigences peuvent être résumées comme suit :

- Désignation d'autorités compétentes : Chaque État membre doit désigner *une ou plusieurs autorités compétentes* chargées de veiller à l'application et au respect du Data Act. Il est possible de s'appuyer sur des entités existantes ou d'en créer de nouvelles, du moment que l'ensemble des missions définies par le règlement est couvert sans lacune. En d'autres termes, toutes les obligations et droits introduits par le Data Act (du partage des données IoT au changement de fournisseur de cloud) doivent être placés sous la surveillance d'une instance nationale identifiée.

- Coordinateur national des données (« data coordinator ») : Si plusieurs autorités sont désignées, l'État membre doit nommer parmi elles un *coordinateur national des données*. Ce coordinateur sert de point de contact unique pour toutes les questions relatives au Data Act dans le pays et facilite la coopération inter-agences. L'objectif est qu'une entité concernée (détenteur des données, utilisateur des données, tiers, entreprise, citoyen, Commission européenne, autorité étrangère) puisse s'adresser à un guichet unique pour toute requête relative au Data Act, le coordinateur se chargeant ensuite de répartir ou relayer la demande au bon interlocuteur. Cette exigence vise à éviter le piège d'une fragmentation bureaucratique et à assurer une vue d'ensemble nationale claire et facilement compréhensible pour l'ensemble des acteurs concernés.

- Rôle de l'autorité de protection des données à caractère personnel : Pour les aspects relatifs à *la protection des données à caractère personnel*, le Data Act consacre la compétence inchangée des autorités de protection des données qui restent responsables de veiller à ce que l'application du Data Act respecte le Règlement Général sur la Protection des Données[2] (ci-après « RGPD »), en s'appuyant sur leurs pouvoirs et procédures habituels. Le texte garantit ainsi qu'il n'y aura pas de double autorité sur la matière personnelle et que l'autorité existante reste le gendarme des données personnelles, y compris dans le contexte du partage de données encadré par le Data Act.

- Respect des compétences sectorielles existantes : Le règlement précise que les compétences des *autorités sectorielles existantes* doivent être respectées pour les questions spécifiques relevant de leur domaine. Par exemple, si le Data Act s'applique à des données du secteur de la santé ou de la finance, les régulateurs existants dans ces domaines doivent

[2] https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr

pouvoir conserver un rôle d'expertise ou de support. De plus, l'article 37(4) stipule que l'autorité chargée des dispositions relatives aux services de traitement de données (c'est-à-dire le cloud et l'interopérabilité, chapitres VI-VII du règlement) dispose d'une expérience avérée en matière de données et de communications électroniques.

- Indépendance et ressources : Comme dans de nombreux règlements récents, le Data Act requiert que les autorités désignées agissent en toute impartialité, à l'abri de toute influence extérieure indue, et qu'elles disposent des ressources (humaines, techniques, financières) suffisantes pour exercer leurs missions. L'article 37(8) impose aux États membres de garantir cette indépendance et de doter les autorités compétentes de moyens adéquats. Cela peut impliquer d'ajuster le cadre légal national pour renforcer le statut de l'autorité (p.ex. autonomie administrative, protections contre la révocation arbitraire de ses dirigeants) et d'allouer un budget pour recruter du personnel qualifié (technologues de données, juristes spécialisés, etc.).

2) Missions et pouvoirs des autorités

L'article 37(5) dresse une liste détaillée des missions que les États membres doivent confier à leurs autorités compétentes. Parmi ces missions figurent notamment :

- Information et promotion de la conformité : Les autorités doivent sensibiliser les acteurs (entreprises, utilisateurs, administrations) aux nouvelles règles du Data Act. Cela peut passer par la publication de guides pratiques, de FAQ, l'organisation de séminaires, etc., pour expliquer par exemple aux fabricants leurs obligations de partage de données, ou aux PME leurs nouveaux droits. L'approche doit être proactive pour encourager une mise en conformité volontaire.

- Réception des plaintes et résolution des litiges : Tout intéressé (utilisateur d'un produit connecté, entreprise tierce, etc.) doit pouvoir déposer plainte s'il estime qu'une obligation du Data Act n'est pas respectée (p. ex. un refus injustifié de lui donner accès aux données qu'il devrait pouvoir obtenir ou la compromission de la confidentialité du secret des affaires). L'autorité enquêtera sur ces plaintes et rendra une décision motivée. Elle doit tenir informé le plaignant de l'avancement de son dossier et de l'issue qui y est apportée.

- Contrôle et enquêtes d'office : Les autorités peuvent agir de leur propre initiative si elles soupçonnent une violation du Data Act, sans attendre qu'une plainte formelle soit déposée. Elles sont dotées pour cela des pouvoirs d'enquête. Par exemple, elles peuvent exiger la communication de documents ou de données, effectuer des inspections sur place (dans le respect du droit national), ou des audits. Cette capacité d'auto-saisine est cruciale pour détecter des manquements systémiques ou des infractions dont les victimes n'ont pas conscience.

- Pouvoir de sanction : L'autorité doit pouvoir imposer *des sanctions effectives, proportionnées et dissuasives* en cas d'infraction constatée. Le Data Act laisse aux législations nationales le soin de fixer les barèmes, mais suggère des amendes administratives et des astreintes journalières en cas de non-respect persistant. Par exemple, une entreprise refusant de donner accès aux données pourrait se voir infliger une amende,

et si elle persiste après mise en demeure, une astreinte (amende par jour de retard) pourrait courir jusqu'à exécution. L'autorité peut aussi initier des actions en justice pour faire prononcer des sanctions par les tribunaux compétents.

- Surveillance des évolutions technologiques et commerciales : L'autorité doit garder un œil sur le contexte évolutif, les nouvelles technologies pour la mise à disposition et l'utilisation des données, les pratiques émergentes de marché. Par exemple, suivre l'apparition de nouveaux formats de données dans l'IoT, ou l'évolution des offres cloud, afin d'anticiper les enjeux d'interopérabilité. Cette veille permet d'adapter l'application du règlement et d'émettre des recommandations ou lignes directrices actualisées.

- Coopération nationale et européenne : L'article 37(5) insiste sur la coopération à plusieurs niveaux. Au niveau national, entre les diverses autorités compétentes et avec les autres régulateurs concernés pour assurer une application cohérente avec les autres législations (RGPD, lois sectorielles, etc.). Au niveau européen, avec les autorités homologues des autres États membres et la Commission européenne ; notamment via la participation au European Data Innovation Board (EDIB), le comité européen prévu par le Data Act, pour échanger sur les bonnes pratiques et conseiller la Commission. Ainsi, l'autorité luxembourgeoise devra contribuer aux discussions européennes sur les cas transfrontaliers ou l'élaboration de standards communs.

- Mise en œuvre des dispositions spécifiques : L'autorité doit veiller au respect de dispositions précises du règlement, par exemple : la suppression progressive des frais de changement de fournisseur de cloud d'ici 2027, la bonne exécution des demandes d'accès aux données par les organismes publics en situation d'exception d'urgence (chapitre V) et l'examen des refus éventuels des entreprises de partager des données pour motif valable.

Ces exigences légales encadrent la conception de l'architecture de gouvernance nationale. Elles justifient notamment la création d'un data coordinator et la définition de rôles complémentaires entre autorités, afin de couvrir toutes les missions précitées sans vide ni chevauchement.

3) Enjeux relatifs au choix des autorités compétentes

La FEDIL estime qu'il est nécessaire de prendre en compte plusieurs enjeux nationaux dans l'application du Data Act au Luxembourg : l'existence d'autorités réglementaires déjà en place dans divers domaines ainsi que la nécessité de ne pas alourdir inutilement la charge administrative pour les entreprises. La FEDIL propose de considérer initialement deux grands modèles théoriques de gouvernance : un *modèle centralisé* vs. un *modèle distribué*, mais la solution optimale pourra combiner des éléments des deux.

a) Modèle « Autorité Unique » (Centralisé) vs. « Autorités Multiples » (Distribué)

- Option A : Une autorité unique polyvalente

Une approche consisterait à confier toutes les missions du Data Act (hormis celles relevant du RGPD) à une seule entité nationale qui agirait à la fois comme autorité compétente et coordinateur.

Avantage : Cela apporte une simplification substantielle du point de vue des acteurs économiques, qui n'auraient qu'un guichet unique pour toutes leurs questions ou démarches liées au Data Act. Cela garantirait également une interprétation uniforme des règles.

Inconvénient : Aucune autorité luxembourgeoise actuelle n'a, à elle seule, l'ensemble des compétences requises pour couvrir tous les chapitres du Data Act (aspects techniques IoT, règles sectorielles, cloud…). Doter une autorité unique de toutes ces expertises supposerait un effort considérable de recrutement et de formation. De plus, isoler complètement le sujet au sein d'une seule structure pourrait la priver de l'appui d'autres organismes spécialistes (risque de *silo*), notamment si le processus d'interaction entre les différentes autorités n'est pas soigneusement élaboré.

- Option B : Plusieurs autorités spécialisées

À l'inverse, une autre option pourrait s'appuyer sur plusieurs autorités existantes, chacune intervenant sur la partie du Data Act relevant de son savoir-faire sectoriel, avec un coordinateur pour centraliser les informations.

Avantage : Cette option propose de capitaliser sur l'expertise de chaque secteur. Chaque régulateur connaît bien les acteurs et enjeux de son domaine, ce qui favorise une application éclairée. Le Luxembourg a adopté une telle logique dans le projet de loi transposant le Règlement sur l'IA (répartition des tâches entre CNPD, ILR, CSSF, ILNAS…), avec la CNPD comme point de contact unique.

Inconvénient : Cela peut entraîner une certaine complexité pour les acteurs économiques s'ils devaient identifier plusieurs interlocuteurs selon la nature de leurs données. Sans une coordination rigoureuse, le risque de dédoublements d'actions ou des divergences d'approche ou d'interprétation entre autorités peut survenir.

b) Couverture de l'éventail des sujets du Data Act

Le Data Act comporte plusieurs chapitres aux thématiques assez variées (partage de données IoT en B2B2C, accès des pouvoirs publics en cas d'urgence, portage et changement de fournisseur cloud, normes d'interopérabilité, etc.). Chaque thème pourrait entraîner des enjeux de gouvernance spécifiques.

En partant du constat que le Data Act est une réglementation transversale et qu'il touche à un large éventail de secteurs et de situations, la FEDIL est d'avis qu'aucune de ces deux options extrêmes ne semble pleinement satisfaisante isolément. Les enjeux de gouvernance consisteront donc à allier la clarté pour les usagers (ils doivent savoir à qui s'adresser) et l'efficacité technique (attribuer chaque mission à l'organisme le mieux placé). Une autorité unique aurait la simplicité pour les usagers, mais serait difficile à outiller en compétences multiples. Plusieurs autorités spécialisées apporteraient l'expertise, mais pourraient semer la confusion s'il n'y a pas un front uni vers l'extérieur.

C. Le modèle de gouvernance

1) Vers un modèle "hybride" centralisé-collaboratif

La FEDIL insiste sur l'importance de désigner un interlocuteur national clairement identifiable que ce soit sur le plan national ou international. Le principe du guichet unique ("single point of contact") est pratiquement un impératif pour un petit État comme le Luxembourg. En effet, il faut éviter de "saucissonner" les guichets administratifs. Un chef d'entreprise ou une start-up qui cherche de l'aide ne doit pas se perdre dans un labyrinthe d'autorités. Dans cette optique, la FEDIL recommande de ne pas créer de nouvelle structure ex nihilo si l'on peut s'en passer, mais plutôt de renforcer une entité existante qui servirait de pivot. Cela évitera de multiplier les entités dans un paysage administratif déjà restreint.

Par ailleurs, le Luxembourg dispose déjà de plusieurs autorités aux compétences pointues. Par exemple, l'ILR maîtrise les sujets de communications électroniques ; la CNPD a une expertise inégalée en matière de protection des données à caractère personnel ; la CSSF connaît bien la réglementation du secteur financier, etc. Or, le Data Act couvre des thématiques parfois très techniques (données des produits connectés (chap. II) et accès des utilisateurs, obligations contractuelles loyales (chap. III-IV), demandes d'accès des autorités publiques en situation d'urgence (chap. V), changement de fournisseur cloud (chap. VI) et interopérabilité (chap. VIII)). La FEDIL trouverait judicieux de mettre à contribution ces gisements d'expertise existants plutôt que de repartir de zéro. Cela permettra aux décisions prises d'être bien informées des réalités de chaque secteur.

Quelle que soit l'architecture retenue, le succès reposera sur une coordination forte et la coopération fluide entre les acteurs. Il faudra également penser au flux d'informations. Par exemple, si une entreprise invoque le secret des affaires pour refuser de partager des données, elle doit notifier l'autorité nationale qui, elle, doit en faire rapport annuel à la Commission. Qui tiendra ce registre et compilera ces rapports ? Probablement le coordinateur national, d'où l'importance de bien centraliser. Une coordination solide constitue donc la clef de voûte pour qu'un modèle à acteurs multiples fonctionne comme un tout cohérent.

Les entreprises attendent une mise en œuvre pragmatique et non bureaucratique du Data Act. Elles craignent les démarches complexes autant que l'insécurité juridique. Une gouvernance bien calibrée peut transformer le Data Act en opportunité (en ouvrant l'accès à de nouvelles données) plutôt qu'en contrainte.

Il est crucial de définir une organisation claire pour les usagers (minimalement fragmentée vers l'extérieur), compétente techniquement (mobilisant le savoir-faire des régulateurs existants), et efficiente et faisant preuve d'innovations sans sacrifier la rigueur.

2) Choix du modèle de gouvernance

À la lumière des analyses précédentes, la FEDIL invite le gouvernement à privilégier une architecture hybride, articulée autour d'une autorité principale renforcée, combinant une centralisation du pilotage et une collaboration structurée avec les autorités sectorielles.

Concrètement, cela consisterait en désigner une autorité principale qui sera le visage public du Data Act (guichet unique), tout en faisant participer d'autres autorités compétentes à l'instruction des cas qui touchent à leur domaine d'expertise. Cette approche offrirait la lisibilité d'un point de contact unique pour les entreprises, tout en assurant que derrière ce point de contact, les bonnes compétences sont mobilisées selon la nature du problème.

Nous établissons ci-dessous les piliers de ce modèle :

1. **Désigner une autorité nationale principale** qui jouerait le rôle d'autorité compétente centrale pour l'ensemble du Data Act (hors aspects relevant exclusivement des données à caractère personnel au sens du RGPD, pour lesquelles les autorités chargées de l'application du RGPD continueront à surveiller la mise en œuvre du Data Act conformément à l'article 37) et de coordinateur national des données au sens de l'article 37. Cette entité serait le guichet unique et le chef d'orchestre de la gouvernance.
2. **Impliquer les autorités existantes pertinentes** via des mécanismes de coopération clairement définis. Ces autorités ne seraient pas destinataires directes des plaintes, mais agiraient en soutien expert de l'autorité principale pour les cas qui touchent leur domaine de compétence.
3. **Renforcer les moyens (ressources, compétences) de l'autorité principale** afin qu'elle puisse s'acquitter efficacement de ses nouvelles missions, et formaliser par écrit (loi, conventions) les modalités d'interaction entre tous les acteurs de cette gouvernance.

D. Désignation des autorités compétentes

1) Potentiels défis entre le mandat principal de la CNPD et le rôle d'autorité centrale

Compte tenu des spécificités du Data Act, la CNPD pourrait être désignée comme autorité principale pour la mise en œuvre du Data Act. Cependant, la FEDIL estime que la CNPD ne semble pas être l'autorité la plus adéquate pour assumer seule le rôle d'autorité centrale dans sa mise en œuvre. Avis que nous émettons tout en ayant pris note qu'elle est, en l'état, l'autorité compétente par défaut dans le cadre de la mise en œuvre de l'IA Act. Nous expliquons ci-après pour quelles raisons par l'analyse de son mandat actuel, les missions prévues par l'article 37 du Data Act et les écarts entre les deux.

a) Les exigences du Data Act

La CNPD joue un rôle essentiel dans l'écosystème réglementaire luxembourgeois en tant qu'autorité administrative indépendante chargée de veiller au respect de la législation en matière de protection des données à caractère personnel. Son action, fondée sur la loi du 1er août 2018 transposant le RGPD, est centrée sur la défense des droits fondamentaux des individus. Elle traite les plaintes des citoyens, ou encore contrôle la conformité des traitements opérés par les entités publiques et privées. Son expertise juridique est solidement ancrée dans les domaines de la protection et de la sécurité des données personnelles.

Toutefois, le champ d'application du Data Act s'étend bien au-delà de la seule sphère des données à caractère personnel. Il vise à encadrer les données, personnelles et non personnelles, en tant que ressource économique, à réguler les échanges entre entreprises, à faciliter le changement de fournisseurs de services cloud, à favoriser l'innovation et à garantir une concurrence équitable. Ces objectifs appellent des compétences pluridisciplinaires : juridiques (droit des contrats, de la concurrence, de la consommation, protection du secret des affaires), techniques (interopérabilité, cybersécurité, protocoles d'accès aux données), et sectorielles (objets connectés, services cloud, etc.). L'autorité compétente devra également être en mesure de dialoguer avec ses homologues européens et avec les entreprises dans des contextes de médiation ou de litiges commerciaux.

Dans ce contexte, il semble apparaître que les missions traditionnelles de la CNPD ne couvrent pas l'ensemble de ces dimensions. Sa culture institutionnelle est orientée vers la protection des personnes et la minimisation des traitements. En même temps, les enjeux du Data Act requièrent une approche plus large, davantage tournée vers l'économie des données.

Par exemple, lorsqu'un utilisateur, qui peut être une personne morale au sens du Data Act, rencontre un refus de la part d'un fabricant de transmettre des données techniques issues d'un produit connecté, le différend relève d'un arbitrage économique et technique. Ce type de situation illustre la nécessité d'une mise en œuvre adaptée aux spécificités du texte. La CNPD pourrait se doter des experts techniques et élargir le champ de ses compétences pour le Data Act, mais il convient de s'interroger s'il n'existe pas une autre autorité qui a déjà des compétences transversales et des experts techniques qui pourrait facilement surveiller la mise en œuvre du Data Act sans avoir des besoins de recrutement supplémentaires.

Si la CNPD assumait le rôle de l'autorité centrale pour la mise en œuvre du Data Act, il est important de noter qu'elle sera déjà mobilisée sur la mise en œuvre de l'AI Act, notamment pour évaluer l'impact des technologies d'intelligence artificielle sur les droits fondamentaux. Dans ce contexte, nous estimons que lui confier simultanément une nouvelle mission aussi vaste et complexe que la mise en œuvre du Data Act pourrait aboutir à diluer ses ressources et nuire à l'efficacité de ses missions principales.

Enfin, il apparaît que certaines dispositions du Data Act, notamment celles du chapitre VI relatives à la facilitation du changement de fournisseur de services cloud et du chapitre VIII relatives à l'interopérabilité des services de traitement des données, s'éloignent encore davantage des compétences traditionnelles d'une autorité de protection des données. Ces sujets relèvent avant tout de considérations techniques et contractuelles liées au fonctionnement du secteur IT et cloud computing, sans lien direct avec la protection des données à caractère personnel.

Dans cette optique, la FEDIL recommande que l'autorité compétente pour la mise en œuvre du Data Act dispose d'une expertise élargie, d'une capacité à appréhender les enjeux économiques, techniques et juridiques dans leur globalité. Une telle approche garantirait une régulation équilibrée, cohérente avec les objectifs du règlement européen, tout en préservant la complémentarité des missions entre les différentes autorités concernées.

b) Compatibilité des différentes missions : les limites potentielles du choix de la CNPD

Les chapitres II et III du Data Act visent à concilier deux objectifs fondamentaux : d'une part, la protection des intérêts légitimes tels que le secret des affaires ou les droits de propriété intellectuelle, d'autre part, la promotion d'un partage élargi, sécurisé et équitable des données. Cette ambition suppose une régulation fine, capable de prendre en compte des enjeux parfois complémentaires, parfois en tension.

Dans ce contexte, il est important de s'interroger sur la manière dont les missions de régulation sont réparties. Confier à une même autorité la responsabilité de la protection des données à caractère personnel (dans le cadre du RGPD) et celle de l'accessibilité et du partage des données (dans le cadre du Data Act) pourrait soulever des défis d'articulation.

Ce type de dilemme souligne l'intérêt d'une répartition claire des rôles entre autorités, afin de garantir une mise en œuvre rapide et efficace et la lisibilité du cadre pour les acteurs économiques. Il s'agit ici de reconnaître que la diversité des objectifs poursuivis par le Data Act appelle une complémentarité d'expertises. Aujourd'hui, une PME identifie clairement la CNPD comme l'interlocuteur pour les questions liées au RGPD. Demain, dans le cadre d'un litige contractuel sur des données industrielles non personnelles, il serait souhaitable qu'elle puisse s'adresser à une autorité spécifiquement compétente sur ces enjeux.

L'article 37 du Data Act prévoit d'ailleurs explicitement que les autorités de protection des données conservent leurs compétences pour les aspects relevant du RGPD. Cela implique la mise en place d'une articulation claire entre le régulateur désigné pour le Data Act et la CNPD en cas de situations mixtes. Cette articulation serait d'autant plus fluide si les rôles étaient bien différenciés dès le départ, permettant à chaque autorité de se concentrer sur son cœur de mission tout en coopérant efficacement.

c) Nécessité d'une expertise technique

La complexité du Data Act requiert des connaissances techniques, car tant pour la mise en œuvre des chapitres II et III que pour la mise en œuvre des chapitres VI et VIII, il faut comprendre le modèle de business, les structures contractuelles et les enjeux des entreprises dans le secteur technologique. C'est pour cela que le Data Act a lui-même requis qu'une autorité ayant des connaissances dans les secteurs des communications électroniques soit compétente pour la mise en œuvre des chapitres VI et VIII. Les experts techniques qui ont une compréhension sur l'architecture et le fonctionnement des réseaux physiques pourraient plus facilement aider les experts juridiques dans l'interprétation du Data Act. Par exemple, même dans le cadre d'une analyse sur la légalité du transfert indirect des données non-personnelles (à travers un API) d'un produit connecté, il faut avoir une bonne compréhension de l'architecture des systèmes facilitant ce transfert ainsi que le fonctionnement de l'infrastructure cloud que le système facilitant le transfert utilise.

Une autorité qui est plus concentrée sur la minimisation du traitement des données personnelles ne va probablement pas avoir les connaissances techniques nécessaires pour la mise en œuvre du Data Act (sans se doter des experts techniques), car pour ses tâches quotidiennes, ces connaissances ne sont pas nécessaires.

C'est dans cette logique que l'Allemagne a choisi (dans le projet de loi sur l'implémentation du Data Act) un modèle hybride : l'autorité de la régulation sectorielle des réseaux (Bundes Netz Agentur) qui a de fortes connaissances techniques sera en charge de la mise en œuvre du Data Act. Elle se concertera avec le BfDI, le Commissariat Fédéral Allemand à la protection des données et à la liberté d'information si, dans le cadre d'une investigation qu'elle va mener, des aspects portant sur la licéité du traitement des données personnelles sont découvertes.

2) L'ILR comme autorité centrale du Data Act

Au regard de tout ce qui précède et après évaluation de la mission des autorités sectorielles qui composent le paysage Luxembourgeois, la FEDIL est d'avis que *l'Institut Luxembourgeois de Régulation (ILR)* ressort comme l'autorité la mieux placée pour répondre aux missions stipulées dans le Data Act. Dès lors, la FEDIL préconise de conférer un double rôle à l'ILR en élargissant son mandat actuel. L'ILR assumerait ainsi deux fonctions essentielles : *(a)* être l'autorité compétente centrale de référence pour la plupart des dispositions du Data Act et (b) être désigné coordinateur national des données.

a) Justifications du choix de l'ILR

- L'ILR possède déjà un large savoir-faire dans la régulation de secteurs techniques. Il est le régulateur historique des communications électroniques (télécoms, Internet), il supervise également d'autres secteurs, et s'est vu confier de nouvelles tâches en matière de cybersécurité (transposition de NIS2) et de médias. Surtout, pour le Data Act, son profil répond à l'exigence d'expérience en communications électroniques afin de traiter le volet cloud et interopérabilité. Aucun autre organisme au Luxembourg n'a autant d'expérience sur les questions de connectivité et de données numériques. Il est donc logique et efficient de tirer parti de cette expertise en désignant l'ILR comme pilier central de la gouvernance du Data Act.

- Du point de vue pratique, l'ILR est une autorité indépendante bien établie, avec une structure collégiale, des services juridiques et techniques internes, et une culture de l'enquête et de la sanction. Il serait plus rapide d'étendre progressivement les compétences de l'ILR (en recrutant les profils manquants) que de créer ex nihilo une nouvelle entité dédiée. Dans un pays de la taille du Luxembourg, il est rationnel de capitaliser sur l'existant plutôt que de disperser les ressources. Il faudra bien sûr fournir à l'ILR les moyens supplémentaires nécessaires, mais cet investissement servira non seulement pour le Data Act, mais aussi pour d'autres régulations numériques futures (*effet de levier*).

- L'ILR a l'habitude de se coordonner avec d'autres entités et de représenter le Luxembourg à l'étranger. Il participe aux réseaux européens de régulateurs (BEREC pour les télécoms, ERGP pour la poste, CEER pour l'énergie, etc.). En lui confiant le rôle de coordinateur national Data Act, on s'assure que le Luxembourg aura une voix expérimentée et crédible au European Data Innovation Board, et dans les coopérations transfrontalières sur des cas impliquant plusieurs pays. De plus, l'ILR a démontré sa capacité à travailler avec la Commission européenne sur des dossiers complexes, ce qui sera un atout pour l'application harmonisée du Data Act.

b) Rôles et prérogatives de l'ILR en tant qu'autorité principale du Data Act

- Point de contact unique : L'ILR deviendrait l'adresse où toutes les questions et plaintes liées au Data Act convergeront. Il mettrait en place un guichet (physique et numérique) dédié. Par exemple une section "Data Act" sur son site web, et éventuellement une ligne téléphonique, pour orienter et renseigner les entreprises et utilisateurs. Toute entité souhaitant déposer plainte, ou signaler un problème (ex : difficulté à changer de fournisseur cloud, refus d'accès à des données d'un produit…), s'adresserait à l'ILR qui enregistrerait la demande. La plateforme SERIMA pourrait servir de base de travail à la création de ce guichet.

- Instruction des dossiers : L'ILR traiterait en interne les cas relatifs aux thèmes du Data Act pour lesquels il peut développer l'expertise. Cela inclut en particulier : le chapitre II (accès aux données des objets connectés et partage aux tiers), le chapitre III (équité des contrats de partage de données entre entreprises, clauses abusives envers les PME), le chapitre V (demandes d'accès aux données émanant des autorités publiques en cas de besoin exceptionnel) et notamment chapitre VI (changement de fournisseur des services cloud). Par exemple, si une PME se plaint de ne pas obtenir les données d'une machine industrielle qu'elle utilise, l'ILR mènera l'enquête, dialoguera avec le fabricant, vérifiera si le refus est justifié ou non, et pourra le cas échéant ordonner la fourniture de ces données. De même, si une autorité publique luxembourgeoise sollicite des données d'entreprise en situation d'urgence (crise sanitaire, inondation…), l'ILR examinera la légitimité de la demande et surveillera sa mise en œuvre, assurant l'interface entre l'organisme public demandeur et l'entreprise détentrice. De même, si un client de services cloud se plaint que son fournisseur n'a pas réduit ses frais de changement de fournisseur ou les a réduits à ses coûts pour une utilisation en parallèle, ou lorsque les autorités nationales doivent apporter leurs contributions à la Commission européenne lors de la sélection des standards d'interopérabilité au titre de l'article 35, l'ILR peut plus facilement s'appuyer sur son expertise actuelle pour effectuer cette évaluation.

- Coordination nationale : En tant que coordinateur, l'ILR établira des procédures de coopération avec les autres autorités impliquées (voir point suivant). Il présidera par exemple un comité de coordination Data Act regroupant des représentants de la CNPD et d'autres régulateurs clés, se réunissant régulièrement pour partager les informations et statuer sur les cas multi-compétences. L'ILR centralisera l'échange d'informations. Par exemple, il consolidera la liste annuelle des refus de partage de données pour cause de secret des affaires à transmettre à la Commission. Il assurera que toutes les autorités luxembourgeoises impliquées appliquent de façon cohérente les orientations européennes reçues via l'EDIB.

- Enquêtes et sanctions : La loi de transposition devra conférer à l'ILR les pouvoirs d'enquête et de sanction nécessaires conformément au règlement. L'ILR pourra alors instruire les dossiers, exiger des documents ou explications des entreprises, réaliser des inspections (le cas échéant avec mandat judiciaire si requis par le droit national), et à l'issue des procédures, prononcer des décisions contraignantes. Celles-ci pourront inclure : des injonctions de se conformer (avec délai), des amendes administratives en cas d'infraction caractérisée, et des astreintes journalières en cas d'inexécution, ainsi que la capacité de clôture des dossiers sans amende et d'accepter des engagements des entreprises concernées par l'enquête. Ces

pouvoirs, exercés avec proportionnalité, donneront du poids aux décisions de l'autorité et inciteront les acteurs à respecter spontanément la loi.

- Interface européenne : L'ILR notifiera officiellement à la Commission européenne sa désignation comme autorité compétente et coordinateur, comme exigé par le Data Act, et fournira les informations de contact. Il participera activement au European Data Innovation Board, et aux éventuelles actions conjointes entre régulateurs (p. ex., enquête coordonnée avec d'autres pays sur une grande plateforme de données opérant dans plusieurs États).

En résumé, l'ILR serait le pivot de la mise en œuvre du Data Act au Luxembourg. Ce choix apparaît comme *« de bon sens et le mieux placé »* malgré l'élargissement significatif de ses tâches actuelles. La FEDIL a conscience qu'aucune autorité ne remplit aujourd'hui 100% des critères, mais en dotant l'ILR des ressources additionnelles et en l'entourant d'expertises, cela aboutirait à une solution robuste et évolutive.

c) Articulation avec la CNPD et les autres autorités compétentes

i. Rôle de la CNPD (données personnelles) : Il est impératif de formaliser l'intervention de la CNPD (Commission Nationale pour la Protection des Données) dans le dispositif, étant donné que le Data Act touche inévitablement à certaines données personnelles. Conformément à l'Article 37(3) du Data Act, la CNPD reste seule compétente pour surveiller l'application du Data Act en ce qui concerne la protection des données personnelles. En pratique, cela signifie :

   - Si une affaire traitée par l'ILR comporte un aspect relatif à des données personnelles, l'ILR devra associer la CNPD au traitement de cet aspect. Par exemple, supposons qu'un utilisateur (personne physique) se plaint que le fabricant de son appareil connecté refuse de lui communiquer certaines données d'utilisation. Cette situation relève à la fois du Data Act (droit d'accès de l'utilisateur aux données de son objet, chap. II) et du RGPD (droit d'accès aux données personnelles). Le mécanisme pourrait être le suivant : l'ILR et la CNPD instruisent conjointement la plainte, chacun selon ses prérogatives – l'ILR sur l'obligation du fabricant au titre du Data Act, la CNPD sur le respect des droits du RGPD – puis coordonnent leurs conclusions pour apporter une réponse unifiée à l'utilisateur. Ainsi, l'utilisateur n'aura pas à saisir deux autorités distinctes ou à subir des décisions contradictoires.

   - La loi nationale devrait prévoir explicitement cette collaboration. Par exemple, en introduisant un article stipulant que l'ILR transmet sans délai à la CNPD toute plainte qu'il reçoit qui porte sur des données personnelles, et que la décision concernant ces éléments sera prise par la CNPD (éventuellement intégrée dans la décision globale). Réciproquement, la CNPD pourrait informer l'ILR si, dans une plainte qu'elle traite, émergent des questions relevant du Data Act.

   - Les deux autorités synchroniseraient leurs actions pour ne pas double-pénaliser au-delà du raisonnable, mais ceci relève de la coordination pratique.

La CNPD doit dont être intégrée uniquement en tant que partie prenante consultée lorsque des questions relatives au traitement des données personnelles se posent, sans être surchargée d'un rôle de coordinateur global. Un protocole d'accord ILR-CNPD pourrait détailler cette articulation pour éviter toute ambiguïté. Cela garantit le respect du RGPD sans créer de latence inutile pour les plaignants.

ii. **Consultation des régulateurs sectoriels** : En dehors de la CNPD, certaines dispositions du Data Act pourront concerner des secteurs régulés spécifiques. Plutôt que de leur confier formellement des pans entiers du Data Act (au risque de rendre le schéma illisible pour les entreprises), nous préconisons une implication à travers des avis consultatifs ou des coopérations ponctuelles. Par exemple :

   - L'ILR, compte tenu de son expertise technique et réglementaire, et de son expérience dans la mise en œuvre de la Directive NIS2 qui couvre également les fournisseurs de services cloud, pourrait facilement développer les compétences nécessaires pour contribuer à la supervision des fournisseurs de services cloud (chap. VI du Data Act), bien que ce secteur soit distinct des télécommunications traditionnelles…
   - Si une question liée au Data Act émerge dans le secteur financier (par ex. partage de données bancaires), l'ILR pourrait consulter la CSSF pour s'assurer qu'il n'y a pas de conflit avec les obligations y relatives ou d'autres régulations financières. La CSSF n'émettrait pas une décision au sens Data Act, mais son avis technique guiderait l'ILR dans son évaluation.

Ces consultations doivent être encadrées par la loi ou des conventions. On peut imaginer que la loi énumère les autorités sectorielles susceptibles d'être consultées et oblige celles-ci à répondre dans un certain délai aux demandes d'avis de l'ILR. L'ILR restera décisionnaire final, sauf à éventuellement déléguer formellement un volet si cela s'impose. Mais la philosophie est de ne pas éclater le pouvoir de décision, pour conserver la cohérence et la responsabilité unique vis-à-vis des entreprises.

iii. **Comité de coordination** : L'ILR/coordinateur devrait mettre sur pied une instance de concertation périodique rassemblant la CNPD et les points de contact désignés de chaque autorité sectorielle partenaire. Ce comité pourrait se réunir trimestriellement (et en urgence si un cas le nécessite), pour, entre autres, échanger sur les cas en cours, ou encore, discuter des **lignes d'interprétation** du règlement, afin que toutes les entités soient alignées (par exemple, comment interpréter la notion de « préjudice économique grave » justifiant un refus de partager des données pour secret d'affaires). Ce comité renforcera la cohésion interne du dispositif et préviendra surtout les divergences d'interprétation afin d'assurer l'harmonisation. C'est aussi une structure agile pour résoudre rapidement d'éventuels accrochages de compétence sans que le justiciable n'en fasse les frais. Bien entendu, ce mécanisme ne doit pas alourdir le traitement des dossiers individuels : il s'agit d'un filet de sécurité coordinationnel, pas d'un niveau hiérarchique supplémentaire.

E. Conclusion

En conclusion, la FEDIL estime que le modèle de gouvernance proposé, une autorité nationale renforcée (ILR) faisant office de coordinateur unique, épaulée par la CNPD et les régulateurs sectoriels au sein d'une architecture collaborative, représente l'approche la plus équilibrée pour mettre en œuvre le Data Act au Luxembourg.

Ce modèle répond aux exigences légales européennes tout en étant adapté aux spécificités du pays :

- Il offre **simplicité et clarté** aux entreprises (un point de contact unique, un message réglementaire cohérent), évitant le morcellement qui pourrait diluer la compréhension et l'effectivité du règlement.
- Il mobilise les **meilleures expertises disponibles** (compétences techniques de l'ILR, expérience RGPD de la CNPD, savoir-faire de la CSSF ou autres quand requis) sans multiplier les structures, ce qui est essentiel pour un petit marché où chaque ressource compte.
- Il garantit une **cohésion nationale** dans l'application du Data Act : via le coordinateur, le Luxembourg parlera d'une voix unifiée tant aux acteurs internes qu'au niveau européen. Cela renforcera la crédibilité du pays dans l'enceinte de l'EDIB et vis-à-vis de la Commission, ce qui permettra de mieux défendre nos intérêts et d'influencer les futures orientations.
- Ce schéma permet d'intégrer la dimension pro-innovation du Data Act tout en protégeant nos entreprises des écueils (en offrant un accompagnement de proximité). Un cadre clair encouragera l'utilisation effective des nouvelles opportunités de partage de données, plutôt qu'une attitude frileuse.

La FEDIL invite le gouvernement à adhérer à ce principe de gouvernance hybride centrée sur l'ILR. Il conviendra d'associer dès que possible les autorités concernées (ILR, CNPD, etc.) afin qu'elles préparent la transition.

La FEDIL se tient également à disposition pour contribuer à l'élaboration de guides sectoriels ou à la diffusion d'information auprès des entreprises, dans l'optique d'une appropriation rapide du nouveau cadre par ces dernières.

En adoptant ces recommandations, le Luxembourg a le potentiel de transformer les obligations du Data Act en avantage compétitif : en devenant un des premiers États membres à se doter d'une gouvernance efficace et lisible, le pays renforce son image de place innovante et business-friendly. Au-delà du strict respect du règlement, c'est une occasion de faire du Luxembourg un modèle en matière de gestion publique des données, conciliant protection des acteurs économiques et promotion d'un écosystème numérique dynamique, au bénéfice tant du tissu entrepreneurial que de la réussite de la stratégie nationale sur l'économie des données.

XXX