Avis n° 84/2018 du 14 septembre 2018

Objet : Projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (CO-A-2018-070)

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 de M. Michel, Premier ministre, reçue le 20 juillet 2018 ;

Vu le rapport de Monsieur F. De Smet ;

Émet, le 14 septembre 2018, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le 20 juillet 2018, le Premier ministre (ci-après "le demandeur") a sollicité l'avis de l'Autorité sur un projet de loi *établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique* (ci-après "le Projet").

2. Le Projet vise la transposition de la Directive européenne (EU) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 *concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union* (ci-après "la Directive"). Les principaux destinataires des obligations de la Directive sont les entités susceptibles, en cas d'incident affectant la sécurité de leurs réseaux et systèmes d'information, de perturber de manière importante la fourniture de services essentiels et de services numériques essentiels au maintien d'activités sociétales ou économiques critiques[1]. La Directive a notamment pour objectif de veiller à ce que des mesures de sécurité techniques et organisationnelles soient prises par les opérateurs de services essentiels et les fournisseurs de service numérique afin de prévenir les incidents ou d'en limiter l'impact, en vue d'assurer la continuité de ces services. Dans le même esprit, l'obligation de notification d'incidents reprise dans la Directive concerne les incidents ayant un impact significatif sur les services fournis[2].

3. Différentes autorités sont chargées de l'exécution des dispositions du Projet. Le Roi désignera notamment plusieurs autorités qui assureront les rôles suivants[3]:

   - L'Autorité nationale, chargée du suivi et de la coordination de la mise en œuvre de cette loi. Cette Autorité nationale est aussi le "point de contact national unique". Il s'agit d'une fonction de liaison – créée par la Directive – qui doit assurer une coopération européenne ;
   - le centre national de réponse aux incidents de sécurité informatique (ci-après le "NCSIRT"), chargé de recevoir et de traiter les notifications d'incidents des opérateurs de services essentiels et du fournisseur de service numérique, ainsi que des notifications d'autres pays ;
   - les Autorité sectorielles[4] et les centres sectoriels de réponse aux incidents de sécurité informatique (ci-après "SCSIRT"), chargés au sein de leur secteur de veiller à la mise en œuvre des dispositions du Projet ;
   - une autorité chargée de "*maintenir à jour la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information*"[5];

[1] Il s'agit par exemple d'entreprises d'électricité, de fournisseurs d'eau, de transporteurs aériens, d'établissements de crédit, d'établissements de soins de santé, etc. (voir l'annexe 1 du Projet).

- Les services d'inspection qui veillent au respect du Projet et de ses arrêtés d'exécution par les opérateurs de services essentiels ou les fournisseurs de service numérique.

4. Dans le contexte du Projet, les traitements de données réalisés seront (au moins) les suivants :
   - échange général d'informations depuis les opérateurs de services essentiels et les fournisseurs de service numérique vers les autorités visées au point 3 et depuis ces autorités vers d'autres autorités (étrangères)[6];
   - traitement d'informations que les autorités énoncées au point 3 reçoivent de la part des opérateurs de services essentiels et des fournisseurs de service numérique
     - o lors de la notification de leur "*point de contact pour la sécurité informatique*"[7];
     - o dans le cadre de notifications d'incidents[8];
   - traitements par les services d'inspection[9] (cf. point 3, dernière puce) dans le cadre de la surveillance des opérateurs de services essentiels et des fournisseurs de service numérique, et ce notamment en ce qui concerne le respect des exigences de sécurité ou des exigences en matière de notification d'incidents. L'article 44 du Projet octroie à ces services d'inspection de larges pouvoirs d'enquête. Ils peuvent notamment "*procéder à tout examen, contrôle et audition*" et peuvent requérir toutes les informations qu'ils estiment nécessaires à l'exercice de leur mission[10];
   - traitements par les Cours et Tribunaux (dans les procédures pénales) ou par les "autorités sectorielles"[11] (dans les procédures administratives) dans le cadre de la répression d'infractions au Projet ;
   - traitements par le NCSIRT et les SCSIRT dans le cadre de la gestion d'incidents de sécurité[12].

---

[2] Pages 1 à 3 de l'Exposé des motifs du Projet.

[3] Voir l'article 7 du Projet.

[4] Elles seront notamment chargées de l'identification des opérateurs de services essentiels dans leur secteur (cf. article 11 du Projet).

[5] Article 10, § 1 du projet.

[6] Article 9 du projet.

[7] Articles 23 et 34 du Projet.

[8] Articles 24 e.s. et 35 e.s. du Projet.

[9] - Voir le point 3, dernière puce.

- Voir le Titre 4 : Chapitre 1, section 2 & Chapitre 2 du Projet.

[10] Article 44, § 3, 3° du Projet.

[11] Voir le point 3, dernière puce.

[12] Voir le Titre 5 du Projet.

II. EXAMEN DE LA DEMANDE D'AVIS

1. Remarques générales

5. L'Autorité est très positive à l'égard de la *ratio legis* du Projet : protéger au mieux certains réseaux et systèmes d'information qui sont importants pour la sécurité publique. Comme l'indique à juste titre l'Exposé des motifs du Projet (p. 3), une telle gestion des risques de sécurité est conforme au RGPD.

6. L'Autorité accueille également favorablement l'obligation de coopération entre elle-même et les instances énoncées au point 3[13], ainsi que la plateforme commune qui sera créée en vue de notifier les incidents[14]. Spécifiquement à propos de cette plateforme de notification, l'Autorité attire toutefois l'attention sur le fait que – vu le principe de "responsabilité" du RGPD – il faudra veiller, lors de sa conception, à ce qu'il incombe toujours au responsable du traitement de décider à quelle(s) instance(s) il adresse la notification et à laquelle/auxquelles il ne le fait pas. En d'autres termes, la réalisation de cette plateforme ne peut pas impliquer un report de cette responsabilité du responsable du traitement vers une ou plusieurs instances qui reçoivent des notifications via cette plateforme.

7. Par ailleurs, l'Autorité attire l'attention sur le fait que dans la pratique, de nombreux points communs apparaîtront entre les dispositions du Projet et les règles en matière de protection des données. À cet égard, l'Autorité souligne aussi que le RGPD reste intégralement d'application aux traitements de données à caractère personnel qui auront lieu dans le contexte du Projet. Tous les acteurs soumis aux dispositions du Projet devront donc (dans la mesure où ils traitent des données à caractère personnel) tenir compte également de la réglementation en matière de protection des données. Ils pourraient toutefois avoir l'impression erronée qu'ils agissent en toute légalité en respectant les règles du Projet alors qu'ils perdent peut-être le RGPD de vue. L'Autorité plaide dès lors pour :
    - insérer dans le Projet une disposition établissant le principe selon lequel le Projet ne porte pas préjudice au RGPD ainsi qu'aux lois d'exécution nationales y afférentes[15];

[13] Article 8, § 2 du Projet. Les articles 48 et 52 de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données* permet d'ailleurs aussi à l'Autorité de collaborer avec d'autres acteurs dans ce contexte.

[14] Article 31, § 1, dernier alinéa et article 36, § 3 du Projet.

[15] L'article 2 de la Directive semble le permettre, étant donné que cette disposition renvoie aux règles classiques en matière de protection des données (à savoir à l'ancienne Directive 95/46/CE, qui a entre-temps été remplacée par le RGPD) en ce qui concerne le traitement de données à caractère personnel qui sera réalisé dans le présent contexte.

- signaler dans l'Exposé des motifs du Projet les similitudes et différences spécifiques entre les règles du Projet et les obligations du RGPD[16].

2. Finalité

8. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes. L'Autorité constate que le Projet vise une finalité (certes générale) claire et légitime : veiller à ce que des mesures de sécurité techniques et organisationnelles soient prises par les opérateurs de services essentiels afin de prévenir les incidents ou d'en limiter l'impact, en vue d'assurer la continuité de services essentiels. Parallèlement, l'Autorité plaide pour que l'on reprenne explicitement dans le Projet (cf. point 12) la sous-finalité de chaque catégorie distincte de traitements (cf. point 4).

3. Fondement juridique

9. Tout traitement de données à caractère personnel doit reposer sur un fondement juridique au sens de l'article 6 du RGPD. En outre, le traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions est soumis à des conditions strictes (article 10 du RGPD).

10. Pour le traitement de données à caractère personnel qui n'appartiennent pas aux catégories particulières des articles 9 et 10 du RGPD, le Projet peut éventuellement se baser sur les deux fondements juridiques suivants :

- l'article 6.1.c) du RGPD en ce qui concerne les traitements qui sont réalisés par les opérateurs de services essentiels et les fournisseurs de service numérique. Ils communiquent en effet certaines données à caractère personnel aux acteurs visés au point 3, parce que le Projet les y oblige ;
- l'article 6.1. e) du RGPD en ce qui concerne les traitements réalisés par les acteurs visés au point 3. Ils accomplissent en effet une mission d'intérêt public.

[16] À titre d'exemple :

- les articles 24 e.s. et 35 e.s. du Projet imposent une obligation de notification pour les incidents de sécurité, alors que les articles 33 et 34 du RGPD prévoient une obligation de notification pour les "*violations de données à caractère personnel*" ;
- l'article 23, § 1 du Projet prévoit une obligation de notification pour le "*point de contact pour la sécurité des réseaux et systèmes d'information*" et l'article 37.7 du RGPD dispose que les coordonnées du délégué à la protection des données doivent être communiquées à l'autorité de contrôle.

11. À cet égard, l'Autorité attire l'attention sur l'article 6.3 du RGPD qui – lu conjointement avec l'article 8 de la CEDH et l'article 22 de la Constitution -[17] prescrit que la réglementation qui encadre le traitement de données à caractère personnel doit en principe mentionner au moins les éléments essentiels suivants de ce traitement :
    - la finalité du traitement ;
    - les types ou catégories de données à caractère personnel qui feront l'objet du traitement ;
    - les personnes concernées ;
    - les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ;
    - les durées de conservation ;
    - ainsi que la désignation du responsable du traitement.

12. Le Projet doit être précisé et complété en ce sens. Cela pourrait par exemple se faire en insérant dans le Titre 6 du Projet un article précisant, par type de traitement (voir le point 4 ci-avant), au moins la finalité du traitement. Les autres éléments essentiels des traitements doivent également être repris dans cette nouvelle disposition, sauf si une délégation au Roi est prévue à cet effet.

13. À cet égard, l'Autorité attire également l'attention sur l'article 20 de la loi-cadre en matière de protection des données[18] qui impose aux autorités fédérales[19] l'obligation de conclure des protocoles d'accord pour les échanges de données qui sont basés sur l'article 6.1.e) du RGPD.

14. Par ailleurs, l'Autorité constate que des <u>données</u> seront également traitées <u>au sujet de condamnations pénales et d'infractions pénales</u>[20], ce qui concerne des traitements qui, en vertu de l'article 10 du RGPD, ne sont permis que sous le contrôle d'une autorité publique (ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées). En l'occurrence, le traitement de ce type de données sera réalisé sous le contrôle d'une autorité publique, à savoir les acteurs visés au point 3, ce qui est conforme à l'article 10 du RGPD. Cette disposition du RGPD doit par ailleurs aussi être lue conjointement avec les articles

---

[17] Voir les arrêts de la Cour constitutionnelle : arrêt n° 44/2015 du 23 avril 2015 (p. 63), arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et arrêt n° 29/2018 du 15 mars 2018 (p. 26).

[18] Loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*

[19] Un décret flamand impose d'ailleurs des obligations similaires aux services publics flamands (voir l'article 16 du décret du 8 juin 2018 *contenant l'ajustement des décrets au 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)*.)

[20] Voir par exemple l'article 54, premier alinéa, du Projet : le procureur du Roi informera l'autorité sectorielle lorsque que des poursuites pénales ont été engagées.

6 du RGPD[21], 22 de la Constitution et 8 de la CEDH, ce qui implique que – même si le traitement de ce type de données a lieu sous le contrôle d'une autorité publique – les éléments essentiels du traitement de ce type de données doivent également être fixés dans la réglementation, ce qui est encore insuffisamment le cas en l'espèce (voir les points 11-12).

4. Principe de minimisation des données

15. L'article 5.1.c) du RGPD dispose que les données à caractère personnel doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ("minimisation des données").

16. L'Autorité constate avant tout que l'article 9, § 3, dernier alinéa du Projet[22] reprend le principe selon lequel les informations échangées doivent être limitées "au minimum nécessaire et sont proportionnées à l'objectif de cet échange". L'Autorité conseille d'ajouter une disposition similaire au Titre 6 du Projet, afin que cette règle ait un effet transversal. Le Projet comporte en effet encore d'autres dispositions impliquant des traitements de données – voir par exemple les articles 29, 37, § 1 et 62, deuxième alinéa – qui bénéficieraient d'une plus-value du point de vue de la protection des données si elles étaient explicitement soumises au même principe.

17. L'Autorité attire ensuite l'attention sur le fait que le principe de "minimisation des données" implique aussi que lorsqu'une certaine finalité peut être réalisée sans traiter des données à caractère personnel, il faut opter pour cette solution. Les instances énoncées au point 3 doivent avoir pleinement conscience de cela et il peut dès lors être utile de le mentionner dans l'Exposé des motifs du Projet.

5. Délai de conservation

18. Selon l'article 5.1.e) du RGPD, les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. Le Projet ne prévoit un délai de conservation déterminé que pour les traitements relatifs à des infractions (cf. ci-après, point 22, puce 6). Pour les autres finalités de traitements, l'Autorité recommande d'encore prévoir

---

[21] Voir le considérant 51 du RGPD : "(...) *Outre les exigences spécifiques applicables à ce traitement [de données sensibles], les principes généraux et les autres règles du présent règlement devraient s'appliquer, en particulier en ce qui concerne les conditions de licéité du traitement. (...)"*

Voir aussi la p. 15 de l'avis n° 06/2014 du Groupe 29 *sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*.

[22] Voir le point 4, première puce.

- soit dans le Projet, soit dans un arrêté d'exécution - des délais de conservation spécifiques ou des critères de délimitation pour les délais de conservation.

6. Responsabilité

19. L'article 4.7. du RGPD prévoit que pour les traitements dont les finalités et les moyens sont déterminés par la réglementation, le responsable du traitement est celui qui est désigné par la réglementation en question. Le Projet ne désigne aucun responsable du traitement et l'Autorité recommande de combler cette lacune (par exemple au Titre 6 du Projet).

20. L'Autorité constate par ailleurs que les opérateurs de services essentiels, les fournisseurs de service numérique ainsi que les autorités énoncées au point 3, doivent tous, en vertu du Projet, désigner un délégué à la protection des données[23]. Elle accueille bien entendu favorablement cette mesure.

7. Droit des personnes concernées

21. L'article 23 du RGPD autorise les États membres à prévoir, dans certaines limites déterminées et pour des objectifs spécifiques, des exceptions aux droits des personnes concernées. Les finalités spécifiques pour lesquelles c'est possible sont énoncées à l'article 23.1 du RGPD. Toute mesure législative prévoyant des limitations aux droits de la personne concernée doit au moins contenir des dispositions spécifiques relatives aux éléments énumérés à l'article 23.2 du RGPD, comme :
    - les finalités du traitement (ou des catégories de traitement),
    - les catégories de données à caractère personnel,
    - l'étendue des limitations introduites,
    - les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites,
    - la détermination du (des) responsable(s) du traitement (ou des catégories de responsables du traitement),
    - les durées de conservation,
    - les risques pour les droits et libertés des personnes concernées et
    - le droit des personnes concernées d'être informées de la limitation.

22. L'Autorité analyse ci-après dans quelle mesure ces conditions sont respectées :
    - en ce qui concerne la finalité du traitement : dans le cadre de *"la notification des incidents" et des "contrôles visés au Titre 4 du Projet"*, le Projet exclut tous les

[23] Article 66 du Projet. L'Autorité estime d'ailleurs que cet article devrait se situer juste avant l'article 65 du Projet, étant donné qu'il est à présent situé entre deux articles qui traitent d'un autre sujet (à savoir la limitation des droits de la personne concernée).

droits visés aux articles 12 à 22 inclus du RGPD[24]. L'Autorité fait remarquer que la description de la finalité "*les contrôles visés au Titre 4 du Projet*" devrait être développée avec plus de précision. Cela pourrait par exemple se faire en renvoyant aux articles précis du Projet qui contiennent les traitements soumis aux limitations des droits établis à l'article 65 du Projet. L'Autorité rappelle, par souci d'exhaustivité, que ces limitations doivent rester dans les limites du strict nécessaire[25];

- en ce qui concerne les catégories de données à caractère personnel : *"toutes les catégories de données à caractère personnel traitées par le ou les responsables du traitement en lien avec les finalités [précitées]"*[26] ; l'Autorité insiste pour que l'on précise cette description.
- en ce qui concerne l'étendue des limitations : le Projet ne prévoit rien en la matière et l'Autorité estime que cette lacune doit être comblée. À titre d'illustration, l'Autorité renvoie au point 41 de l'avis n° 34/2018[27].
- en ce qui concerne les garanties visant à prévenir un abus ou un accès ou une transmission illicite :
  - *"Chaque responsable du traitement est tenu de prendre des mesures appropriées pour éviter toute forme d'abus, d'accès ou de transfert illicites desdites données à caractère personnel"*[28]. L'Autorité prie le demandeur de clarifier (par exemple dans l'Exposé des motifs) quelles "mesures appropriées" concrètes seront prises pour éviter un accès illicite ;
  - "*Le délégué à la protection des données du responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition de l'Autorité de protection des données.*"[29] Cette procédure ne semble toutefois s'appliquer que pour les limitations du droit de rectification ce qui est donc insuffisant (cf. infra, point 23).

---

[24] Article 65, § 2 du Projet.

[25] Cf. point 38 de l'avis n° 34/2018.

[26] Article 65, § 4 du Projet.

[27] *"(...) En ce qui concerne l'étendue des limitations :*

- *pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle ou d'une enquête (y compris les actes préparatoires de maximum 1 an après réception de la demande d'exercice du droit) et pendant la période en vue d'exercer les poursuites en la matière ;*
- *dans la mesure où l'exercice des droits nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires ou risque de violer le secret de l'enquête pénale. (...)"*

[28] Article 65, § 4 du Projet.

[29] Article 67, § 3, deuxième alinéa du Projet.

- en ce qui concerne la détermination des responsables du traitement : l'opérateur de services essentiels, le fournisseur de service numérique ou les autorités visées au point 3[30];
- en ce qui concerne les durées de conservation : les données relatives à des infractions ne peuvent pas être conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées et au maximum pour la durée des délais de prescription[31]. Les articles du Projet auquel il est renvoyé à cet égard ne contiennent toutefois aucun délai de prescription. L'Autorité demande dès lors de reprendre les délais explicitement dans le Projet pour chaque traitement.
- en ce qui concerne les risques pour les droits et libertés des personnes concernées :
  - o le délégué à la protection des données informe la personne concernée de la possibilité d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel[32] ;
  - o le délégué à la protection des données consigne les motifs de fait ou de droit sur lesquels se fonde sa décision et ces informations sont mises à la disposition de l'autorité de contrôle compétente[33];

  L'Autorité observe que ces procédures ne semblent s'appliquer que pour les limitations du droit de rectification (cf. infra, point 23).

  Elle recommande par ailleurs de reprendre aussi à l'article 67 du Projet une disposition qui précise que le délégué à la protection des données informe immédiatement la personne concernée de la levée d'une limitation, et ce directement après la clôture du contrôle ou de l'enquête (sauf si le dossier est transmis au ministère public ou à l'instance compétente pour statuer sur les constatations de l'enquête).

- en ce qui concerne le droit de la personne concernée d'être informée de la limitation : à cet égard, deux dispositions du Projet sont pertinentes :
  - o *"Le délégué à la protection des données du responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, de tout refus ou de toute limitation à son droit de rectification, ainsi que des motifs du refus ou de la limitation. Ces informations concernant le*

[30] Article 65, § 3 du Projet.

[31] Article 65, § 5 du Projet.

[32] Article 67, § 3, premier alinéa du Projet.

[33] Article 67, § 3, deuxième alinéa du Projet.

refus ou la limitation peuvent ne pas être fournies lorsque leur communication risque de compromettre l'une des finalités énoncées à l'article 65."[34]

- o le responsable du traitement peut donner accès à la personne concernée aux "*informations limitées*" concernant le traitement de ses données à caractère personnel, "*dans la mesure où cette communication ne compromet pas la réalisation des objectifs de la présente loi.*"[35]

L'Autorité a deux remarques à formuler à cet égard :

- o elle se demande tout d'abord ce que l'on entend par "*informations limitées*". Une explication dans le Projet pourrait clarifier ces termes ;
- o Deuxièmement, elle demande de préciser le contenu et la portée des termes "*des objectifs de la présente loi*" et "*des finalités énoncées à l'article 65*".

23. Ensuite, l'Autorité attire l'attention de manière générale sur la nécessité de corriger la rédaction de l'article 67 du Projet. Le premier paragraphe dispose que les personnes concernées peuvent "*adresser une demande concernant leur droits au délégué à la protection des données*" et les deuxième et troisième paragraphes décrivent la procédure que ce délégué doit suivre à cet égard. Cette procédure semble toutefois se limiter aux cas dans lesquels une personne concernée exerce son droit de rectification (article 16 du RGPD). L'Autorité demande dès lors que cette procédure soit également appliquée aux cas dans lesquels les personnes concernées souhaitent exercer d'autres droits que le droit de rectification. À défaut, les garanties précitées (point 22, puces 4, 7 et 8) ne s'appliqueront pas à ces cas et ces limitations ne répondront absolument pas aux exigences de l'article 23 du RGPD.

24. Pour améliorer la rédaction des articles 65 et 67 du Projet en ce sens, on pourrait d'ailleurs s'inspirer des articles 59 e.s. de la 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.*

25. Enfin, l'Autorité constate aussi que l'obligation de notification de l'article 34 du RGPD est limitée, à savoir à l'article 67, § 5 du Projet. On ne motive pas la nécessité de cette dérogation. La rédaction de l'article 67, § 5 n'est en outre pas claire, étant donné que l'on utilise également les mêmes termes vagues (les "*objectifs de la présente loi*") qui font déjà l'objet de critiques ci-avant au point 22, puce 8. Le texte de cette disposition ne correspond en outre pas à

[34] Article 67, § 2 du Projet.

[35] Article 67, § 4 du Projet.

l'explication qui en est donnée dans l'Exposé des motifs (p. 35). L'Exposé des motifs indique en effet qu'il faut une autorisation de l'autorité de contrôle avant qu'un responsable du traitement soit déchargé de l'obligation de notification reprise à l'article 34 du RGPD, alors que cette condition ne ressort pas du texte de l'article 67, § 5. L'Autorité insiste dès lors pour que cette disposition soit retravaillée en profondeur.

III. CONCLUSION

26. À condition que les remarques suivantes soient intégrées dans le texte :
    - sensibiliser les acteurs concernés via le Projet (ou l'Exposé des motifs du Projet) afin que les traitements de données qui auront lieu en vertu du Projet soient conformes au RGPD (voir le point 7) ;
    - intégrer tous les éléments essentiels des traitements de données envisagés dans le Projet (voir les points 11, 12, 14, 18 et 19) ;
    - implémenter encore davantage le principe de "minimisation des données" dans (l'Exposé des motifs du) Projet (voir les points 16 & 17) ;
    - retravailler les articles 65 et 67 du Projet conformément aux suggestions reprises aux points 22 à 25 inclus.

l'Autorité estime que le Projet offre suffisamment de garanties quant à la protection des données à caractère personnel des personnes concernées.

PAR CES MOTIFS,

l'Autorité émet un **avis favorable** sur le projet de loi *établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*, et ce à la condition explicite que les remarques précitées soient intégrées.

L'Administrateur f.f., La Présidente,

(sé) An Machtens (sé) Willem Debeuckelaere