

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal relatif à la plateforme de données énergétiques

Délibération n° 21/AV9/2024 du 26 avril 2024

- Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après la « Commission nationale » ou la « CNPD ») « conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ». Par ailleurs, l'article 36.4 du RGPD dispose que « [I]les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».

Par ailleurs, l'article 36.4 du RGPD dispose que « [I]les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».

- Par courrier en date du 3 octobre 2023, Monsieur le Ministre de l'Énergie et de l'Aménagement du territoire a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif à la plateforme informatique de données énergétiques, approuvé par le Conseil de gouvernement dans sa séance du 29 septembre 2023 (ci-après le « projet de règlement grand-ducal »).
- Le projet de règlement grand-ducal entend préciser certaines mesures d'exécution relatives à la plateforme informatique de données énergétiques prévue à l'article 27ter de la loi modifiée du 1^{er} août 2007 relative à l'organisation du marché de l'électricité. Les dispositions dudit article avaient d'ores et déjà été commentées par la CNPD dans son avis du 1^{er} juillet 2022 relatif au projet de loi n°7876¹.

¹ Délibération n°27/AV11/2022 du 1^{er} juillet 2022 de la Commission nationale de la protection des données, document parlementaire n°7876/04.



4. Elle se prononcera, dès lors, sur les dispositions du projet de règlement grand-ducal ayant un impact en matière de protection de données à caractère personnel.

I. Sur les différents acteurs de la plateforme

5. Les dispositions de l'article 3 du projet de règlement grand-ducal entendent préciser les responsabilités des différents acteurs de la plateforme d'un point de vue du RGPD.

L'article 3.1 du projet de règlement grand-ducal dispose, en effet, que « *[c]onformément à l'article 27ter, paragraphe 1^{er}, alinéa 1^{er}, de la loi modifiée du 1^{er} août 2007 relative à l'organisation du marché de l'électricité, le responsable de la plateforme assure le rôle de responsable de traitement au sens du [RGPD] pour l'ensemble des traitements des données énergétiques opérés sur ou par la plateforme. Quant aux données énergétiques visées à l'article 2, paragraphes 1^{er}, point 2^o, 2, point 2^o, et 4, point 2^o, les entreprises d'électricité et de gaz naturel sont des tiers au sens du [RGPD] qui sont responsables de la collecte de ces données auprès des personnes concernées et pour leur importation dans la plateforme. Le responsable de la plateforme est responsable des traitements des données importées au moyen des interfaces visées à l'article 2, paragraphes 1^{er}, point 1^o, lettre b), et 4, point 1^o, lettre a). Quant aux traitements des données à caractère personnel visés à l'article 2, paragraphe 2, point 1^o, lettre a), point ii., les entreprises d'électricité et de gaz naturel y visées sont considérées comme sous-traitants du responsable de la plateforme au sens RGPD* ».

6. Il convient de saluer les efforts des auteurs du projet de règlement grand-ducal pour de telles précisions alors que la Commission nationale avait dans son avis du 1^{er} juillet 2022 relatif au projet de loi n°7876 soulevé que « *tant les dispositions légales prévues par le projet de loi que les explications fournies par les auteurs du projet de loi ne permettent pas de déterminer clairement les rôles respectifs du gestionnaire de réseau de transport et des entreprises d'électricité ou de gaz d'un point de vue de la protection des données* »².

1) Remarques liminaires

7. Cependant, il y a lieu de relever que l'article 27ter de la loi modifiée du 1^{er} août 2007 relative à l'organisation du marché de l'électricité précise d'ores et déjà que le gestionnaire de réseau de transport est le responsable du traitement pour les traitements de données à caractère personnel effectués sur la plateforme. Or, le Conseil d'Etat rappelle que « *les dispositions qui n'ont d'autre*

² Délibération n°27/AV11/2022 du 1^{er} juillet 2022 de la Commission nationale de la protection des données, document parlementaire n°7876/04, sous point I, B, page 8.



objet que de rappeler une disposition hiérarchiquement supérieure, soit en la reproduisant, soit en la paraphrasant, n'ont pas leur place dans les lois et règlements »³.

8. En outre, l'article 3.2 du texte sous avis dispose que « *[I]l*le responsable du traitement procède à une analyse d'impact relative à la protection des données conformément à l'article 35 du RGPD ». La Commission nationale se demande si de telles dispositions ne sont pas superfétatoires alors que le responsable du traitement doit, en tout état de cause, respecter les obligations qui lui incombent en vertu du RGPD. Parmi celles-ci figure notamment la conduite d'une analyse d'impact conformément à l'article 35 du RGPD lorsque le responsable du traitement identifie des traitements susceptibles « *d'engendrer un risque élevé pour les droits et libertés des personnes physiques concernées* ».

2) Sur le rôle des différents acteurs de la plateforme

9. Les auteurs du projet de règlement grand-ducal précisent dans leur commentaire des articles que si le gestionnaire de réseau de transport est responsable du traitement « *de toutes les opérations opérées sur et par la plateforme, il n'est, conformément à l'alinéa 2 de la disposition précitée, pas responsable de la collecte des données énergétiques auprès des personnes concernées et par conséquent pas responsable de la qualité de ces données* »⁴.
10. Comme relevé par les auteurs du projet de texte sous avis, le gestionnaire de réseau de transport serait le destinataire des données collectées par les entreprises d'électricité et de gaz naturel. Le gestionnaire de réseau de transport traiterait ensuite les données reçues pour effectuer des traitements de données via la plateforme informatique.

Il convient dès lors de distinguer :

- Les traitements effectués par les entreprises d'électricité et de gaz naturel, lors de l'importation de données sur la plateforme. Les entreprises d'électricité et de gaz naturel seraient dans ce contexte à qualifier de responsables de traitement ; et
- Les traitements effectués, avec les données reçues, par le gestionnaire de réseau de transport sur la plateforme informatique, qui serait pour de tels traitements à qualifier de responsable du traitement.

11. Par conséquent, dans le cadre de leurs traitements de données respectifs, tant le gestionnaire de réseau de transport que les entreprises d'électricité et de gaz naturel sont tenus de respecter les principes et obligations qui leur incombent en vertu du RGPD. En tant que responsables de

³ Avis 60.516 du Conseil d'État du 16 juillet 2021, page 8.

⁴ V. projet de loi, commentaire des articles, Ad article 3, pages 11 à 12.



traitement, ils doivent notamment respecter les principes visés à l'article 5 du RGPD, dont le principe d'exactitude. En vertu de ce principe, les données personnelles doivent être exactes, et si nécessaire, tenues à jour.

12. La CNPD se permet dès lors de rappeler ses observations formulées dans son avis relatif au projet de loi n°7876, en ce qu'elle avait relevé que « *les dispositions sous avis ne devraient pas décharger le ou les responsables du traitement des obligations qui leur incombent en vertu du RGPD. Ainsi, si le gestionnaire de réseau de transport devait être le responsable du traitement alors les dispositions de l'article 27ter.1. du projet de loi ne devraient pas exclure sa responsabilité quant à la « véracité et l'exactitude des données » qui seraient utilisées via la plateforme* »⁵.

En outre, elle avait également rappelé que « *la détermination du responsable du traitement est primordiale alors que c'est sur ce dernier que pèse le respect de l'ensemble des principes énoncés à l'article 5 du RGPD. L'article 24 du RGPD dispose encore à ce sujet que « le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* »⁶.

Par conséquent, les dispositions précitées ne sauraient exonérer le gestionnaire de réseau de transport de ses obligations, en tant que responsable du traitement, dans le cadre des traitements effectués sur la plateforme visée par le texte sous avis.

Par ailleurs, il convient d'attirer l'attention des auteurs du projet de règlement grand-ducal sur l'article 19 du RGPD en vertu duquel « *[I]l responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué conformément à l'article 16, à l'article 17, paragraphe 1, et à l'article 18, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés* ». Ainsi, lors des traitements relatifs à l'importation des données sur la plateforme, les entreprises d'électricité et de gaz naturel, en tant que responsables de traitement, devraient notamment notifier au gestionnaire de réseau de transport, en tant que destinataire, « *toute rectification ou tout effacement de données à caractère personnel* ».

13. L'article 3.1 alinéa 2 du projet de règlement grand-ducal dispose que « *[q]uant aux données énergétiques visées à l'article 2, paragraphes 1^{er}, point 2[°], 2, point 2[°] et 4, point 2[°], les entreprises*

⁵ Délibération n°27/AV11/2022 du 1^{er} juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, B, page 9.

⁶ Délibération n°27/AV11/2022 du 1^{er} juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, B, page 9



d'électricité et de gaz naturel sont des tiers au sens du [RGPD] qui sont responsables de la collecte de ces données auprès des personnes concernées et pour leur importation dans la plateforme ».

14. Au sujet de ces dispositions, les auteurs du texte sous avis précisent que les entreprises d'électricité et de gaz naturel collectent les données visées par les dispositions précitées et « assurent le rôle de responsable de traitement au moment de la collecte auprès des personnes concernées et les importent dans la plateforme au moyen d'interfaces mis en place par le responsable de la plateforme. Ils agissent ainsi comme des « tiers » au sens du [RGPD] précité, et sont responsables de leurs propres traitements »⁷.

En vertu de ces dispositions, la Commission nationale comprend que ces dernières seraient donc à considérer comme des responsables de traitement en ce qui concerne l'importation des données sur la plateforme, comme mentionné au point 10 supra.

15. Cependant, les auteurs du projet de règlement grand-ducal indiquent encore que les entreprises d'électricité et de gaz naturel agissent comme des « tiers » au sens du RGPD tout en étant « responsables de leurs propres traitements ». Il convient de rappeler que l'article 4 du RGPD définit un tiers comme « une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ».

Or, l'utilisation du terme « tiers » ne semble pas la qualification appropriée alors qu'il ressort des dispositions sous avis et du commentaire des articles que les entreprises d'électricité et de gaz naturel sont à considérer comme responsables des traitements visés aux articles 2.1.2°, 2.2.2° et 2.4.2°. L'emploi du terme « tiers », combiné avec la notion de responsable du traitement dans la même disposition, est susceptible de créer une confusion dans l'esprit du lecteur quant à la qualification juridique desdites entités.

Il est suggéré de remplacer les dispositions actuelles précitées du projet de règlement grand-ducal par les dispositions suivantes : « [q]uant aux données énergétiques visées à l'article 2, paragraphes 1^{er}, point 2°, 2, point 2° et 4, point 2°, les entreprises d'électricité et de gaz naturel sont des tiers au sens du [RGPD] à qualifier de responsable du traitement en ce qui concerne qui sont responsables de la collecte de ces données auprès des personnes concernées et pour leur importation dans la plateforme ».

⁷ V. projet de loi, commentaire des articles, Ad article 3, pages 11 à 12.



Pour le surplus, la CNPD se permet de renvoyer à l'ensemble de ses développements qu'elle avait formulés à ce sujet concernant le projet de loi N°7876⁸.

II. Sur les mesures de sécurité

16. Conformément à l'article 5.1.f) du RGPD, les données à caractère personnel doivent être « *traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)* ».
17. L'article 32 du RGPD dispose encore que « *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ». Pareilles mesures doivent être mises en œuvre afin d'éviter notamment des accès non-autorisés aux données, des fuites de données ou des modifications non désirées.
18. Il y a lieu de rappeler qu'il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne ou le service, au sein de l'entité concernée, et à quelles données précises cette personne ou ce service aurait accès.
19. En outre, il est nécessaire de prévoir un système de journalisation des accès. Sur ce point, la CNPD recommande que les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.
20. Il convient encore de souligner l'importance d'effectuer proactivement des contrôles en interne. A cet effet, il convient conformément à l'article 32.1.d) du RGPD de mettre en œuvre une procédure « *visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».
21. En outre, tel que relevé par le Conseil d'État dans son avis relatif au projet de loi n°8089 prévoyant notamment la création d'une plateforme sécurisée permettant le stockage d'actes administratifs, « *le RGPD impose au responsable du traitement de mettre en œuvre et de documenter toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité* ».

⁸ Délibération n°27/AV11/2022 du 1^{er} juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, B.



*adapté au risque », notamment compte tenu de l'état des connaissances sachant que l'évolution permanente des meilleures techniques et pratiques en la matière nécessite des adaptations en continu*⁹. Selon le Conseil d'État, cette exigence devrait s'imposer au responsable du traitement qui devrait mettre en œuvre des mesures au-delà des minima prévus dans un règlement grand-ducal¹⁰.

22. Par ailleurs, la CNPD estime primordial, en ce qui concerne l'accès et la gestion de la plateforme informatique de données énergétiques, que de telles mesures de sécurité soient mises en œuvre par le responsable du traitement afin d'assurer la confidentialité et la sécurité des données.
23. Elle se félicite que de telles mesures soient prévues à l'article 2 et soient également précisées et détaillées aux paragraphes 2 et 3 de l'article 4 du projet de règlement grand-ducal. Toutefois, certaines des dispositions appellent les remarques suivantes de la CNPD.
 - 1) Ad article 2
24. L'article 2.2.1°.a) du projet de règlement grand-ducal prévoit notamment les modalités des moyens d'identification aux fins d'attribution d'un identifiant unique pour accéder à la plateforme sous avis. Les moyens d'identification consistent en la vérification de l'identité de l'utilisateur de la plateforme :
 - « à distance par une vérification digitale » ; ou
 - « aux guichets physiques des entreprises d'électricité et de gaz naturel par le biais d'une vérification de l'identité ».
25. Quant à la vérification de l'identité de l'utilisateur de la plateforme par les moyens susvisés, il convient de préciser que les dispositions des articles 24¹¹ et 32 du RGPD seront à respecter, en sus de l'ensemble des principes énoncés à l'article 5 du RGPD¹².

⁹ Avis 61.218 du Conseil d'État du 12 mars 2024, page 9.

¹⁰ Avis 61.218 du Conseil d'État du 12 mars 2024, page 9.

¹¹ Voir point 30 paragraphes 3 et 4 du présent avis.

¹² L'article 5 du RGPD dispose que « 1. Les données à caractère personnel doivent être :

- a. traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
- b. collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;
- c. adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;



Avis de la Commission nationale pour la protection des données

relatif au projet de règlement grand-ducal relatif à la plateforme de données énergétiques

26. En ce qui concerne plus particulièrement la vérification de l'identité de l'utilisateur « à distance par une vérification digitale », les auteurs du projet de règlement grand-ducal précisent à ce sujet qu' « elle se fait par exemple par l'accès à une application bancaire ou à la plateforme myguichet.lu ». Il y a lieu de regretter que les modalités pratiques de tels accès ne soient pas plus détaillées dans le commentaire des articles, de sorte que la CNPD ne peut pas réellement analyser quelles seraient les éventuelles questions qui se poseraient en termes de protection des données.

Par ailleurs, en l'absence de précisions quant à l'emploi du terme « digital », la Commission nationale tient à attirer l'attention des auteurs du projet de règlement grand-ducal sur les conséquences de l'éventuel recours à la reconnaissance faciale. Si tel devait être le cas, elle se permet de souligner qu'un tel traitement de données serait à qualifier de traitement de données biométriques. Les dispositions de l'article 9 du RGPD devraient donc être respectées. Elle rappelle que de tels traitements sont en principe interdits à moins que l'une des conditions de l'article 9.2 du RGPD soit remplie et que « les principes généraux et les autres règles du [RGPD], en particulier en ce concerne les conditions de licéité du traitement »¹³ doivent être respectés.

Notons par ailleurs que le législateur luxembourgeois n'a pas prévu de dispositions nationales spécifiques concernant les données biométriques sur base de l'article 9.4 du RGPD.

2) Ad article 4.2

27. Ainsi, s'il y a lieu de féliciter les auteurs du texte sous avis de prévoir « un stockage encrypté et isolé sur la plateforme » des données de comptage visées à l'article 27ter.3.b), de la loi modifiée du 1^{er} août 2007 relative à l'organisation du marché de l'électricité, dont des données issues des compteurs intelligents, ne faudrait-il pas également prévoir un tel encryptage de données lors de leur importation sur la plateforme par les entreprises d'électricité et de gaz naturel ? En effet, la

-
- d. exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;
 - e. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;
 - f. traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ».

¹³ V. considérant 51 du RGPD.



CNPD avait fait part de ses vives préoccupations dans son avis du 1^{er} juillet 2022 en ce qui concerne l'utilisation de telles données pour des finalités différentes de celles pour lesquelles elles auraient été collectées¹⁴.

28. En outre, concernant la politique de gestion des accès, l'article 4.2.1° du projet de règlement grand-ducal dispose que « *[c]haque utilisateur de la plateforme a accès à ce journal afin de pouvoir retracer les accès et traitements en lien avec les données les concernant* ».

Il convient de préciser que l'accès à ce journal, qui concerne la traçabilité des accès aux traitements de données effectués via la plateforme, devrait en premier lieu pouvoir être effectué par le responsable du traitement de la plateforme afin de pouvoir détecter et, dans la mesure du possible, prévenir que la confidentialité, l'intégralité ou la disponibilité des données traitées via la plateforme ne soient compromises. L'accès à ce journal permet ainsi au responsable du traitement de respecter son obligation de sécurité qui lui incombe en vertu des articles 24 et 32 du RGPD.

Toutefois, la Commission nationale se demande quelles seraient les raisons d'un tel accès par les utilisateurs de la plateforme qui sont définis comme « *toute personne disposant d'un accès individualisé sur la plateforme en vertu de l'article 27ter, paragraphe 5 à 7, de la loi modifiée du 1^{er} août 2007 relative à l'organisation du marché de l'électricité* »¹⁵.

Il y a lieu de regretter que les auteurs du projet de règlement grand-ducal n'aient pas précisé dans le commentaire des articles les justifications d'un tel accès pour chacun des utilisateurs de la plateforme, à savoir les entreprises d'électricité et de gaz naturel¹⁶, les utilisateurs du réseau et des preneurs de raccordement¹⁷ ainsi que le ministre, le régulateur, Commissaire du Gouvernement à l'Energie ou à l'Institut national de la statistique et des études économiques¹⁸. Des précisions à ce sujet devraient être apportées.

En outre, si la volonté des auteurs du texte sous examen est de prévoir que cet accès permettrait aux utilisateurs du réseau et des preneurs de raccordement de constater tout accès illicite à leurs données, alors une telle volonté devrait être reflétée dans le projet de règlement grand-ducal. Si cela devait être le cas, la CNPD pourrait accueillir favorablement de telles dispositions, qui permettraient auxdites personnes concernées de se prémunir contre d'éventuels traitements illicites de leurs données à caractère personnel.

¹⁴ Délibération n°27/AV11/2022 du 1^{er} juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, C, pages 10 à 13, et point 3, pages 21 à 23.

¹⁵ V. article 1 du projet de règlement grand-ducal.

¹⁶ V. article 27ter.5 de la loi modifiée du 1^{er} août 2007 relative à l'organisation du marché de l'électricité.

¹⁷ V. article 27ter.6 de la loi modifiée du 1^{er} août 2007 relative à l'organisation du marché de l'électricité.

¹⁸ V. article 27ter.7 de la loi modifiée du 1^{er} août 2007 relative à l'organisation du marché de l'électricité.



Enfin, compte tenu de la multiplicité des utilisateurs de la plateforme, le responsable du traitement devrait veiller à éviter que des personnes accèdent à des données qui ne les concernent pas et/ou que des utilisateurs accèdent à des données pour lesquelles ces derniers ne devraient pas avoir accès.

3) Ad article 4.3

29. Enfin, l'article 4.3 du projet de règlement grand-ducal dispose que les entreprises d'électricité et de gaz naturel « *mettent en œuvre les mesures techniques et organisationnelles de sécurité appropriées afin de garantir un niveau de sécurité adapté aux risques liés à leurs activités* ». Il convient de rappeler que les obligations visées aux articles 24 et 32 du RGPD leur incombent en tant que responsable du traitement pour leurs propres traitements de données.

30. De même lorsque celles-ci agissent en tant que sous-traitants du gestionnaire de réseau de transport, alors elles doivent également veiller au respect des mesures de sécurité techniques et organisationnelles conformément aux articles 32.1 et 28.3.c) du RGPD.

Sur ce point, il convient de préciser que « *[t]out traitement de données à caractère personnel effectué par un sous-traitant doit être régi par un contrat ou un autre acte juridique établi par écrit (...). L'accord de traitement ne devrait toutefois pas simplement reproduire les dispositions du RGPD ; il devrait inclure des informations plus spécifiques et concrètes sur la manière dont les conditions seront remplies et sur le niveau de sécurité requis pour le traitement de données à caractère personnel qui fait l'objet dudit accord* »¹⁹.

Il y a lieu de souligner également que « *le responsable du traitement doit toujours stipuler certains éléments dans l'accord de sous-traitance, tels que, en ce qui concerne l'exigence de sécurité, l'instruction de prendre toutes les mesures requises conformément à l'article 32 du RGPD. L'accord doit également indiquer que le sous-traitant doit aider le responsable du traitement à garantir le respect de l'article 32, par exemple. En tout état de cause, le responsable du traitement reste responsable de la mise en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que le traitement est effectué conformément au règlement (article 24) et être en mesure de le démontrer* »²⁰.

¹⁹ V. Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 du 7 juillet 2021 sur les notions de responsable du traitement et de sous-traitant, page 4, disponibles sous https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

²⁰ V. Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 du 7 juillet 2021 sur les notions de responsable du traitement et de sous-traitant, para. 41, page 18, disponibles sous https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.



Enfin, le contrat relatif aux activités de traitement « doit inclure ou mentionner des informations relatives aux mesures de sécurité à adopter, l'obligation faite au sous-traitant d'obtenir le consentement du responsable du traitement avant d'apporter des modifications et le réexamen régulier des mesures de sécurité afin de s'assurer de leur adéquation au regard des risques, lesquels peuvent évoluer au fil du temps. Le degré de détail des informations relatives aux mesures de sécurité à inclure dans le contrat doit permettre au responsable du traitement d'appréhender le caractère approprié des mesures conformément à l'article 32, paragraphe 1, du RGPD. En outre, la description est également nécessaire pour permettre au responsable du traitement de se conformer à son obligation de rendre des comptes en vertu de l'article 5, paragraphe 2, et de l'article 24 du RGPD en ce qui concerne les mesures de sécurité imposées au sous-traitant »²¹.

III. Remarques finales

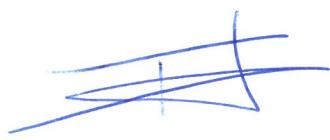
31. La Commission nationale se permet de réitérer ses observations en ce qui concerne ses interrogations « quant aux motivations qui justifieraient qu'une entreprise privée gèrerait une telle plateforme dans l'intérêt public, plutôt que le ministre ayant l'énergie dans ses attributions ou encore l'Institut Luxembourgeois de Régulation (ci-après « l'ILR ») ? » et renvoie à ses développements formulés dans son avis précité²².

Ainsi adopté à Belvaux en date du 26 avril 2024.

La Commission nationale pour la protection des données



Tine A. Larsen
Présidente



Thierry Lallemand
Commissaire



Marc Lemmer
Commissaire



Alain Herrmann
Commissaire

²¹ V. Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 du 7 juillet 2021 sur les notions de responsable du traitement et de sous-traitant, para. 126, page 42, disponibles sous https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

²² Délibération n°27/AV11/2022 du 1^{er} juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, pages 2 à 3.



Avis de la Commission nationale pour la protection des données
relatif au projet de règlement grand-ducal relatif à la plateforme de données énergétiques