Avis n° 76/2018 du 5 septembre 2018

Objet : Projet d'arrêté du Gouvernement flamand modifiant l'arrêté relatif à l'énergie du 19 novembre 2010 en ce qui concerne le déploiement de compteurs numériques (CO-A-2018-068)

L'Autorité de protection des données (ci-après "l'Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 ;

Vu la demande d'avis du Ministre flamand du Budget, des Finances et de l'Énergie, reçue le 18 juillet 2018 ;

Vu le rapport du Président ;

Émet, le 5 septembre 2018, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. La Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité (ci-après la Commission), s'est déjà prononcée précédemment sur les compteurs intelligents. L'Autorité attire notamment l'attention sur les avis suivants :

- l'avis n° 17/2017 du 12 avril 2017 *sur le Projet de note "uitrol van digitale meters in Vlaanderen" (déploiement des compteurs numériques en Flandre)*[1] ;
- l'avis d'initiative n° 36/2017 du 26 juillet 2017[2] *concernant un projet de loi modifiant la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité en vue d'améliorer la flexibilité de la demande et le stockage d'électricité* [3] ;
- l'avis n° 73/2017 du 13 décembre 2017 *sur le projet d'arrêté du Gouvernement flamand modifiant l'arrêté relatif à l'énergie du 19 novembre 2010*[4]. Ce projet concernait notamment les fonctionnalités des compteurs intelligents ;
- l'avis n° 07/2018 du 17 janvier 2018 *sur le projet de décret modifiant le Décret flamand sur l'Énergie du 8 mai 2009, en ce qui concerne le déploiement de compteurs numériques et modifiant les articles 7.1.1., 7.1.2., 7.1.5. et 13.2.1. de ce même décret*[5].

2. Le 18 juillet 2018, l'Autorité a reçu une demande d'avis du Ministre flamand du Budget, des Finances et de l'Énergie (ci-après "le demandeur") concernant un projet d'arrêté du Gouvernement flamand modifiant l'arrêté relatif à l'énergie du 19 novembre 2010 en ce qui concerne le déploiement de compteurs numériques (ci-après "le projet").

II. CONTENU DU PROJET

3. Le présent projet adapte d'une part diverses dispositions de l'arrêté relatif à l'énergie du 19 novembre 2010. D'autre part, plusieurs articles du Décret sur l'Énergie du 8 mai 2009 sont exécutés.

4. L'Autorité ne se prononce ci-après que sur les modifications figurant dans le projet qui concernent le respect du RGPD[6] ou qui ont un impact sur les droits et libertés des personnes concernées au sens du RGPD. Il s'agit notamment :

[1] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_17_2017.pdf.
[2] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_36_2017.pdf.
[3] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_36_2017.pdf.
[4] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_73_2017.pdf.
[5] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_07_2018.pdf.

[6] 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 ou RGPD).

- de l'application, par le fournisseur, après le 1er avril 2020, de tarifs dynamiques si la personne concernée manifeste sa volonté à cet effet et que le gestionnaire de données met à disposition des données d'utilisateur validées par quart d'heure (article 8 du projet) ;
- de la "fermeture" standard des ports utilisateurs en application des principes de protection des données dès la conception et de protection des données par des paramètres standard (article 9 du projet) ;
- de la possibilité d'augmenter la fréquence et l'unité de temps de la lecture des données (article 11 du projet) ;
- du soutien du rôle du délégué à la protection des données au sein du gestionnaire de données (article 12 du projet) ;
- de la communication d'informations complémentaires à la personne concernée (article 12 du projet) ;
- de la conclusion d'un contrat de sous-traitance (article 12 du projet) ;
- de la création d'un datawarehouse pour la comparaison et le croisement de données (article 12 du projet).

III. EXAMEN DU PROJET

1. Licéité du traitement concernant la transmission de valeurs par quart d'heure à des fournisseurs afin d'appliquer des tarifs dynamiques (article 6 du RGPD)

5. L'article 8 du projet insère l'article suivant dans l'arrêté relatif à l'énergie :

"Art. 3.1.38/1. Si le fournisseur d'électricité au point d'accès propose des prix dynamiques, il informe l'utilisateur du réseau de distribution d'électricité à basse tension des périodes d'utilisation dynamiques ou non et des prix de l'énergie dynamiques qui sont d'application de manière à ce que l'utilisateur du réseau de distribution d'électricité puisse faire un choix réfléchi et informé.

Le fournisseur informe l'utilisateur du réseau de distribution d'électricité concernant :
1° le consentement pour utiliser les données de consommation par période élémentaire que l'utilisateur du réseau de distribution d'électricité doit donner pour permettre une agrégation de consommations sur les périodes d'utilisation ;
2° les fluctuations possibles des prix d'un tel produit et leurs implications.

À condition que l'utilisateur du réseau de distribution d'électricité donne son consentement pour utiliser les données de consommation par période élémentaire et à condition que le dispositif de mesure permette à l'utilisateur du réseau de distribution

d'électricité de choisir un système de mesure permettant de mettre à disposition les données de consommation par période élémentaire, le gestionnaire de données mettra à disposition du titulaire d'accès pour le point d'accès en question, à partir du 1er avril 2020, les données de consommation validées par quart d'heure qui constituent la base pour la facturation, par le titulaire d'accès, des prix dynamiques de l'énergie." [NdT : tous les passages cités du projet ou du dossier de demande sont des traductions libres réalisées par le Secrétariat de l'Autorité, en l'absence de traduction officielle]

6. La note au Gouvernement précise pour l'article 8 : "*Un contrat exige une entente et constitue donc un consentement, pour autant qu'il réponde évidemment à ces conditions dans ce règlement et dans toute autre réglementation applicable. Si dans un tel contrat, il est convenu d'utiliser les données de consommation par période élémentaire, cela suffit.*"

7. La note prend clairement pour point de départ la méthode visant à choisir, sur la base de la manifestation de volonté de la personne concernée, un tarif dynamique et à transmettre à cet effet les valeurs par quart d'heure aux fournisseurs via une manifestation de volonté dans un simple contrat.

8. Bien que la note laisse entendre que cette manifestation de volonté doit répondre au RGPD, on ne sait pas clairement comment se concrétisera cette intention dans la pratique sur un marché où les fournisseurs d'énergie travaillent aujourd'hui *de facto* avec des contrats d'adhésion et qu'il n'y a aucune preuve que les fournisseurs d'énergie rempliront (pourront remplir) toutes les conditions liées par le RGPD à la notion de consentement.

9. L'Autorité conclut que travailler avec le consentement au sens du RGPD en tant que justification du traitement "choisir un tarif dynamique" n'a aucun sens dans la pratique. Elle attire l'attention sur le fait qu'au cours des derniers mois, le consentement de la personne concernée a été appliqué à tort et (surtout) à travers, alors que d'autres fondements pour conférer une licéité au traitement tel que l'article 6.1.b) du RGPD n'ont souvent même pas été examinés.

10. L'Autorité estime dès lors qu'il serait préférable que l'article 8 du projet se fonde sur le traitement qui "*est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie*[7]". Cette méthode doit éviter la confusion autour de la notion de "consentement". Cela peut aussi contrer le risque qu'une réutilisation des valeurs par quart d'heure ait lieu de manière non transparente et pour d'autres finalités que l'offre d'un tarif dynamique. L'Autorité attire l'attention sur le risque d'un profilage commercial de la personne concernée en dehors du contexte de l'offre d'un tarif dynamique. Ce profilage n'est pas autorisé, à moins de disposer du consentement de la personne concernée au sens du RGPD.

[7] Voir l'article 6.1.b) du RGPD.

2. Principes de protection des données dès la conception ("privacy by design") et par des paramètres standard ("privacy by default") appliqués à la communication via le port utilisateur

11. L'article 9 du projet modifie l'article 3.1.45 de l'arrêté relatif à l'énergie en y ajoutant la disposition suivante :

> *"Lors du paramétrage standard de chaque port utilisateur dont dispose le compteur numérique, les données de mesure ne sont pas lisibles localement.*
> *Lors de l'installation du compteur numérique, la personne concernée est clairement informée que le port utilisateur n'est pas lisible localement lors de l'installation. La personne concernée peut toutefois toujours demander, via le portail Internet, mentionné à l'article 3.1.80, que le gestionnaire du réseau de distribution paramètre la lisibilité des données localement gratuitement."*

12. L'Autorité prend acte du fait que l'article 9 du projet ferme par défaut le port utilisateur (ce qu'on appelle "le port P1"). Le demandeur suit ainsi les avis antérieurs[8] de la Commission.

13. L'Autorité souligne toutefois que la démarche de la personne concernée visant à ouvrir le port ne signifie pas qu'il s'agit directement d'un consentement juridique au sens du RGPD pour que des tiers réutilisent ces données. Il ressort néanmoins de l'article 12 du projet (nouvel article 3.1.80) que ces deux éléments sont mis dans le même panier. Pour la réutilisation de données via un port utilisateur que l'utilisateur du réseau a "ouvert", **une double validation sera toujours nécessaire**. Cela veut dire qu'après l'ouverture du port utilisateur, les données à caractère personnel ne peuvent pas servir directement pour des tiers. Cela requiert une base légale particulière ou un document distinct supplémentaire[9] pour donner un consentement indépendant des services énergétiques, des factures, des offres pour des compteurs numériques et des actes d'installation et d'entretien, ..., et ce afin de donner un consentement libre, spécifique et éclairé au sens du RGPD.

3. Augmentation de la fréquence et de l'unité de temps de la lecture des données

14. L'article 11 du projet régit la possibilité pour le gestionnaire de données de lire les données via une connexion distincte (indépendante du port utilisateur). En principe, la lecture du prélèvement et de l'injection (dans la mesure où c'est pertinent) du compteur se fait au moins une fois par jour.

---

[8] Voir le *point 18 in fine* de l'avis n° 17/2017 du 12 avril 2017.
[9] Le considérant 42 du RGPD dispose que : "(...) *Conformément à la directive 93/13/CEE du Conseil, une déclaration de consentement rédigée préalablement par le responsable du traitement devrait être fournie sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples, et elle ne devrait contenir aucune clause abusive*".

15. À partir du 1er avril 2020, à la demande de l'utilisateur du réseau, une lecture sera possible par le gestionnaire de données par valeur par quart d'heure pour les valeurs de prélèvement et d'injection (dans la mesure où c'est pertinent) en matière d'électricité et de gaz. En vertu de l'article 11 du projet, le Ministre flamand peut déterminer les conditions complémentaires relatives à la lecture.

16. En outre, l'article 11 du projet dispose qu'une lecture avec une unité de temps encore plus fréquente ou plus petite peut avoir lieu "*à la demande de l'utilisateur du réseau ou dans le cadre de la communication des données nécessaires au gestionnaire du réseau de distribution, au gestionnaire du réseau de transmission, à la société de transport et au gestionnaire du réseau de transport local et si cela est nécessaire pour l'exécution de leurs tâches relatives à la gestion du réseau et à la sécurité opérationnelle du réseau*".

3.1. Augmentation de la fréquence et de l'unité de temps s'il y a une ingérence (grave) dans la vie privée au sens des articles 8 de la CEDH, 22 de la Constitution et 7 de la Charte des droits fondamentaux de l'Union européenne

17. Si l'article 11 du projet permet de paramétrer la fréquence et l'unité de temps de la lecture des compteurs intelligents sur une lecture continue et en secondes, **le risque pour l'utilisateur du réseau concerné augmente de manière substantielle**. La Commission a déjà prévenu précédemment[10] que la réutilisation des données par les gestionnaires de réseau ne pouvait pas impliquer une surveillance continue du comportement de la personne concernée dans la lutte contre la fraude sociale : "*Enfin, il convient de souligner une fois encore qu'il faut veiller à ce que les critères de sélection prévus ne placent pas en permanence certains groupes de population sous une surveillance (...)*."

18. L'application de l'article 11 est certes limitée à "*la demande de l'utilisateur du réseau, ou dans le cadre de la communication des données nécessaires au gestionnaire du réseau de distribution, au gestionnaire du réseau de transmission, à la société de transport et au gestionnaire du réseau de transport local et si cela est nécessaire pour l'exécution de leurs tâches relatives à la gestion du réseau et à la sécurité opérationnelle du réseau*."

19. La définition susmentionnée est toutefois tellement vague que des risques substantiels subsistent. Ainsi, les décisions du gestionnaire de données de rendre la lecture plus fréquente et/ou sur la base d'une unité de temps plus petite ne sont pas transparentes. La personne concernée ne peut pas prévoir quand et pour combien de temps le gestionnaire du réseau a autorisé des lectures fréquentes ou avec une unité de temps plus petite (la personne concernée peut-elle même en

[10] Voir le point 19 de l'avis n° 24/2015 du 17 juin 2015, publié à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_24_2015.pdf.

demander un relevé, par ex. si elle soupçonne une fuite de données ?). Le risque existe que le gestionnaire de données programme le critère de lecture sur une haute fréquence et une petite unité de temps car cela coûterait moins cher que d'adapter systématiquement la lecture selon le besoin de la partie requérante. Même la demande de l'utilisateur du réseau n'est pas sans risque, étant donné que le but de cette demande n'est pas déterminé et que les utilisateurs du réseau pourraient être persuadés de consentir à la lecture la plus fréquente sur l'unité de temps la plus petite, en échange d'un avantage économique limité, même si toutes les personnes concernées (la famille de l'utilisateur du réseau) n'étaient pas d'accord.

20. L'article 11 du projet ne tient donc pas suffisamment compte des risques pour les droits et libertés des personnes concernées au sens du RGPD (par ex. en cas de fuites de données, on ne sait pas si ce risque est repris dans une DPIA, ...).

21. L'Autorité signale qu'avec chaque augmentation supplémentaire de la fréquence et de l'unité de temps des lectures, une image (encore plus) fidèle, complète et précise du comportement et du profil des individus (utilisateurs du réseau et également leurs familles, ...) est ébauchée. La lecture des données des compteurs sans pseudonymisation et aux niveaux les plus élevés de l'unité de temps et de la fréquence (plus que sur une base du quart d'heure et plus qu'une fois par jour) implique également une **ingérence grave dans la vie privée**[11] des utilisateurs du réseau concernés et de leur famille, il s'agit donc de données à caractère personnel "qualifiées"[12]. Les données concernent la vie domestique et se prêtent par excellence au profilage d'une partie sans cesse croissante de la population (utilisateurs du réseau et leur famille) auprès de laquelle il faudra en outre obligatoirement installer un compteur intelligent.

22. L'ingérence dans la vie privée doit, selon les articles 8 de la CEDH et 22 de la Constitution, être prévue dans une loi formelle (donc le Décret sur l'Énergie) dont l'application est suffisamment prévisible. En vertu de l'exigence de prévisibilité, la Cour européenne des droits de l'homme[13] exige de plus en plus que des **garanties** minimales contre l'exercice arbitraire des compétences par les pouvoirs publics soient élaborées dans la loi. Plus grande est la compétence discrétionnaire du

[11] Cour de Justice, 21 décembre 2016, affaire C-203/15 Tele2 Sverige, § 122 : *"Compte tenu de la quantité de données conservées, du caractère sensible de ces données ainsi que du risque d'accès illicite à celles-ci, les fournisseurs de services de communications électroniques doivent, aux fins d'assurer la pleine intégrité et la confidentialité desdites données, garantir un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles appropriées*", § 74 des conclusions de l'avocat général Cruz Villalón dans l'affaire Digital Rights Ireland et commentaires au § 253-256 des conclusions de l'avocat général H. Saugmandsgaard du 19 juillet 2016 dans l'affaire Tele2Sverige.

[12] Termes utilisés au § 74 des conclusions de l'avocat général Cruz Villalón du 12 décembre 2013 dans l'affaire C-293/12 : "*Les données en question, il importe également d'insister encore une fois à cet égard, ne sont pas des données personnelles au sens classique du terme, se rapportant à des informations ponctuelles sur l'identité des personnes, mais des données personnelles pour ainsi dire qualifiées, dont l'exploitation peut permettre l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée*".

[13] Cour européenne des droits de l'homme, arrêt-Maestri c. Italie du 17 février 2004, § 30.

gestionnaire de données pour augmenter la fréquence et l'unité de temps de la lecture, plus grand est le besoin de garanties contre les risques et les abus.

23. L'Autorité constate que l'article 11 du projet ne satisfait pas à l'exigence de prévisibilité.

- Tout d'abord, on ne sait pas clairement quelle base légale est exécutée dans le Décret sur l'Énergie, ni si ce décret permet vraiment une telle ingérence grave. Il ne s'agit en tout cas pas d'une mesure qui peut être prévue dans un arrêté du Gouvernement flamand sans une base décrétale claire[14].
- Le projet ne fournit à la personne concernée aucune garantie suffisante contre une ingérence arbitraire dans sa vie privée au sens de l'article 8 de la CEDH. Ainsi, il n'y a pas suffisamment de dispositions qui garantissent la transparence pour la personne concernée et qui doivent empêcher les abus au sein du gestionnaire de données si celui-ci statue sur la fréquence et l'unité de temps des lectures[15].
- Les cas (pour quelles finalités) où une unité de temps et une fréquence encore plus élevées (et à quel niveau) seraient nécessaires pour chacun des quatre services susmentionnés ne sont pas suffisamment définis. La personne concernée ne peut pas suffisamment évaluer quand et à quelle fréquence son compteur est placé sous une lecture plus fréquente et/ou avec une unité de temps plus petite, ni quand quel service en fait la demande au gestionnaire de données. Le mode de définition offre aux services concernés une liberté d'appréciation trop large pour appliquer, de manière continue ou non, une mesure de contrôle potentiellement très extrême. En outre, on ne sait pas clairement si le projet autorise indirectement les analyses du comportement domestique des personnes concernées pour lutter contre la fraude, les infractions administratives, divers délits, ... sur la base de compétences d'enquête de diverses autorités au niveau fédéral et régional, parfois définies de manière très générale. Vu que la disponibilité des données correspond souvent à une demande ou à un besoin, l'Autorité considère que ce risque est réel.

3.2. Augmentation de la fréquence et de l'unité de temps à la lumière des exigences du RGPD

24. L'Autorité évalue ci-après les cas où la fréquence et l'unité de temps de la lecture des données des compteurs intelligents peuvent être augmentées à la lumière du RGPD.

25. Le renvoi à la finalité légitime de "**nécessaire à l'exercice de leurs missions relatives à la gestion du réseau et à la sécurité opérationnelle du réseau**" n'empêche pas le fait qu'il n'y

[14] Voir le point 11 des avis 37.748 et 37.749 du 23 novembre 2004 du Conseil d'État sur des avant-projets de loi "modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité" (37.748/AG) et "modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité" (37.749/AG), publiés à l'adresse suivante : http://www.dekamer.be/FLWB/PDF/51/1598/51K1598001.pdf.

[15] Cour européenne des droits de l'homme, 25 février 1993, Funke c. France, § 57.

ait pas suffisamment de garanties concrètes contre la grande liberté d'appréciation par les services concernés, sans un mécanisme de contrôle clair de l'utilisation des données les plus risquées, alors qu'une obligation de documentation et de motivation s'impose pour les différents responsables en vertu de l'article 5.2 du RGPD (ce qu'on appelle le principe d' "accountability").

26. L'Autorité met également en cause la conformité du dernier alinéa de l'article 11 du projet vis-à-vis du principe de minimisation des données (article 5.1.c) du RGPD) et des principes de proportionnalité, de protection des données dès la conception et de protection des données par des paramètres standard (article 25 du RGPD).

27. Si le législateur maintient l'article 11, l'Autorité souhaite dès lors, en outre, à la lumière des articles 32 à 36 inclus du RGPD, que chaque augmentation de la fréquence et de l'unité de temps de la lecture des données aille de pair avec un niveau encore plus élevé de **protection des données du compteur** et l'enregistrement dans une **analyse d'impact relative à la protection des données** au niveau des services concernés (le gestionnaire du réseau de distribution, le gestionnaire du réseau de transmission, la société de transport et le gestionnaire du réseau de transport local).

4. Manque de soutien du délégué à la protection des données (article 37 du RGPD)

28. L'article 12 du projet définit de manière très détaillée les conditions que doit remplir le gestionnaire de données. Il est également question d'un "corporate governance comité" au sein de l'organe d'administration du gestionnaire de données (si un administrateur ne répondant pas à l'exigence d'indépendance est désigné).

29. Le même article n'accorde qu'une attention très limitée au délégué à la protection des données (en dehors du principe d'engagement transparent du délégué), et ce en contradiction avec le rôle crucial que cette (ces) personne(s) devra (devront) remplir en vertu du RGPD (nouvel article 3.1.83, § 4). Le fait que le projet accorde bien plus d'attention aux exigences du gestionnaire de données donne l'impression et crée le risque que le rôle du délégué à la protection des données devienne, dans la pratique, une "boîte vide" à l'égard du Conseil d'administration du gestionnaire de données et du "corporate governance comité" dont le fonctionnement a toutefois été réglé.

30. Le projet doit explicitement tenir compte du fait que le délégué à la protection des données doit pouvoir faire **directement rapport** à l'organe d'administration du gestionnaire de données ("**le niveau le plus élevé de la direction**" au sens de l'article 38.3 du RGPD).

31. Le projet aurait aussi pu ajouter l'implication du délégué à la protection des données dans plusieurs dispositions concrètes à l'article 12 du projet. L'article 12 ne définit nulle part si et comment

le délégué à la protection des données doit être **associé aux analyses d'impact relatives à la protection des données périodiques et complémentaires** en vertu du nouvel article 3.1.83, § 3, alors que selon le RGPD, cela doit avoir lieu pour "*toutes les questions relatives à la protection des données à caractère personnel*" (articles 38.1 et 38.2 du RGPD). On peut ainsi s'attendre à ce que le délégué à la protection des données soit aussi associé aux aspects mentionnés à l'article 12 du projet comme :

- des discussions relatives à la gestion des risques (mentionnée dans un nouvel article 3.1.69 de l'article 12 du projet), dont des demandes d'augmentation de la fréquence et de l'unité de temps de la transmission de données à caractère personnel (article 11 du projet)
- des décisions pertinentes (pour la protection des données) du Conseil d'administration ou du "corporate governance comité"
- la conclusion d'un contrat de sous-traitance (mentionné dans un nouvel article 3.1.82 de l'article 12 du projet qui renvoie à l'article 28.3 du RGPD)
- le traitement de questions et de plaintes (en matière de protection des données) émanant de personnes concernées
- les cas où, selon un nouvel article 3.1.82 *in fine* de l'article 12 du projet, le sous-traitant doit prêter assistance au gestionnaire de données, à savoir :

"1° pour la réponse à une demande de la personne concernée d'exercer ses droits en vertu du règlement général sur la protection des données ;
2° pour la notification d'une violation de données à caractère personnel à l'autorité de contrôle concernée ou à la personne concernée ;
3° pour la réalisation d'une analyse d'impact relative à la protection des données et de l'éventuelle consultation préalable de l'autorité de protection des données ;
4° pour la réalisation d'un audit ou d'une inspection par le gestionnaire de données ou par une personne qui y a été habilitée par le gestionnaire de données."

32. Il serait souhaitable d'également accorder de l'attention à un règlement visant à prévenir et traiter des conflits d'intérêts internes au sein du gestionnaire de données s'il s'agit de discussions relatives à la protection de la vie privée et des données (par ex. différence de point de vue entre le service juridique, le "corporate governance comité" et le délégué à la protection des données, ...). Dans le cadre de l'article 5.2 du RGPD (responsabilité ou "accountability"), il importe que les avis et recommandations du délégué à la protection des données soient conservés et que d'éventuelles décisions dans lesquelles ses avis sont ou non suivis par le président du Conseil d'administration puissent être consultées et suivies par l'autorité de contrôle.

33. Le délégué à la protection des données est normalement la personne de contact des personnes concernées, comme par exemple dans le cas de fuites de données (article 38.4 du RGPD). L'article 12 du projet prévoit la possibilité de désigner une autre personne de contact que le délégué à la protection des données[16] en cas de fuites de données. Bien que le RGPD ne l'interdise pas (toutes les instances visées ne devront pas désigner un délégué à la protection des données), le choix d'une personne de contact (par ex. au sein du service clientèle) peut toutefois comporter un risque de conflit d'intérêts et dans ce cas, il est toutefois préférable de prévoir une transparence à l'égard du délégué à la protection des données et/ou une délégation par ce dernier à une personne de contact. L'autorité de contrôle pourra quoi qu'il en soit également s'adresser au délégué à la protection des données, même si l'organisation a désigné une autre personne de contact. Le RGPD dispose en effet que le délégué à la protection des données devra collaborer avec l'autorité de contrôle (article 39.1.d) du RGPD).

5. Transparence supplémentaire concernant les flux de données

34. L'Autorité prend acte des règles complémentaires en matière de transparence qui sont ajoutées à l'article 12 du projet (nouveaux articles 3.1.80 et 3.1.81). L'utilisateur du réseau pourra consulter gratuitement sur un portail Internet personnel les informations complémentaires suivantes concernant le statut de son port utilisateur et les flux de données :

> *"1° des informations sur les possibilités et le statut des ports utilisateurs de l'utilisateur du réseau, mentionnés à l'article 3.1.45, § 2 ;*
> *2° la possibilité de donner son consentement[17] pour ouvrir ou fermer les ports utilisateurs gratuitement ;*
> *3° un relevé des parties qui ont accès, via un consentement[18], aux données validées de l'utilisateur du réseau, ainsi que les données validées, la date à partir de laquelle le consentement prend effet et la mention soit de la date de fin du consentement, soit que le consentement est valable jusqu'à ce que celui-ci soit retiré ;*
> *4° le renvoi et l'hyperlien vers le relevé des parties mandatées qui est mis à disposition sur le site Internet du VREG* [NdT : Vlaamse regulator van de energiemarkt (régulateur flamand du marché de l'énergie)]*, tel que mentionné à l'article 3.1.81, troisième alinéa du présent arrêté".*

[16] Voir la formulation dans le nouvel article 3.1.83, § 5 (article 12 du projet).
"Les parties mentionnées au premier alinéa désignent une personne de contact, communiquent aux personnes concernées, via leur site Internet, qui est cette personne de contact et mettent en place une procédure permettant aux personnes concernées d'exercer simplement les droits qui leur sont attribués en vertu du règlement général.
Les parties mentionnées au premier alinéa désignent également une personne de contact qui fait office d'interlocuteur pour l'autorité de protection des données."
[17] Usage abusif de la notion de consentement (pas au sens du RGPD).
[18] Usage abusif de la notion de consentement (pas au sens du RGPD).

35. L'Autorité estime que ce qui précède est pertinent au sens de l'arrêt Smaranda Bara de la Cour de Justice[19]. Elle attire l'attention du demandeur sur le fait qu'une double extension de la transparence susmentionnée est nécessaire pour garantir la conformité avec le RGPD :

- Limiter les informations à une liste des parties n'est pas suffisant. Pour avoir le moindre sens, les informations doivent également concerner "[les] finalités de ce traitement ainsi que [les] catégories de données concernées"[20] (voir par analogie la liste des autorisations publiée par plusieurs services publics sur leur site Internet).
- On a déjà[21] fait remarquer que le demandeur doit accorder une attention aux cas dans lesquels la personne concernée (au sens du RGPD) ne sera pas l'utilisateur du réseau. Une plus grande attention doit être accordée à l'application des droits d'accès (article 15 du RGPD) et à l'information en vertu des articles 13 et 14 du RGPD même si la personne concernée n'est pas l'utilisateur du réseau. Dans la pratique, le projet devrait prévoir une procédure pour également offrir à la personne concernée une transparence égale à celle offerte à l'utilisateur du réseau. En cas de différend au sein d'un ménage entre deux conjoints concernant les données exactes du compteur, il n'est pas logique, à la lumière du RGPD, que la personne ayant le statut d'utilisateur du réseau bénéficie d'un statut privilégié en matière de transparence.

6. Un datawarehouse des compteurs intelligents et la comparaison et le croisement des données

36. L'article 12 du projet insère un nouvel article 3.1.82, § 3 qui est libellé comme suit :

"§ 3. Les données à caractère personnel que les parties, mentionnées aux articles 4.1.22/6 à 4.1.22/13 inclus du Décret sur l'Énergie du 8 mai 2009[22], traitent sont conservées dans une banque de données qui ne peut être comparée à ou croisée avec d'autres données que dans les cas où cela est défini légalement ou si cela est absolument nécessaire pour l'exécution d'obligations légales.

[19] Cour de Justice, 1er octobre 2015 (C-201/14), Smaranda Bara e.a., § 39.
[20] Considérant 43 de l'arrêt Smaranda Bara.
[21] Voir le point 44 de l'avis n° 07/2018 susmentionné du 17 janvier 2018.
[22] Il s'agit notamment de traitements par le gestionnaire de données (4.1.22/6), les gestionnaires de réseau et leur société de travail (4.1.22/7), les fournisseurs d'énergie (4.1.22/8), les fournisseurs de services énergétiques (4.1.22/9), le responsable de l'équilibre et l'affréteur (4.1.22/10), les pouvoirs publics (pour les données qu'ils sont autorisés à connaître en vertu d'une loi, d'un décret ou d'une ordonnance) (4.1.22/11), les institutions et les personnes physiques ou morales (pour les informations dont elles ont besoin pour remplir les missions d'intérêt public qui leur ont été confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance) (4.1.22/12) et le VREG (4.1.22/13). Selon le demandeur, ces dispositions citées du Décret sur l'Énergie (qui doit être modifié) (articles 4.1.22/6 à 4.1.22/13 inclus) n'étaient pas encore entrées en vigueur le 02/08/2018, ni publiées officiellement. Le 29 juin 2018, le Gouvernement flamand a approuvé définitivement le projet de décret modificatif, après quoi ce dernier a été déposé auprès du Parlement flamand.

Le VREG met à disposition sur son site Internet une liste des situations dans lesquelles il est légalement établi que des banques de données peuvent être combinées.

La banque de données, mentionnée au premier alinéa, n'est accessible qu'aux personnes qui travaillent au sein ou pour les différentes parties, pour lesquelles il est nécessaire d'exécuter les missions mentionnées aux articles 4.1.22/6 à 4.1.22/13 inclus du décret susmentionné. Cette banque de données est sécurisée au moyen de mesures techniques appropriées afin de garantir la sécurité de l'information. Les données à caractère personnel que les parties, mentionnées aux articles 4.1.22/6 à 4.1.22/13 inclus du décret susmentionné, traitent sont autant que possible pseudonymisées et cryptées."

37. L'explication dans la Note au Gouvernement flamand est très sommaire et n'apporte pas grand-chose de plus[23].

38. L'Autorité constate que le paragraphe précédent implique la création d'un **datawarehouse** qui est alimenté par diverses parties du secteur privé et du secteur public. Elle attire l'attention du demandeur sur les risques substantiels qui vont de pair avec chaque concentration de données et sur une liste de recommandations[24] et d'avis[25] antérieurs de la Commission concernant des projets similaires.

39. En principe, l'Autorité n'est pas favorable à la création d'un datawarehouse. Le concept n'est a priori pas proportionnel, ni nécessaire, comparé au modèle d'une banque-carrefour qui peut servir une finalité similaire avec une meilleure sécurité par le biais d'une fonction de contrôle et de référence.

---

[23] "Au paragraphe trois, des exigences sont imposées à la banque de données dans laquelle les données sont conservées. Les données provenant de cette banque de données ne peuvent être comparées ou croisées avec d'autres données que dans les cas où cela est établi légalement ou si cela est absolument nécessaire pour l'exécution d'obligations légales. Cette banque de données doit être sécurisée au moyen de mesures techniques appropriées. Les mesures antivirus nécessaires sont au moins prises et les contrôles d'accès effectués, par exemple via un mot de passe ou un code d'accès."

[24] Recommandation d'initiative n° 01/2012 du 18 janvier 2012 *concernant la possibilité d'un inventaire des banques de données pertinentes et d'une amélioration de l'échange d'informations dans le cadre de la lutte contre la fraude sociale*, publiée à l'adresse suivante : https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2012_0.pdf..

[25] Avis n° 06/2012 du 8 février 2012 *relatif à l'avant-projet de loi-programme en ce qui concerne la lutte contre la fraude et plus particulièrement le contrôle sur l'abus des adresses fictives par les assurés sociaux* , publié à l'adresse suivante : http://www.privacycommission.be/sites/privacycommission/files/documents/avis_06_2012_0.pdf ; avis n° 24/2015 du 17 juin 2015 *sur le Chapitre II du projet de loi portant des dispositions diverses, relatif aux données de consommation des sociétés de distribution et des gestionnaires de réseaux de distribution*, publié à l'adresse suivante : https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/avis_24_2015.pdf ; avis n° 05/2016 du 3 février 2016 *sur un projet de loi modifiant la loi-programme du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires des prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation des sociétés de distribution et des gestionnaires de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale*, publié à l'adresse suivante : https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/avis_05_2016.pdf ; ; points 26 et suivants de l'avis n° 34/2018 du 11 avril 2018 *concernant un avant-projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre 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*, publié à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_34_2018.pdf..

40. La manière de décrire la création d'un datawarehouse dans le projet suscite plusieurs remarques substantielles d'un point de vue du droit à la protection de la vie privée et des données :

- Une base légale claire dans le Décret sur l'Énergie pour la création d'un datawarehouse sur le marché flamand de l'énergie semble faire défaut, alors que seule une loi formelle peut régir une telle ingérence[26] substantielle (article 22 de la Constitution). Le VREG ne peut dès lors établir une liste de telles bases légales dans la législation flamande en matière d'énergie qui satisfont aux exigences des articles 8 de la CEDH et 22 de la Constitution.
- Le projet ne contient pas les éléments suivants de l'article 6.3 du RGPD qui sont nécessaires pour faire comprendre de manière concluante l'ingérence dans la vie privée si une obligation légale ou une mission d'intérêt public sont invoquées.
  a) les types de données traitées (les "données à caractère personnel que les parties (...) traitent" ne constituent pas une définition claire) ;
  b) les personnes concernées qui peuvent faire l'objet de la mesure (chaque utilisateur du réseau peut être visé par la disposition) ;
  c) la limitation des finalités (la banque de données est alimentée par les sources de données les plus diverses avec des finalités sources propres) ;
  d) les durées de conservation (ne sont pas déterminées) ;
  e) les procédures et activités de traitement[27], dont des mesures pour veiller à un traitement licite et loyal (ne sont pas déterminées) ;
  f) l'indication d'une finalité d'intérêt public (les finalités définies "dans les cas où cela est légalement établi ou cela est absolument nécessaire pour l'exécution d'obligations légales" est une formulation beaucoup trop vague pour être considérée comme une finalité claire et une disposition légale prévisible) ;
  g) la proportionnalité de l'utilisation du datawarehouse et de la comparaison de fichiers avec la finalité légitime poursuivie.

- Le responsable du traitement pour la banque de données n'est pas défini clairement, de sorte que la question de (la possibilité de) l'exercice des droits des personnes concernées à l'égard de ce traitement n'est *de facto* pas prévue, ni facilitée.
- L'application des cas concrets d'ingérence dans la vie privée (croisement et comparaison de banques de données) n'est pas définie suffisamment clairement et n'est pas suffisamment prévisible.
- On ne sait pas clairement à quel traitement la garantie "autant que possible pseudonymisées et cryptées" se rapporte.

[26] Cour européenne des droits de l'homme, 4 décembre 2008, S. et Marper c. Royaume-Uni, § 67.
[27] Par exemple l'utilisation de l'eID.

- L'intervention d'un "Trusted Third Party" (TTP ou tiers de confiance) n'est pas prévue, ni l'existence d'un mécanisme de contrôle indépendant qui veille à l'utilisation correcte de ce datawarehouse (pas de contrôle intégré des demandes). Pourtant, le précédent avis n° 47/2017 du 20 septembre 2017 de la Commission[28] renvoyait notamment à ces exigences à l'égard des gestionnaires de réseaux de distribution.

41. L'Autorité conclut que le nouvel article 3.1.82, § 3 de l'article 12 du projet (concernant le datawarehouse et les compétences d'enquête y afférentes de comparer et de croiser des fichiers) ne répond pas aux exigences des articles 8 de la CEDH et 22 de la Constitution.

IV. CONCLUSION

L'Autorité estime que le projet présente de graves manquements sur certains points importants :

- avec l'ouverture du niveau le plus élevé de fréquence et d'unité de temps des données de compteurs intelligents à la demande de certains services sur le marché de l'énergie, l'article 11 du projet crée une possibilité d'ingérence grave dans la vie privée via des données à caractère personnel qualifiées pour laquelle les risques n'ont pas été suffisamment examinés à la lumière du RGPD (points 17-27). Face à ces risques, le cadre légal n'offre pas suffisamment de garanties précises pour encadrer de manière efficace une consultation arbitraire dans des cas présentant un risque élevé ;
- l'article 12 du projet ne soutient pas suffisamment le délégué à la protection des données auprès du gestionnaire de données. Le délégué ne peut dès lors pas assurer son rôle comme le requiert le RGPD (points 28-33) ;
- le règlement concernant la création d'un datawarehouse et la comparaison et le croisement de données dans le nouvel article 3.1.82, § 3 de l'article 12 du projet présente de graves manquements à la lumière des exigences des articles 8 de la CEDH, 22 de la Constitution et 6.3 du RGPD (points 36-41).

Le projet suit sur plusieurs points des avis antérieurs de la Commission. Il accorde notamment une plus grande attention :

- à l'indépendance du gestionnaire de données
- au suivi des risques via une analyse d'impact relative à la protection des données
- à la mise en œuvre d'une transparence supplémentaire pour l'utilisateur du réseau (points 34 et 35).

[28] Voir les points 15 et 16 de cet avis, publié à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_47_2017.pdf..

D'un point de vue terminologique, le projet n'est pas toujours cohérent à la lumière du RGPD. Ainsi, l'ouverture (la fermeture) d'un port utilisateur et/ou la conclusion d'un contrat avec un fournisseur pour obtenir un tarif variable ne peut pas, en soi, être assimilée à l'octroi d'un consentement au sens du RGPD pour l'utilisation des données à caractère personnel en question. L'emploi des termes "utilisateur du réseau" à la place de "personne concernée" dans le projet a des conséquences concrètes (par ex. en matière de transparence supplémentaire) pour lesquelles l'Autorité demande plus d'attention (points 13, 19 et 35).

PAR CES MOTIFS,

l'Autorité ne se prononce pas sur les diverses dispositions du projet qui n'impliquent pas un traitement de données à caractère personnel ;

l'Autorité émet un **avis défavorable** sur les dispositions évoquées des articles 11 et 12 du projet qui concernent (1) la possibilité d'augmenter la fréquence et l'unité de temps de la lecture des compteurs numériques sans base légale, ni garanties, (2) l'absence de soutien de la position du délégué à la protection des données et (3) l'absence d'un cadre légal efficace et de garanties pour la création d'un datawarehouse ;

émet un avis favorable quant au reste.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere