



Avis n° 73/2017 du 13 décembre 2017

Objet : Projet d'arrêté du Gouvernement flamand modifiant l'arrêté relatif à l'énergie du 19 novembre 2010 (CO-A-2017-073)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu la demande d'avis du Ministre flamand du Budget, des Finances et de l'Énergie, reçue le 30 octobre 2017 ;

Vu le rapport du Président ;

Émet, le 13 décembre 2017, l'avis suivant :

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement général 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 la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016^[1].

Le Règlement, couramment appelé RGPD (Règlement général sur la protection des données), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et est automatiquement applicable deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) de l'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. La Commission vie privée s'est déjà prononcée dans 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) du ministre flamand du Budget, des Finances et de l'Énergie (ci-après "l'avis 17/2017").

^[1] 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)

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil*

<http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC>

<http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC.>

2. Le 30 octobre 2017, la Commission 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 (ci-après "le projet d'arrêté") du Gouvernement flamand modifiant l'arrêté relatif à l'énergie du 19 novembre 2010 en ce qui concerne la définition des conditions, visées à l'article 4.1.22/2, § 3 du décret sur l'énergie du 8 mai 2009, auxquelles les compteurs numériques doivent satisfaire.

II. CONTENU DU PROJET

3. Le présent projet d'arrêté exécute l'article 4.1.22/2, § 3 du décret sur l'énergie en vertu duquel le Gouvernement flamand arrête les conditions auxquelles les compteurs numériques et le "système de mesure"¹ doivent satisfaire. Sont principalement visées ici les fonctionnalités (minimales et techniques) auxquelles les compteurs (d'électricité) intelligents doivent satisfaire, lesquelles sont énumérées à l'article 1 de l'arrêté. Cet article insère une section IX dans le titre III, chapitre I de l'arrêté du Gouvernement flamand relatif à l'énergie du 19 novembre 2010.

4. Les articles 2 et 3 du projet d'arrêté concernent l'introduction d'un "in-homedisplay" (dispositif d'affichage à domicile) via lequel la personne concernée peut visualiser les soldes (montant rechargé, ...) des compteurs d'électricité et de gaz. Vu que ces articles ne comportent aucun risque particulier pour la vie privée, ils ne sont pas examinés plus avant dans ce qui suit.

III. EXAMEN DU PROJET

1. Relation entre la liste des fonctionnalités et la LVP ainsi que le RGPD

5. Les fonctionnalités mentionnées à l'article 1 du projet d'arrêté impliqueront intrinsèquement un traitement de données à caractère personnel ou auront un impact direct en la matière (par ex. en ce qui concerne la sécurité). Tel est le cas pour les fonctionnalités des données de communication via un port d'utilisateur local d'un compteur (voir ci-après), la fonctionnalité d'ouverture et de fermeture à distance d'un circuit, une reconfiguration et une mise à jour à distance d'un micrologiciel, ...

6. Chaque fonctionnalité aura en outre un profil de risque déterminé, ce qui est pertinent en vertu du RGPD mais n'est pas reflété en tant que tel dans le projet d'arrêté. La Commission souhaite que le projet d'arrêté en tienne quand même compte afin de pouvoir garantir une application correcte du RGPD à partir du 25 mai 2018 (voir ci-après).

¹ Dans la note au Gouvernement flamand, il est fait référence au "consumer energy management system" ou "CEMS".

2. Proportionnalité et principes de protection des données dès la conception et de protection des données par défaut

7. Le projet d'arrêté insère un nouvel article 3.1.45, § 2 dans l'arrêté relatif à l'énergie. Cet article est libellé comme suit :

"§ 2. Le compteur numérique d'électricité est équipé d'un port utilisateur permettant de connecter des applications au niveau de l'utilisateur du réseau de distribution d'électricité et d'envoyer des informations à ces applications, afin que ces informations soient lisibles et utilisables par la personne compétente pour traiter ces informations.

*Les données de mesures suivantes **sont envoyées au port utilisateur par seconde et par période tarifaire applicable** :*

- 1° la puissance active actuelle, visée au paragraphe 1, 1° ;*
- 2° les relevés actuels en kWh, visés au paragraphe 1, 2° ;*
- 3° la qualité de la fourniture d'électricité, visée au paragraphe 1, 5° ;*
- 4° le statut de l'équipement de mesure, visé au paragraphe 1, 6°." [Ndt : tous les passages extraits du projet d'arrêté sont des traductions libres effectuées par le Secrétariat de la Commission, en l'absence de traduction officielle]*

8. D'après le demandeur, le compteur numérique mesure : " *les flux d'énergie par seconde et ces données sont dès lors disponibles localement en tant que telles via le port P1 ainsi que pour les différentes applications qui peuvent y être connectées. Cette granularité fine est souhaitée notamment par exemple pour les visualisations. Les données de mesures qui sont échangées avec le gestionnaire de données sont en effet des données quadrihoraires. Pour les applications où des données sont réclamées auprès du gestionnaire de données, ceci est en effet suffisant. L'échange de données par seconde avec le gestionnaire de données aurait également pour effet que de beaucoup plus grandes quantités de données devraient être échangées/conservées et traitées.*"

9. La Commission constate que le projet d'arrêté **se fonde sur le traitement de données de mesure par seconde** (lors de la communication via le "port utilisateur" P1), ceci alors que dans le nouvel article 3.1.45, § 1 (pour une autre fonctionnalité), on se base sur une granularité plus élevée au niveau de l'enregistrement (intervalle de **15 minutes**)².

² " Art. 3.1.45. § 1. Le compteur numérique pour l'électricité placé par le gestionnaire de réseau de distribution ou par le gestionnaire d'un réseau de distribution fermé convient pour :

- ^{1°} enregistrer la puissance active actuelle en watts et la puissance réactive actuelle en VAR tant lors du prélèvement que lors de l'injection et indiquer la puissance active actuelle sur l'écran d'affichage du compteur ;
- ^{2°} enregistrer l'index actuel en kWh et en kVAh pour l'électricité prélevée et pour l'électricité injectée pour les différentes périodes d'utilisation et indiquer l'index actuel sur l'écran d'affichage du compteur ;

10. La Commission estime que la possibilité de suivre de manière continue le comportement (relatif à l'énergie) d'une personne physique d'une manière détaillée au maximum (par seconde) comporte un risque particulièrement élevé d'abus de telles données de mesures à haute granularité, ce contre quoi la personne concernée doit être suffisamment protégée. C'est d'autant plus le cas si la personne concernée est autorisée à connecter les applications les plus diverses (notamment GSM) de différents fournisseurs de services énergétiques au port P1, ce qui semble être l'intention de l'article 1 du projet d'arrêté.

11. Il est également frappant de constater que la note au Gouvernement ne motive aucunement pourquoi une telle fonctionnalité à risque devrait être prévue, ce qui avait fait l'objet d'une demande d'informations complémentaires au demandeur par la Commission. Il ressort d'une réponse du demandeur reçue le 1^{er} décembre 2017 que la fonctionnalité de la communication par seconde via le P1 est demandée par les fournisseurs de services énergétiques. La réponse précise ce qui suit : *"Cette granularité permet de formuler des propositions d'économie et de donner des conseils à distance, de remettre des prix pour le prélèvement d'énergie renouvelable produite localement, ainsi que de prendre des rendez-vous pour des solutions de flexibilité (par exemple le débranchement temporaire à distance d'appareils énergivores tels que des congélateurs afin de pouvoir surmonter des pics de demandes de consommation, ..."*. Dans une réponse complémentaire reçue le 3 décembre 2017, le demandeur se réfère à une réponse d'un gestionnaire de réseau de distribution qui indique que le port P1 sera intégré à l'analyse d'impact relative à la protection des données ("DPIA"), *dans laquelle "une attention spécifique sera consacrée aux risques inhérents à l'ouverture par défaut de ce port lors du placement du compteur numérique"*. D'autre part, le gestionnaire de réseau de distribution affirme ceci : *"Nous confirmons dès à présent que le gestionnaire de réseau pourra fermer le port à distance sur simple demande de l'utilisateur du réseau"*².

12. La Commission déduit de cette option que la mise à disposition de données non agrégées via le port P1 aux diverses applications externes de tiers telles que des applications GSM d'un fournisseur d'énergie sera possible de manière standard, impliquant le risque de nombreux traitements dérivés (profilage, data mining, marketing direct) qui seront proposés uniquement en combinaison avec la fourniture du service énergétique proprement dit.

^{3°} enregistrer comme granularité la plus fine les données, mentionnées au point 2°, par quart d'heure ;"

13. Bien que la Commission prenne acte de la remarque formulée dans la lettre d'accompagnement du demandeur selon laquelle le statut ouvert ou fermé du port P1 constitue un aspect qui sera examiné dans un projet d'arrêté à venir, il ressort malgré tout de la réponse susmentionnée du demandeur que cette question est manifestement déjà décidée par les gestionnaires de réseau de distribution.

14. La combinaison du statut ouvert par défaut du port P1 et de la communication par défaut "par seconde" des valeurs de données aux fournisseurs de services énergétiques n'offre pas une protection "par défaut" suffisante, même si cet aspect est intégré ultérieurement dans un DPIA par une instance qui a manifestement déjà décidé que le compteur devait par défaut être ouvert.

15. La Commission considère au contraire que la personne concernée doit pouvoir donner son **consentement**³ libre, spécifique et basé sur des informations préalables concernant la transmission de ses propres données à caractère personnel via le port P1 aux fournisseurs de services énergétiques. C'est ce qui découle des principes de proportionnalité ainsi que des principes de protection des données dès la conception ("privacy by design") et de protection des données par défaut ("privacy by default"), auxquels elle s'est déjà référée dans un précédent avis.⁴

16. Par ailleurs, l'option **permettant la fermeture totale du port** ne permet pas à l'utilisateur du réseau de pouvoir profiter quand même des services énergétiques qui lui sont utiles sans corrompre également d'emblée la protection de ses données. La cause en est le couplage automatique fréquent d'un service commercial à la réutilisation comme le profilage, les traitements en vue de marketing direct par des fournisseurs de services énergétiques et/ou de parties commerciales au sein ou en dehors du marché de l'énergie, pour qui de telles données relatives aux habitudes domestiques (liées à l'énergie) sont extrêmement intéressantes, sans que la personne concernée soit suffisamment informée de ces traitements dérivés.

17. L'option de la "**semi-fermeture**" du port via un **droit particulier d'opposition** pourrait être inscrite dans le décret sur l'énergie en tant que fonctionnalité, en combinaison avec le consentement de la personne concernée. Ainsi, le demandeur pourrait aussi bien bénéficier du service énergétique à sa demande spécifique, mais aussi faire en sorte que la demande du service énergétique n'implique pas d'emblée qu'il y ait toutes sortes de traitements commerciaux ultérieurs (dérivés) par

³ Voir l'article 1^{er}, § 8 de la LVP et la notion renforcée de consentement en vertu du RGPD.

⁴ CPVP, avis n° 17/2017 du 12 avril 2017 *relatif au projet de note "uitrol van digitale meters in Vlaanderen" (déploiement des compteurs numériques en Flandre)* du ministre flamand du Budget, des Finances et de l'Énergie, publié sur https://www.privacycommission.be/sites/privacycommission/files/documents/avis_17_2017.pdf

des fournisseurs d'énergie, comme du profilage commercial, un traitement en vue de marketing direct, le commerce de données à caractère personnel. Ceci découle d'ailleurs déjà du caractère "spécifique" du consentement, mais il est utile d'insister davantage, dans le décret sur l'énergie, sur cette option plus équilibrée pour la personne concernée.

3. Sécurité de données à caractère personnel associées à certaines fonctionnalités.

18. Un certain nombre de fonctionnalités de l'article 1 du projet d'arrêté comporteront, par nature, un risque (élevé) particulier pour les droits et libertés des personnes physiques. Tel est le cas pour les fonctionnalités en rapport avec le profil de la personne concernée (client domestique, PME, ...) et qui peuvent impliquer des conséquences ou des décisions pour la personne concernée, comme c'est le cas pour :

- les informations sur le "mauvais usage ou l'usage contraire de l'installation de mesure ou toute tentative en ce sens", qui peuvent fournir une indication de fraude à l'énergie dans le chef de la personne concernée ;
- les conditions d'utilisation détaillées (avec comme granularité la plus fine les mesures quadrihoraires), qui peuvent donner une compréhension particulière des habitudes de la personne concernée (périodes d'absence de l'habitation, type de profil de consommation, ...) ;
- le fonctionnement du compteur en mode prépaiement qui peut contenir une indication d'une donnée à caractère personnel sensible dans la mesure où ceci porte sur un mode de compteur à budget (plutôt qu'une option de futur prépaiement commercial) ;
- la possibilité pour la personne concernée de connecter des applications via le port utilisateur sur le compteur intelligent (nouvel article 3.1.45, § 2 de l'arrêté relatif à l'énergie), ce qui accroît le risque de fuites de sécurité (voir les risques propres aux autorisations beaucoup trop larges dans les applications GSM) ;
- la disponibilité (entre autres) de données de mesure par seconde en cas de lecture via le port utilisateur.

19. Le traitement des données associé à certaines autres finalités implique un niveau de risque plus important pour les droits et libertés des personnes concernées, comme les données qui enregistrent la qualité de la fourniture d'électricité (tension fournie en volts).

20. La constatation susmentionnée de la présence d'un niveau de risque différent selon la fonctionnalité aura un impact particulier sur les obligations y afférentes du responsable du traitement au niveau de (en s'adaptant au risque) la sécurité, de l'évaluation et de la gestion du risque selon les fonctionnalités correspondantes, et de la prise en compte de ces aspects en vertu de l'analyse d'impact relative à la protection des données ("DPIA"), de l'obligation d'information (de la personne concernée) des violations de sécurité et de l'obligation de consultation à l'égard de l'autorité de protection des données en cas de risque résiduel élevé.

21. Il ressort de ce qui précède que les gestionnaires de réseau de distribution devront prouver à l'autorité de protection des données qu'ils prennent des mesures adaptées pour maîtriser et assurer le suivi des risques inhérents élevés pour les droits et libertés des personnes concernées qui sont propres aux fonctionnalités susmentionnées ("risk assessment" et "risk management").

22. La Commission estime approprié que le projet d'arrêté consacre également explicitement une attention au risque propre à chaque fonctionnalité ainsi qu'à l'obligation des gestionnaires de réseau de distribution et/ou des gestionnaires du système de mesure ("CEMS") de tenir compte de la variabilité des risques pour les personnes concernées en vertu des articles 25 et 32 à 36 inclus du RGPD.

IV. CONCLUSION

23. Le point d'attention principal dans le texte est la fonctionnalité (potentielle) à l'article 1 de l'arrêté (un nouvel article 3.1.45, § 2 du décret sur l'énergie) concernant la transmission des données de mesure par seconde via le port P1 (points 7 à 13 inclus), combinée à l'ouverture par défaut du port. Ceci n'est pas compatible avec la légitimation du traitement sur la base du consentement, les principes de proportionnalité, la protection des données dès la conception et la protection des données par défaut.

24. Pour le reste, la Commission estime que le projet offre suffisamment de garanties de protection des données à caractère personnel concernées, à condition d'intégrer les remarques suivantes : la prise en compte des risques de chaque fonctionnalité pour les personnes concernées et leur intégration dans une analyse d'impact relative à la protection des données (voir les points 18 à 20 inclus) ;

PAR CES MOTIFS,

la Commission émet un **avis défavorable** sur la combinaison de l'ouverture par défaut du port P1 et de la communication par défaut des valeurs de données "par seconde" aux fournisseurs de services énergétiques. Elle considère cette combinaison comme contraire aux principes de proportionnalité, de "privacy by design" et de "privacy by default" ainsi qu'à l'exigence d'un traitement légitime sur la base du consentement de la personne concernée (compris au sens de la LVP et du RGPD).

La Commission émet pour le reste un **avis favorable** sur le projet d'arrêté, à condition qu'il soit tenu compte des remarques formulées aux points 6 et 18 à 20 inclus.

L'Administrateur f.f.,

Le Président,

(sé) An Machtens

(sé) Willem Debeuckelaere