Avis n° 102/2019 du 5 juin 2019

Objet : Projet d'arrêté royal portant exécution de la loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de certaines dispositions de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (CO-A-2019-115)

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 (ci-après "la LCA") ;

Vu le 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, ci-après "le RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis du Premier Ministre, reçue le 10 avril 2019 ;

Vu le rapport de Madame Alexandra Jaspar, Directrice du Centre de Connaissances de l'Autorité de protection des données ;

Émet, le 5 juin 2019, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. En date du 10 avril 2019, le Premier Ministre a sollicité l'avis de l'Autorité sur un projet d'arrêté royal *portant exécution de la loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique,*, *ainsi que de certaines dispositions de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques* (ci-après "le Projet").

2. Un projet de texte de la loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après "la loi") a déjà fait l'objet de l'avis n° 84/2018[1] de l'Autorité. La loi vise la transposition de la Directive européenne (UE) 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*. Cette 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 - laquelle a été mise en oeuvre dans le droit belge au moyen de la loi - concerne les incidents ayant un impact significatif sur les services fournis.

3. Le Projet vise principalement à :

- établir le cadre général pour les notifications d'incidents de sécurité au sens de la loi,
- désigner les "autorités compétentes" dont il est question dans la loi[2] et
- définir les conditions de certification générales pour les organismes qui doivent exécuter les audits externes des opérateurs de services essentiels.

[1] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_84_2018.pdf.

[2] À titre d'exemple :

- article 7, § 1er de la loi : "*Le Roi désigne désigne l'autorité chargée, au titre d'autorité nationale, du suivi et de la coordination de la mise en œuvre de la présente loi.*"

- article 10, § 1er de la loi : "*Le Roi désigne, par arrêté délibéré en Conseil des ministres, l'autorité chargée de maintenir à jour la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.*"

(Voir aussi le point 3 de l'avis n° 84/2018).

II. EXAMEN DE LA DEMANDE D'AVIS

4. Dans son avis n° 84/2018, l'Autorité attirait déjà l'attention sur le fait que dans la pratique, de nombreux points communs apparaîtraient entre les dispositions de la loi et les règles relatives à la protection des données. Tous les acteurs soumis aux dispositions de la loi doivent notamment - dans la mesure où ils traitent également des données à caractère personnel - aussi tenir compte du RGPD et de ses lois d'exécution[3]. Cela vaut par exemple également en ce qui concerne la notification d' "incidents de sécurité" au sens de la loi et de "violations de données à caractère personnel" au sens du RGPD. Dès lors, l'Autorité profite d'abord de l'occasion pour plaider en faveur d'une communication claire à ce sujet[4] sur le site Internet de la plate-forme commune de notification d'incidents de sécurité qui sera créée conformément au Projet.

5. Par ailleurs, l'Autorité prend acte du règlement repris dans le Projet pour la notification d'incidents de sécurité au sens de la loi. Le Chapitre 3 (articles 4 à 9 inclus) du Projet traite notamment de la "Notification et [du] traitement des incidents" et le Chapitre 4 (article 10) du Projet des "Notifications volontaires". L'article 6, § 1er du Projet dispose que la notification d'incidents de sécurité au sens de la loi doit être réalisée via la plate-forme de notification et sur la base d'un formulaire qui sera rédigé par la Computer Security Incident Response Team. Le deuxième paragraphe de l'article 6 du Projet prévoit également une disposition d'exception en ce qui concerne la notification de violations de données à caractère personnel[5]. Sur la base de cette disposition, ces dernières notifications sont spécifiquement soumises au RGPD et aux règles imposées par l'Autorité.

6. L'Autorité juge positivement ce régime d'exception pour la notification de violations de données à caractère personnel et plaide également pour qu'une portée plus générale soit conférée à l'article 6, § 2 du Projet, vu que cette disposition, dans sa structure actuelle, semble ne prévoir qu'une dérogation au premier paragraphe de l'article 6 du Projet et pas aux autres dispositions du Projet. Les règles différentes pour la notification de violations de données à caractère personnel au sens du RGPD devraient toutefois s'appliquer à l'ensemble des Chapitres 3 et 4 du Projet car ces chapitres - outre l'article 6 du projet - comportent également d'autres dispositions prévoyant des règles pour la notification d'incidents de sécurité au sens

---

[3] Points 6 et 7 de l'avis n° 84/2018.

[4] Un point important qu'il conviendrait de souligner dans cette communication concerne le fait qu'il relève de la responsabilité du responsable du traitement de décider à quelle(s) instance(s) il adresse la notification et à laquelle/auxquelles il ne le fait pas (voir le point 6 de l'avis n° 84/2018).

[5] *"Art. 6. § 1er. La notification est réalisée via la plate-forme de notification et moyennant l'utilisation du formulaire de notification d'incident déterminé par le CSIRT national (...)*

§ 2. Il est dérogé au paragraphe 1er pour les notifications de violations de données à caractère personnel, lesquelles suivent les règles légales ou imposées par l'autorité de contrôle (...)".

de la loi[6] et il faut qu'il soit clair que ces notifications sont totalement distinctes de la notification de violations de données à caractère personnel au sens du RGPD.

7. Une telle extension de la portée de l'article 6, § 2 du Projet pourrait par exemple être réalisée en formulant plus largement le libellé de cette disposition (notamment en remplaçant les mots "au paragraphe 1er" par "à ce chapitre") ainsi qu'en reprenant systématiquement cette disposition dans un article distinct au début du Chapitre 3 et au début du Chapitre 4 du Projet.

PAR CES MOTIFS,

- l'Autorité recommande de publier une communication claire sur le site Internet de la plate-forme commune de notification en ce qui concerne la distinction entre les obligations imposées par la loi et celles qui découlent du RGPD (point 4) ;

- l'Autorité juge que l'adaptation suivante du Projet s'impose : ne pas limiter le régime d'exception pour la notification de violations de données à caractère personnel à l'article 6 mais l'étendre à l'ensemble des chapitres 3 & 4 du Projet (points 6-7).

(sé) An Machtens
Administratrice f.f.

(sé) Alexandra Jaspar
Directrice du Centre de Connaissances

[6] Voir par ex. l'article 7 du Projet.