LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[C − 2019/41284]

12 JUILLET 2019. — Arrêté royal portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques

RAPPORT AU ROI

Sire,

Considérations générales

Le présent arrêté royal porte exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

L'arrêté royal a pour objectif principal de fixer le cadre général pour les notifications d'incidents de sécurité, de désigner les autorités compétentes et d'établir les conditions générales de certification des organismes devant réaliser les audits externes des opérateurs de services essentiels. Celui-ci n'aborde pas les aspects spécifiques sectoriels ou les mesures facultatives qui peuvent être prises par le Roi. Les éventuelles mesures d'exécution propres à un secteur ou sous-secteur feront l'objet, le cas échéant, d'un ou plusieurs autres arrêtés royaux.

Le gouvernement se doit, conformément à la notion d'affaires courantes, d'adopter des dispositions réglementaires urgentes ou qui découlent d'obligations internationales de la Belgique, dont celles en matière de transposition de directives européennes. En effet, une procédure d'infraction contre la Belgique a été entamée par la Commission européenne pour retard de transposition de la directive européenne (EU) 2016/1148 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 (« directive NIS »), laquelle devait être transposée pour le 9 mai 2018.

Pour transposer adéquatement la directive NIS en Belgique, il est nécessaire d'adopter le présent projet d'arrêté royal.

Les modalités opérationnelles de traitement des notifications d'incidents entre les administrations concernées seront fixées dans un protocole, comme prévu à l'article 11 du présent arrêté royal.

Conformément au champ d'application de la loi du 7 avril 2019, tel que prévu en ses articles 4 et 5, le présent arrêté royal est sans préjudice des règles applicables :

- au traitement des informations, documents ou données, au matériel, aux matériaux ou matières, sous quelque forme que ce soit, qui sont classifiés en application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

- aux documents nucléaires, au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

Commentaire des articles

CHAPITRE 1er. Objet

Article 1er. Le Conseil d'Etat recommande de préciser que l'arrêté royal qui est adopté vise à transposer la directive européenne 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 dénommée la « directive NIS ».

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[C − 2019/41284]

12 JULI 2019. — Koninklijk besluit tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren

VERSLAG AAN DE KONING

Sire,

Algemene overwegingen

Dit koninklijk besluit voorziet in de uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

Het koninklijk besluit heeft voornamelijk tot doel het algemene kader voor meldingen van beveiligingsincidenten vast te stellen, de bevoegde autoriteiten aan te wijzen en de algemene certificeringsvoorwaarden te bepalen voor de instellingen die de externe audits van de aanbieders van essentiële diensten moeten uitvoeren. Het gaat niet in op de specifieke sectorale aspecten of de facultatieve maatregelen die door de Koning kunnen worden genomen. Eventuele uitvoeringsmaatregelen die specifiek zijn voor een sector of deelsector, zullen in voorkomend geval in een of meer andere koninklijke besluiten worden behandeld.

Overeenkomstig het begrip "lopende zaken" dient de regering dringende regelgevende bepalingen of bepalingen die voortvloeien uit internationale verplichtingen van België goed te keuren, waaronder deze inzake de omzetting van Europese richtlijnen. De Europese Commissie heeft immers een inbreukprocedure tegen België ingesteld wegens niet-tijdige omzetting van de Europese richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie ("NIS-richtlijn"), die tegen 9 mei 2018 moest zijn omgezet.

Om de NIS-richtlijn adequaat om te zetten in België, is het noodzakelijk dat dit ontwerp van koninklijk besluit wordt goedgekeurd.

De operationele modaliteiten voor de verwerking van incidentmeldingen tussen de betrokken besturen zullen worden vastgelegd in een protocol, zoals bepaald in artikel 11 van dit koninklijk besluit.

Overeenkomstig het toepassingsgebied van de wet van 7 april 2019, zoals bepaald in de artikelen 4 en 5 van deze wet, doet dit koninklijk besluit geen afbreuk aan de regels die van toepassing zijn op:

- de verwerking van informatie, documenten of gegevens, materieel, materialen of stoffen, in welke vorm ook, die geclassificeerd zijn overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

- nucleaire documenten in de zin van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

Artikelsgewijze bespreking

HOOFDSTUK 1. Onderwerp

Artikel 1. De Raad van State beveelt aan om te verduidelijken dat het aangenomen koninklijk besluit gericht is op de omzetting van de Europese richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna de "NIS-richtlijn" genoemd.

CHAPITRE 2. Définitions

Art. 2. Au point 4°, le terme « plate-forme de notification » vise la plate-forme créée en vertu de l'article 31 de la loi du 7 avril 2019 et permettant aux opérateurs de services essentiels et aux fournisseurs de service numérique de notifier (1) au CSIRT national (CCB), à l'autorité sectorielle ou son CSIRT sectoriel, et à la Direction générale Centre de Crise du Service public fédéral Intérieur (ci-après dénommée « DGCC »), des notifications d'incidents de sécurité; et/ ou (2) aux autorités de contrôle les violations de données à caractère personnel.

CHAPITRE 3. Autorités compétentes

Art. 3. Dans son avis 63.296/4 du 2 mai 2018, le Conseil d'Etat a insisté sur le fait qu'il revenait au Roi de désigner les services qui seront chargés d'intervenir dans le processus d'application et de mise en œuvre de la loi.

En exécution de l'article 7, § 1er et 2, de la loi du 7 avril 2019, le Centre pour la Cybersécurité Belgique (ci-après dénommé « CCB ») est désigné (1) comme autorité nationale chargée du suivi et de la coordination de la mise en œuvre de la loi du 7 avril 2019 ainsi que (2) comme point de contact national unique en matière de sécurité des réseaux et des systèmes d'information, pour l'ensemble des opérateurs de services essentiels et des fournisseurs de service numérique, pour la Belgique dans ses relations avec la Commission européenne, les États membres de l'Union européenne, le Groupe de coopération et le réseau des CSIRT.

Le CCB est chargé de maintenir à jour la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.

Conformément à l'article 3, 1° et 7°, de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, celui-ci a, en effet, déjà la mission, au titre d'autorité nationale, de superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en matière de cybersécurité, ainsi que de coordonner le suivi des obligations internationales en la matière.

Conformément à l'article 10, § 1er, de la loi du 7 avril 2019, les autorités visées à l'article 7 de la loi du 7 avril 2019 donnent leur avis au CCB sur les propositions d'adaptation de la stratégie nationale. La DGCC fournit un avis notamment pour ce qui concerne les aspects liés à la sécurité physique des sites des opérateurs de services essentiels. En effet, la sécurité des réseaux et systèmes d'information visée par loi et la directive inclut aussi les aspects de sécurité physique liés aux réseaux et systèmes d'information.

En exécution de l'article 7, § 2, de la loi du 7 avril 2019, l'article 3, § 1, al. 2, du présent arrêté royal désigne le Centre pour la Cybersécurité Belgique comme le centre national de réponse aux incidents de sécurité informatique («CSIRT national»). Le CCB dispose du personnel technique apte pour traiter, au niveau national, les notifications d'incidents et pour porter éventuellement assistance.

En exécution de l'article 7, § 4, de la loi du 7 avril 2019, l'article 3, § 2, du présent arrêté royal désigne la DGCC comme l'autorité chargée, en coopération avec le CCB, de coordonner l'identification des opérateurs de services essentiels. En effet, la DGCC dispose d'une compétence similaire dans le cadre de l'identification des infrastructures critiques visée par la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

En exécution de l'article 7, § 3, de la loi du 7 avril 2019, l'article 3, § 3, de l'arrêté renvoie à l'annexe 1 de l'arrêté royal pour la désignation de certaines autorités sectorielles.

En exécution de l'article 7, § 5, de la loi du 7 avril 2019, l'article 3, § 4, de l'arrêté renvoie à l'annexe 2 de l'arrêté royal pour la désignation de certains services d'inspection.

Il est à noter que certaines autorités sectorielles et certains services d'inspection sont déjà directement désignés par la loi du 7 avril 2019.

Pour le secteur de l'eau potable, l'autorité sectorielle sera créée et désignée par le Roi dans un autre arrêté royal.

Art. 4. Le présent arrêté royal exécute les dispositions nécessaires à la cohérence et la complétude entre la loi du 1er juillet 2011 et la loi du 7 avril 2019.

En exécution des articles 3, 3°, f) et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, le Roi désigne, pour le secteur de la santé, le Ministre fédéral ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur) comme autorité sectorielle et service d'inspection. Cette désignation est effectuée dans l'annexe 1, point c), de l'arrêté royal.

HOOFDSTUK 2. Definities

Art. 2. In punt 4° verwijst de term "meldingsplatform" naar het platform opgericht krachtens artikel 31 van de wet van 7 april 2019 dat aanbieders van essentiële diensten en digitaledienstverleners toelaat (1) beveiligingsincidenten te melden aan het nationale CSIRT (CCB), aan de sectorale overheid of haar sectorale CSIRT, en aan de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken (hierna "ADCC"); en/of (2) inbreuken in verband met persoonsgegevens te melden aan de toezichthoudende autoriteiten.

HOOFDSTUK 3. Bevoegde autoriteiten

Art. 3. In zijn advies 63.296/4 van 2 mei 2018 heeft de Raad van State benadrukt dat het de Koning toekomt te bepalen welke diensten bij de toepassing en de tenuitvoerlegging van de wet een rol dienen te spelen.

In uitvoering van artikel 7, §§ 1 en 2, van de wet van 7 april 2019 wordt het Centrum voor Cybersecurity België (hierna "CCB") aangewezen (1) als nationale autoriteit belast met de opvolging en coördinatie van de uitvoering van de wet van 7 april 2019 en (2) als centraal nationaal contactpunt voor de beveiliging van netwerk- en informatiesystemen, voor alle aanbieders van essentiële diensten en digitaledienstverleners, voor België in zijn relatie met de Europese Commissie, de lidstaten van de Europese Unie, de Samenwerkingsgroep en het CSIRT-netwerk.

Het CCB is belast met de actualisering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen.

Overeenkomstig artikel 3, 1° en 7°, van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België heeft dit centrum immers al de opdracht om, als nationale autoriteit, de uitvoering van het Belgisch beleid op het vlak van cyberveiligheid op te volgen en te coördineren en hierop toe te zien, alsook de opvolging van internationale verplichtingen op dit vlak te coördineren.

Overeenkomstig artikel 10, § 1, van de wet van 7 april 2019 verstrekken de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 het CCB advies over aanpassingsvoorstellen van de nationale strategie. De ADCC verstrekt advies met name over de aspecten rond de fysieke beveiliging van de sites van de aanbieders van essentiële diensten. De beveiliging van netwerk- en informatiesystemen, zoals bedoeld in de wet en de richtlijn, omvat immers ook aspecten rond de fysieke beveiliging van netwerk- en informatiesystemen.

In uitvoering van artikel 7, § 2, van de wet van 7 april 2019, wijst artikel 3, § 1, tweede lid, van dit koninklijk besluit het Centrum voor Cybersecurity België aan als het nationale computer security incident response team ("nationaal CSIRT"). Het CCB beschikt over technisch personeel dat op nationaal niveau incidentmeldingen kan verwerken en eventueel bijstand kan verlenen.

In uitvoering van artikel 7, § 4, van de wet van 7 april 2019 wijst artikel 3, § 2, van dit koninklijk besluit de ADCC aan als autoriteit die, in samenwerking met het CCB, de identificatie van aanbieders van essentiële diensten coördineert. De ADCC beschikt immers over een soortgelijke bevoegdheid in het kader van de identificatie van kritieke infrastructuren bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

In uitvoering van artikel 7, § 3, van de wet van 7 april 2019 verwijst artikel 3, § 3, van het besluit naar bijlage 1 van het koninklijk besluit voor de aanwijzing van sommige sectorale overheden.

In uitvoering van artikel 7, § 5, van de wet van 7 april 2019 verwijst artikel 3, § 4, van het besluit naar bijlage 2 van het koninklijk besluit voor de aanwijzing van sommige inspectiediensten.

Opgemerkt wordt dat sommige sectorale overheden en inspectiediensten al rechtstreeks zijn aangewezen door de wet van 7 april 2019.

Voor de sector drinkwater zal de sectorale overheid door de Koning worden opgericht en aangewezen in een ander koninklijk besluit.

Art. 4. Dit koninklijk besluit regelt de uitvoering van de bepalingen die noodzakelijk zijn voor de samenhang tussen de wet van 1 juli 2011 en de wet van 7 april 2019 en de volledigheid van beide wetten.

In uitvoering van de artikelen 3, 3°, f) en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren wijst de Koning, voor de sector gezondheidszorg, de federale Minister bevoegd voor Volksgezondheid aan of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de Minister per deelsector een andere gemachtigde aanwijzen) als sectorale overheid en inspectiedienst. Deze aanwijzing gebeurt in bijlage 1, punt c), van het koninklijk besluit.

L'article 3, 3°, f), de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques prévoit que le Roi peut prendre des mesures pour assurer la transposition des directives européennes concernant les infrastructures critiques. Il s'agit ici d'assurer qu'une autorité sectorielle et un service d'inspection soient bien désignés pour les éventuelles infrastructures critiques désignées dans le secteur de la santé. Cette désignation est effectuée dans l'annexe 1, point a), de l'arrêté royal.

CHAPITRE 4. Notification et traitement des incidents

Section 1re. Champ d'application et plate-forme de notification

Art. 5. Le chapitre IV vise à exécuter les articles 24, 26, § 1er, 27 et 35 de la loi du 7 avril 2019.

Ces dispositions imposent aux opérateurs de services essentiels ou aux fournisseurs de service numérique l'obligation de notifier aux autorités désignées un incident, lequel est défini à l'article 6, 13°, de la loi comme « tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information ».

En l'absence de niveaux d'incidence et/ou de seuils visés à l'art 24, § 2 de la loi, l'opérateur notifie tous les incidents ayant un impact sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit.

Le fournisseur de service numérique est tenu de notifier les incidents ayant un impact significatif sur la fourniture du service numérique qu'il propose.

Art. 6. En vertu de l'article 31 de la loi du 7 avril 2019, le Roi est chargé de déterminer les modalités de notification et de rapportage des incidents, en ce compris, de créer une plate-forme sécurisée de notification.

Cette plate-forme sera entre autres destinée à être utilisée par les opérateurs de services essentiels et fournisseurs de service numérique spécifiquement visés par la loi du 7 avril 2019.

L'article 6 crée cette plate-forme de notification. Cette plate-forme permet aux opérateurs de services essentiels et aux fournisseurs de service numérique de :

- notifier au CCB, à l'autorité sectorielle ou son CSIRT sectoriel, et à la DGCC, les incidents de sécurité, au sens de la loi du 7 avril 2019;

- notifier éventuellement aux autorités de contrôle les violations de données à caractère personnel, comme imposé par l'article 33, premier alinéa, du règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Art. 7. L'article 7 vise à préciser les modalités de création et de fonctionnement de la plate-forme créée en vertu de l'article 6 de l'arrêté. Lors de la création de la plateforme, il sera prévu une connexion sécurisée à la plate-forme notamment au moyen d'une clé d'identification unique propre à chaque opérateur de services essentiels et fournisseur de service numérique.

Section 2. Notifications

Art. 8. La notification doit être réalisée au moyen de la plate-forme de notification et moyennant un formulaire de notification dont le contenu sera déterminé par le CCB. Les modalités opérationnelles d'utilisation de la plate-forme de notification et les moyens sécurisés de communication figureront dans un guide élaboré par le CCB; celui-ci sera fourni aux opérateurs de services essentiels ainsi qu'aux fournisseurs de service numérique.

La loi du 7 avril 2019 entend favoriser la rapidité des notifications et la résolution des incidents, et par conséquent elle prévoit en son article 25 que les notifications sur la plate-forme doivent être réalisées même si l'opérateur de services essentiels ou le fournisseur de service numérique ne dispose que d'une partie des informations pertinentes pour évaluer le caractère significatif de l'impact de l'incident. Conformément à l'objectif poursuivi par la loi du 7 avril 2019, l'arrêté royal prévoit un système de notification d'incident en trois stades :

a) article 8, §1er : le but de la notification initiale est d'attirer l'attention du CCB, de l'autorité sectorielle ou de son CSIRT sectoriel, et de la DGCC sur l'incident et ses possibles conséquences.

b) article 8, §§ 3-4 : le but des notifications complémentaires est de tenir informés le CCB, l'autorité sectorielle ou son CSIRT sectoriel, et la DGCC sur le statut de l'incident.

c) article 8, § 5 : le but du rapport final est de donner une vue d'ensemble de l'incident et de pouvoir en tirer des conclusions.

Artikel 3, 3°, f), van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren bepaalt dat de Koning maatregelen kan nemen om de omzetting van de Europese richtlijnen betreffende de kritieke infrastructuren te verzekeren. Het is de bedoeling te waarborgen dat een sectorale overheid en een inspectiedienst worden aangewezen voor eventuele kritieke infrastructuren die in de sector gezondheidszorg worden geïdentificeerd. Deze aanwijzing gebeurt in bijlage 1, punt a), van het koninklijk besluit.

HOOFDSTUK 4. Melding en verwerking van incidenten

Afdeling 1. Toepassingsgebied en meldingsplatform

Art. 5. Hoofdstuk IV beoogt de uitvoering van de artikelen 24, 26, § 1, 27 en 35 van de wet van 7 april 2019.

Deze bepalingen leggen aanbieders van essentiële diensten en digitaledienstverleners de verplichting op om de aangewezen autoriteiten elk incident te melden dat in artikel 6, 13°, van de wet is gedefinieerd als "elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen".

Indien geen weerslagniveaus en/of drempelwaarden als bedoeld in artikel 24, § 2, van de wet zijn bepaald, meldt de aanbieder alle incidenten die gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.

Digitaledienstverleners zijn verplicht incidenten te melden die aanzienlijke gevolgen hebben voor de verlening van de door hen aangeboden digitale dienst.

Art. 6. Krachtens artikel 31 van de wet van 7 april 2019 is de Koning belast met het bepalen van de modaliteiten voor de melding en rapportering van incidenten, met inbegrip van de oprichting van een beveiligd meldingsplatform.

Dit platform is onder meer bestemd voor aanbieders van essentiële diensten en digitaledienstverleners die specifiek bedoeld zijn in de wet van 7 april 2019.

Artikel 6 richt dit meldingsplatform op. Dit platform laat aanbieders van essentiële diensten en digitaledienstverleners toe:

- beveiligingsincidenten te melden aan het CCB, de sectorale overheid of haar sectorale CSIRT, en de ADCC, zoals bepaald in de wet van 7 april 2019;

- eventueel inbreuken in verband met persoonsgegevens te melden aan de toezichthoudende autoriteiten, zoals opgelegd door artikel 33, eerste alinea, van verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Art. 7. Artikel 7 verduidelijkt de modaliteiten voor de oprichting en werking van het platform dat krachtens artikel 6 van het besluit wordt gecreëerd. Bij de oprichting wordt voorzien in een beveiligde verbinding met het platform, met name door middel van een voor elke aanbieder van essentiële diensten en digitaledienstverlener unieke identificatiesleutel.

Afdeling 2. Meldingen

Art. 8. Incidenten moeten gemeld worden via het meldingsplatform met behulp van een meldingsformulier waarvan de inhoud door het CCB zal worden bepaald. De operationele gebruiksmodaliteiten van het meldingsplatform en de beveiligde communicatiemiddelen zullen worden vermeld in een gids van het CCB, die aan de aanbieders van essentiële diensten en digitaledienstverleners zal worden bezorgd.

De wet van 7 april 2019 heeft tot doel de snelheid van meldingen en het oplossen van incidenten te bevorderen. Bijgevolg bepaalt artikel 25 van deze wet dat incidenten via het platform moeten worden gemeld zelfs wanneer de aanbieder van essentiële diensten of digitaledienstverlener slechts gedeeltelijk over relevante informatie beschikt om te bepalen of het incident een aanzienlijke impact heeft. Overeenkomstig de doelstelling van de wet van 7 april 2019 voorziet het koninklijk besluit in een incidentmeldingssysteem in drie fasen:

a) artikel 8, § 1: de oorspronkelijke melding heeft tot doel het CCB, de sectorale overheid of haar sectorale CSIRT, en de ADCC te wijzen op het incident en de mogelijke gevolgen ervan.

b) artikel 8, §§ 3-4: de aanvullende meldingen hebben tot doel het CCB, de sectorale overheid of haar sectorale CSIRT, en de ADCC op de hoogte te houden over de status van het incident.

c) artikel 8, § 5: het eindverslag heeft tot doel een overzicht te geven van het incident en er conclusies uit te trekken.

Art. 9. Le Roi charge le CCB de déterminer les modalités opérationnelles de notification à utiliser par les opérateurs de services essentiels et les fournisseurs de service numérique, en cas d'indisponibilité de la plate-forme de notification visée à l'article 6.

Section 3. Traitement de l'incident

Art. 10. En exécution de l'article 31 de la loi du 7 avril 2019, cet article précise les démarches à suivre pour le traitement des incidents notifiés par les opérateurs de services essentiels et les fournisseurs de service numérique.

Le Roi habilite le CCB, l'autorité sectorielle ou son CSIRT sectoriel ou la DGGC à demander à l'opérateur de services essentiels ou au fournisseur de service numérique des informations complémentaires sur les notifications qu'il a effectuées. L'objectif est d'assurer un suivi efficace et approprié de l'incident en vue d'y remédier (article 10, § 1er).

Ensuite, le paragraphe 2 prévoit que le CCB, l'autorité sectorielle ou son CSIRT sectoriel ou la DGCC fournissent à l'opérateur de services essentiels ou au fournisseur de service numérique toutes les informations utiles au suivi de sa notification, et le cas échéant, toutes les informations qui pourraient contribuer à une gestion efficace de l'incident.

Le CCB coordonne les notifications et la coopération au niveau national ainsi qu'au niveau international, sans préjudice de la gestion de crise en cas de cyberincidents, visée à l'article 3, 5°, de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique.

L'objectif est de souligner l'importance de coopérer au niveau national et international en matière de cybersécurité afin de garantir la sécurité des réseaux et des systèmes d'information. Cette coopération devrait également permettre aux CSIRT nationaux d'échanger sur les bonnes pratiques et d'évaluer leurs stratégies nationales en matière de sécurité des réseaux et des systèmes d'information, à renforcer leurs capacités et à évaluer les exercices relatifs à la sécurité des réseaux et des systèmes d'information.

Section 4. Protocole d'accord

Art. 11. Par son article 11, le présent arrêté royal charge le CCB, les autorités sectorielles et la DGCC de conclure un protocole d'accord afin de fixer les modalités opérationnelles de gestion de la plate-forme, de traitements des notifications et des demandes d'informations complémentaires.

CHAPITRE 5. Les notifications volontaires

Art. 12. En exécution de l'article 30 de la loi, l'article 12 du présent arrêté royal charge le CCB de définir et publier sur son site internet les modalités opérationnelles des notifications volontaires.

CHAPITRE 6. Dérogations

Art. 13. Suivant la recommandation de l'Autorité de protection des données, l'arrêté royal déroge aux règles prévues à ses chapitres IV et V pour les notifications les violations de données à caractère personnel.

CHAPITRE 7. Les organismes d'évaluation de la conformité

Art. 14. Exécutant l'article 39 de la loi du 7 avril 2019, l'article 14 détermine les conditions auxquelles doivent répondre les organismes d'évaluation de la conformité qui souhaitent être accrédités par l'autorité nationale d'accréditation ou par une institution qui est co-signataire des accords de reconnaissance du « European Cooperation for Accreditation » pour l'audit externe d'opérateurs de services essentiels ou de fournisseurs de service numérique et la vérification de la conformité de la politique de sécurité de l'information (PSI) qui doit être élaborée par les opérateurs de services essentiels, à savoir :

1° satisfaire, à tout moment, aux critères d'accréditation prévus par les normes ISO/IEC 17021 ou ISO/IEC 17065, lesquelles spécifient (a) les exigences génériques et spécifiées applicables aux organismes procédant à l'audit et à la certification des systèmes de management et; (b) les exigences visant à garantir que les organismes de certification exploitent des programmes de certification avec compétence, cohérence et impartialité;

2° et satisfaire aux procédures de fonctionnement du système d'accréditation qui sont applicables aux organismes accrédités.

CHAPITRE 8. Dispositions finales

Art. 15. Vu la nécessité de transposer la directive NIS dans les plus brefs délais, il est prévu que le présent arrêté entre en vigueur le jour de sa publication au *Moniteur belge*.

Art. 9. De Koning belast het CCB met het bepalen van de operationele modaliteiten voor de melding door aanbieders van essentiële diensten en digitaledienstverleners, indien het meldingsplatform bedoeld in artikel 6 niet beschikbaar is.

Afdeling 3. Verwerking van het incident

Art. 10. In uitvoering van artikel 31 van de wet van 7 april 2019 bepaalt dit artikel welke stappen moeten worden doorlopen voor de verwerking van incidenten die door aanbieders van essentiële diensten en digitaledienstverleners worden gemeld.

De Koning machtigt het CCB, de sectorale overheid of haar sectorale CSIRT, of de ADCC om de aanbieder van essentiële diensten of digitaledienstverlener bijkomende informatie te vragen over diens meldingen. Doel is een doeltreffende en passende opvolging van het incident te waarborgen met het oog op het oplossen ervan (artikel 10, § 1).

Vervolgens bepaalt paragraaf 2 dat het CCB, de sectorale overheid of haar sectorale CSIRT, of de ADCC de aanbieder van essentiële diensten of digitaledienstverlener alle informatie verstrekt die nuttig is voor de opvolging van diens melding, en, in voorkomend geval, alle informatie die kan bijdragen tot een doeltreffende behandeling van het incident.

Het CCB coördineert de meldingen en de samenwerking op nationaal en internationaal niveau, onverminderd het crisisbeheer bij cyberincidenten bedoeld in artikel 3, 5°, van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België.

Doel is het belang te benadrukken van nationale en internationale samenwerking op het vlak van cyberveiligheid om de beveiliging van netwerk- en informatiesystemen te waarborgen. Die samenwerking moet de nationale CSIRT's ook toelaten informatie uit te wisselen over goede praktijken, hun nationale strategieën voor de beveiliging van netwerk- en informatiesystemen te evalueren, hun capaciteiten te versterken en oefeningen rond de beveiliging van netwerk- en informatiesystemen te beoordelen.

Afdeling 4. Protocolakkoord

Art. 11. Artikel 11 van dit koninklijk besluit belast het CCB, de sectorale overheden en de ADCC met het sluiten van een protocolakkoord om de operationele modaliteiten vast te leggen inzake het beheer van het platform, de verwerking van meldingen en de verzoeken om bijkomende informatie.

HOOFDSTUK 5. Vrijwillige meldingen

Art. 12. In uitvoering van artikel 30 van de wet bepaalt artikel 12 van dit koninklijk besluit dat het CCB de operationele modaliteiten van de vrijwillige melding bepaalt en bekendmaakt op zijn website.

HOOFDSTUK 6. Afwijkingen

Art. 13. Op aanbeveling van de Gegevensbeschermingsautoriteit wijkt het koninklijk besluit af van de regels van hoofdstuk IV en V wat betreft de melding van inbreuken in verband met persoonsgegevens.

HOOFDSTUK 7. Instellingen voor de conformiteitsbeoordeling

Art. 14. In uitvoering van artikel 39 van de wet van 7 april 2019 bepaalt artikel 14 de voorwaarden die instellingen voor de conformiteitsbeoordeling moeten vervullen om te worden geaccrediteerd door de nationale accreditatieautoriteit of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft, voor de externe audit van aanbieders van essentiële diensten of digitaledienstverleners en voor het toezicht op de conformiteit van het informatiebeveiligingsbeleid (IBB) dat door aanbieders van essentiële diensten moet worden uitgewerkt, namelijk:

1° op ieder ogenblik voldoen aan de accreditatiecriteria van ISO/IEC 17021 of ISO/IEC 17065. Deze normen specificeren (a) de algemene en specifieke eisen die gelden voor instellingen die audits en certificering van managementsystemen uitvoeren en; (b) voorschriften om ervoor te zorgen dat certificeringsinstellingen certificeringsregelingen op competente, consistente en onpartijdige wijze uitvoeren;

2° en voldoen aan de werkingsprocedures van het accreditatiesysteem die van toepassing zijn op de geaccrediteerde instellingen.

HOOFDSTUK 8. Slotbepalingen

Art. 15. Gelet op de noodzaak om de NIS-richtlijn zo vlug mogelijk om te zetten, wordt bepaald dat dit besluit in werking treedt de dag waarop het in het *Belgisch Staatsblad* wordt bekendgemaakt.

Art. 16. Cette disposition prévoit que le Premier Ministre et le Ministre ayant la Sécurité et l'Intérieur dans ses attributions sont chargés de l'exécution du présent arrêté.

Annexe 1 - Les autorités sectorielles désignées

Vous faites usage de la possibilité qui Vous a été laissée en vertu de l'article 7, § 3, de la loi du 7 avril 2019 de désigner des autorités sectorielles chargées, pour leur secteur respectif, de veiller à la mise en œuvre des dispositions de la loi du 7 avril 2019.

Annexe 2 - Les services d'inspection désignés

Vous faites usage de la possibilité qui Vous a été laissée en vertu de l'article 7, § 5, de la loi du 7 avril 2019 de désigner les services d'inspection compétents pour effectuer le contrôle du respect des dispositions de la loi du 7 avril 2019 et de ses actes d'exécution par les opérateurs de services essentiels ou par les fournisseurs de service numérique.

J'ai l'honneur d'être,

Sire,
de Votre Majesté,
le très respectueux
et très fidèle serviteur,

Le Premier Ministre,
Ch. MICHEL

Le Ministre de la Sécurité et de l'Intérieur,
P. DE CREM

Avis n° 66.225/4 du 22 mai 2019 du Conseil d'Etat sur un projet d'arrêté royal 'portant exécution de la loi du 7 avril 2019 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'

Le 17 mai 2019, le Conseil d'État, section de législation, a été invité par le Premier Ministre à communiquer un avis, dans un délai de cinq jours ouvrables, sur un projet d'arrêté royal 'portant exécution de la loi du 7 avril 2019 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'.

Le projet a été examiné par la quatrième chambre le 22 mai 2019. La chambre était composée de Martine BAGUET, président de chambre, Bernard BLERO et Wanda VOGEL, conseillers d'État, Christian BEHRENDT et Marianne DONY, assesseurs, et Charles Henri VAN HOVE, greffier assumé.

Le rapport a été présenté par Anne VAGMAN, premier auditeur.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Martine BAGUET.

L'avis, dont le texte suit, a été donné le 22 mai 2019.

Suivant l'article 84, § 1er, alinéa 1er, 3°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la demande d'avis doit spécialement indiquer les motifs qui en justifient le caractère urgent.

La lettre s'exprime en ces termes :

« Ce projet d'arrêté royal exécute la loi du 7 avril 2019 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. La loi habilite le Roi dans plusieurs dispositions à adopter des mesures d'exécution de cette loi du 7 avril 2019. Dans son avis du 63.296/4 du 2 mai 2018, le Conseil d'État a insisté sur le fait qu'il revenait au Roi de désigner les services qui seront chargés d'intervenir dans le processus d'application et de mise en œuvre de la loi.

Art. 16. Deze bepaling verduidelijkt dat de Eerste Minister en de Minister bevoegd voor Veiligheid en Binnenlandse Zaken belast zijn met de uitvoering van dit besluit.

Bijlage 1 - De aangewezen sectorale overheden

U maakt gebruik van de U door artikel 7, § 3, van de wet van 7 april 2019 geboden mogelijkheid om sectorale overheden aan te wijzen die, voor hun respectievelijke sector, moeten toezien op de uitvoering van de bepalingen van de wet van 7 april 2019.

Bijlage 2 - De aangewezen inspectiediensten

U maakt gebruik van de U door artikel 7, § 5, van de wet van 7 april 2019 geboden mogelijkheid om de bevoegde inspectiediensten aan te wijzen die moeten toezien op de naleving van de bepalingen van de wet van 7 april 2019 en van de uitvoeringsbesluiten ervan door aanbieders van essentiële diensten en digitaledienstverleners.

Ik heb de eer te zijn,

Sire,
van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaar,

De Eerste Minister,
Ch. MICHEL

De Minister van Veiligheid en Binnenlandse Zaken,
P. DE CREM

Advies nr. 66.225/4 van 22 mei 2019 van de Raad van State over een ontwerp van koninklijk besluit 'tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren'

Op 17 mei 2019 is de Raad van State, afdeling Wetgeving, door de Eerste Minister verzocht binnen een termijn van vijf werkdagen een advies te verstrekken over een ontwerp van koninklijk besluit 'tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren'.

Het ontwerp is door de vierde kamer onderzocht op 22 mei 2019. De kamer was samengesteld uit Martine BAGUET, kamervoorzitter, Bernard BLERO en Wanda VOGEL, staatsraden, Christian BEHRENDT en Marianne DONY, assessoren, en Charles Henri VAN HOVE, toegevoegd griffier.

Het verslag is uitgebracht door Anne VAGMAN, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Martine BAGUET.

Het advies, waarvan de tekst hierna volgt, is gegeven op 22 mei 2019.

Volgens artikel 84, § 1, eerste lid, 3°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, moeten in de adviesaanvraag in het bijzonder de redenen worden opgegeven tot staving van het spoedeisende karakter ervan.

In het onderhavige geval luidt de motivering in de brief met de adviesaanvraag als volgt:

"Ce projet d'arrêté royal exécute la loi du 7 avril 2019 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. La loi habilite le Roi dans plusieurs dispositions à adopter des mesures d'exécution de cette loi du 7 avril 2019. Dans son avis du 63.296/4 du 2 mai 2018, le Conseil d'État a insisté sur le fait qu'il revenait au Roi de désigner les services qui seront chargés d'intervenir dans le processus d'application et de mise en œuvre de la loi.

Le gouvernement peut, conformément à la notion d'affaires courantes, adopter des dispositions réglementaires urgentes et qui découlent d'obligations internationales de la Belgique en matière de transposition de directive européenne. Une procédure d'infraction contre la Belgique a été entamée par la Commission européenne pour retard de transposition de la directive européenne (EU) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information ('directive NIS'), laquelle devait être transposée pour le 9 mai 2018.

Ce retard expose, en effet, la Belgique à une condamnation par la Cour de justice de l'Union européenne et à des sanctions financières. Celle-ci vient par ailleurs de faire l'objet d'un rappel pour retard dans la transposition de la Directive, par courrier de la Commission européenne daté du 7 mars 2019.

Or, pour transposer adéquatement la directive NIS en Belgique, il est nécessaire d'adopter le présent projet d'arrêté royal.

Il convient dès lors de traiter ce projet de manière urgente pour limiter au maximum le dépassement du délai de transposition et d'imposer au plus vite la mise en œuvre de mesures de sécurité des réseaux systèmes et d'information des opérateurs d'intérêt général pour la sécurité publique ».

Compte tenu du moment où le présent avis est donné, le Conseil d'État attire l'attention sur le fait qu'en raison de la démission du Gouvernement, la compétence de celui-ci se trouve limitée à l'expédition des affaires courantes. Le présent avis est toutefois donné sans qu'il soit examiné si le projet relève bien de la compétence ainsi limitée, la section de législation n'ayant pas connaissance de l'ensemble des éléments de fait que le Gouvernement peut prendre en considération lorsqu'il doit apprécier la nécessité d'arrêter ou de modifier des dispositions réglementaires.

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 3°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique du projet, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, le projet appelle les observations suivantes.

FORMALITÉS PRÉALABLES

1. La section de législation n'aperçoit pas ce que vise précisément l'alinéa 6 du préambule comme étant l'« avis des autorités sectorielles sur l'article 11 de la loi du 7 avril 2019 », cet avis ne figurant pas, au demeurant, au dossier. L'alinéa 6 du préambule sera donc omis.

Par contre, dès lors que, comme le mentionne le rapport au Roi, l'article 11 du projet entend procurer exécution à l'article 39, § 1er, de la loi du 7 avril 2019 'établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique', la consultation préalable de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, est requise.

Sur ce point, dès lors que l'arrêté en projet a précisément pour objet de déterminer certaines autorités sectorielles ainsi que l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019, il n'est pas possible, par hypothèse, de consulter ces instances préalablement à l'adoption de l'arrêté en projet.

Par conséquent, ce n'est qu'une fois l'arrêté en projet adopté et en vigueur, qu'il pourra être procédé à l'exécution de l'article 39, § 1er, de la loi du 7 avril 2019.

À ce stade, l'article 11 sera donc omis du projet et fera l'objet d'un arrêté ultérieur, moyennant l'accomplissement des formalités requises.

2. Il ressort du dossier que le projet a été soumis pour avis à l'autorité de protection des données dans le même temps qu'à la section de législation

La date de l'avis de cette autorité sera complétée au préambule.

Par ailleurs, il est rappelé que dans l'hypothèse où le texte du projet serait modifié ultérieurement pour tenir compte de cet avis, il faudrait à nouveau soumettre le texte ainsi modifié à l'avis de la section de législation.

Le gouvernement peut, conformément à la notion d'affaires courantes, adopter des dispositions réglementaires urgentes et qui découlent d'obligations internationales de la Belgique en matière de transposition de directive européenne. Une procédure d'infraction contre la Belgique a été entamée par la Commission européenne pour retard de transposition de la directive européenne (EU) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information ('directive NIS'), laquelle devait être transposée pour le 9 mai 2018.

Ce retard expose, en effet, la Belgique à une condamnation par la Cour de justice de l'Union européenne et à des sanctions financières. Celle-ci vient par ailleurs de faire l'objet d'un rappel pour retard dans la transposition de la Directive, par courrier de la Commission européenne daté du 7 mars 2019.

Or, pour transposer adéquatement la directive NIS en Belgique, il est nécessaire d'adopter le présent projet d'arrêté royal.

Il convient dès lors de traiter ce projet de manière urgente pour limiter au maximum le dépassement du délai de transposition et d'imposer au plus vite la mise en œuvre de mesures de sécurité des réseaux systèmes et d'information des opérateurs d'intérêt général pour la sécurité publique".

Rekening houdend met het tijdstip waarop dit advies gegeven wordt, vestigt de Raad van State de aandacht op het feit dat, wegens het ontslag van de regering, de bevoegdheid van deze laatste beperkt is tot het afhandelen van de lopende zaken. Dit advies wordt evenwel gegeven zonder dat wordt nagegaan of het ontwerp onder die beperkte bevoegdheid valt, aangezien de afdeling Wetgeving geen kennis heeft van alle feitelijke gegevens die de regering in aanmerking kan nemen als zij moet beoordelen of het nodig is een verordening vast te stellen of te wijzigen.

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 3°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving, overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het ontwerp, de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het ontwerp aanleiding tot de volgende opmerkingen.

VOORAFGAANDE VORMVEREISTEN

1. De afdeling Wetgeving begrijpt niet wat in het zesde lid van de aanhef precies wordt bedoeld met het "advies van de sectorale overheden op het artikel 11 van het wet van 7 april 2019", een advies dat zich trouwens niet in het dossier bevindt. Het zesde lid van de aanhef moet dus worden weggelaten.

Aangezien, zoals het verslag aan de Koning stelt, artikel 11 van het ontwerp uitvoering beoogt te verlenen aan artikel 39, § 1, van de wet van 7 april 2019 'tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid', is daarentegen vereist dat de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, van die wet vooraf worden geraadpleegd.

Die instanties kunnen in voorkomend geval onmogelijk worden geraadpleegd voordat het ontworpen besluit is uitgevaardigd, aangezien dat besluit er juist toe strekt bepaalde sectorale overheden alsook de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 aan te wijzen.

Artikel 39, § 1, van de wet van 7 april 2019 kan bijgevolg pas ten uitvoer worden gelegd nadat het ontworpen besluit is vastgesteld en in werking is getreden.

In dit stadium moet artikel 11 dus uit het ontwerp worden weggelaten; het dient in een later besluit te worden opgenomen als de voorgeschreven vormvereisten vervuld zijn.

2. Uit het dossier blijkt dat het ontwerp tegelijk aan de Gegevensbeschermingsautoriteit en aan de afdeling Wetgeving om advies is voorgelegd.

De datum van het advies van de Gegevensbeschermingsautoriteit moet in de aanhef worden aangevuld.

Voorts wordt opgemerkt dat ingeval de ontwerptekst achteraf zou worden gewijzigd om rekening te houden met dat advies, de aldus gewijzigde tekst opnieuw om advies zou moeten worden voorgelegd aan de afdeling Wetgeving.

EXAMEN DU PROJET

OBSERVATION GÉNÉRALE

L'article 6, § 1er, du projet, attribue au CSIRT national la compétence de déterminer le formulaire devant être utilisé pour les notifications d'incidents.

L'article 7 du projet attribue quant à lui au même CSIRT la compétence pour déterminer les modalités de notification à utiliser en cas d'indisponibilité de la plate-forme de notification, tandis que l'article 10 du projet lui confère la compétence d'arrêter les modalités des notifications volontaires visées à l'article 30 de la loi du 7 avril 2019.

Quant à l'article 9, il impose au CSIRT, aux autorités sectorielles et à la DGCC de conclure un « protocole d'accord » dont l'objet ira au-delà de questions purement opérationnelles, et portera sur les « modalités de gestion de la plate-forme de notification », « les modalités du traitement des notifications visées à l'article 8, § 3 » et les « modalités relatives aux demandes d'information complémentaire à l'opérateur de services essentiels ou au fournisseur de service numérique visées à l'article 6, § 4 », des modalités qui, selon le rapport au Roi « n'ont pas encore été définies par le Roi » et concerneraient également le « financement de la plate-forme », bien que le texte en projet ne le prévoie pas expressément.

Comme la section de législation l'a souvent rappelé, il n'est pas admissible que les agents d'une administration qui ne répondent pas politiquement de leurs actes devant les représentants de la Nation, soient investis de compétences de nature réglementaire. Une subdélégation à de telles autorités n'est exceptionnellement concevable que si elle concerne la détermination de mesures de pure administration ou de nature essentiellement technique, ce qui n'est pas le cas en l'espèce.

En conclusion, c'est au ministre que la compétence de déterminer ces différents éléments doit être attribuée. L'ensemble du projet sera revu en conséquence.

OBSERVATIONS PARTICULIÈRES

PRÉAMBULE

1. La directive (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' ne constitue pas le fondement juridique de l'arrêté en projet.

Cette directive ne doit pas être visée au préambule, dont l'alinéa 1er sera dès lors omis(1).

2. L'alinéa 2, devenant l'alinéa 1er, ne mentionnera pas les articles 39, § 1er(2), et 61 de la loi du 7 avril 2019. Il mentionnera en revanche l'article 36 de cette loi.

Cet alinéa sera revu en conséquence.

3. L'alinéa 3, devenant l'alinéa 2, mentionnera l'article 3, 3°, f), inséré par la loi du 7 avril 2019, l'article 24, § 2, alinéa 1er, et l'article 31 de la loi du 1er juillet 2011 'relative à la sécurité et la protection des infrastructures critiques'.

Cet alinéa sera revu en conséquence.

4. À l'alinéa 5, devenant l'alinéa 4, l'accord de la Ministre du Budget a été donné le 30 avril 2019.

DISPOSITIF

Article 1er (nouveau)

Conformément à l'article 25, paragraphe 1, alinéa 3, de la directive (UE) 2016/1148, un article 1er nouveau sera inséré, qui mentionnera que l'arrêté en projet opère une transposition partielle de cette directive.

Article 3

1. Au paragraphe 1er, il y a lieu de remplacer les mots « à l'article 31 » par les mots « à l'article 3, 3°, f) »(3).

2. Au paragraphe 2, il y a lieu de remplacer les mots « à l'annexe 2, point c) » par les mots « à l'annexe 2, point a) ».

Article 5

1. La disposition à l'examen décide de la création de la plate-forme mais sans en fixer les modalités de création et de fonctionnement. Le texte en projet sera complété aux fins de préciser plus avant ces points.

2. Au 2°, in fine, il y a lieu de remplacer les mots « par l'article 31, § 1er, al. 2 de la loi » par les mots « par l'article 31, § 1er, alinéa 2, et par l'article 36, § 2, de la loi ».

ONDERZOEK VAN HET ONTWERP

ALGEMENE OPMERKING

Bij artikel 6, § 1, van het ontwerp wordt aan het nationale CSIRT de bevoegdheid verleend om het formulier vast te stellen dat moet worden gebruikt om incidenten te melden.

Artikel 7 van het ontwerp geeft datzelfde CSIRT voorts de bevoegdheid om vast te stellen welke regels gelden voor de melding indien het meldingsplatform niet beschikbaar is, terwijl artikel 10 van het ontwerp het CSIRT bevoegd maakt om de regels voor de vrijwillige meldingen bedoeld in artikel 30 van de wet van 7 april 2019, vast te stellen.

Daarnaast schrijft artikel 9 voor dat het CSIRT, de sectorale overheden en de ADCC een "protocolakkoord" sluiten dat over meer dan louter operationele kwesties gaat en dat betrekking heeft op de "modaliteiten voor het beheer van het meldingsplatform", op "de modaliteiten voor de verwerking van meldingen, bedoeld in artikel 8, § 3" en op de "modaliteiten betreffende de verzoeken om bijkomende informatie gericht aan de aanbieder van essentiële diensten of digitaledienstverlener bedoeld in artikel 6, § 4". Die "modaliteiten" zijn volgens het verslag aan de Koning "nog niet door de Koning (...) bepaald" en zouden ook op de "financiering van het platform" betrekking hebben, alhoewel dat niet met zoveel woorden in de tekst van het ontwerp staat.

Zoals de afdeling Wetgeving al meermalen heeft opgemerkt, is het niet aanvaardbaar dat regelgevende bevoegdheden worden toegekend aan ambtenaren van een bestuur die aan de volksvertegenwoordiging geen politieke verantwoording verschuldigd zijn voor hun daden. Een subdelegatie aan die overheden is alleen bij uitzondering toegestaan als ze betrekking heeft op het vaststellen van maatregelen van louter bestuur of van in hoofdzaak technische maatregelen, wat in casu niet het geval is.

Het besluit is dan ook dat de bevoegdheid om die verschillende zaken vast te stellen, aan de minister moet worden toegekend. Heel het ontwerp moet dienovereenkomstig worden herzien.

BIJZONDERE OPMERKINGEN

AANHEF

1. Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 'houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie' verleent geen rechtsgrond aan het ontworpen besluit.

Die richtlijn hoort niet in de aanhef te worden vermeld. Het eerste lid van de aanhef moet dan ook worden weggelaten (1).

2. In het tweede lid, dat het eerste lid wordt, horen niet de artikelen 39, § 1,(2) en 61 van de wet van 7 april 2019 te worden vermeld, maar wel artikel 36 van die wet.

Dat lid moet dienovereenkomstig worden herzien.

3. In het derde lid, dat het tweede lid wordt, moet melding worden gemaakt van artikel 3, 3°, f), ingevoegd bij de wet van 7 april 2019, van artikel 24, § 2, eerste lid, en van artikel 31 van de wet van 1 juli 2011 'betreffende de beveiliging en de bescherming van de kritieke infrastructuren'.

Dat lid moet dienovereenkomstig worden herzien.

4. In het vijfde lid, dat het vierde lid wordt, moet worden vermeld dat de minister van Begroting het ontwerp akkoord heeft bevonden op 30 april 2019.

DISPOSITIEF

Artikel 1 (nieuw)

Overeenkomstig artikel 25, lid 1, alinea 3, van richtlijn (EU) 2016/1148 moet een nieuw artikel 1 worden ingevoegd waarin wordt vermeld dat het ontworpen besluit die richtlijn gedeeltelijk omzet.

Artikel 3

1. In paragraaf 1 dienen de woorden "in artikel 31" te worden vervangen door de woorden "in artikel 3, 3°, f)" (3).

2. In paragraaf 2 dienen de woorden "in bijlage 2, punt c)" te worden vervangen door de woorden "in bijlage 2, punt a)".

Artikel 5

1. In de voorliggende bepaling staat dat een platform wordt opgericht, maar er worden geen regels in vastgelegd voor de oprichting en de werkwijze van dat platform. De ontwerptekst moet worden aangevuld zodat hij die punten nader bepaalt.

2. In punt 2°, in fine, dienen de woorden "in artikel 31, § 1, tweede lid, van de wet" te worden vervangen door de woorden "in artikel 31, § 1, tweede lid, en in artikel 36, § 2, van de wet".

Article 12 (nouveau)

Il convient de prévoir un article 12 nouveau, comportant la formule exécutoire.

Annexes

Outre qu'il convient de pourvoir chaque annexe d'un intitulé, celles-ci doivent être complétées par la formule usuelle :

« Vu pour être annexé à notre arrêté... (date et intitulé) »(4).

Le greffier, Le Président,
Charles-Henri VAN HOVE Martine BAGUET

Notes

1 Concernant cette directive, spécialement son article 25, voir l'observation formulée sous l'article 1er (nouveau).

2 Pour les raisons évoquées à l'observation 1 relative aux formalités préalables.

3 Disposition insérée dans la loi du 1er juillet 2011 par l'article 75 de la loi du 7 avril 2019.

4 Principes de technique législative - Guide de rédaction des textes législatifs et réglementaires, www.raadvst-consetat.be, onglet « Technique législative », recommandation n° 172 et formule F 4-8-1.

Artikel 12 (nieuw)

Er dient voorzien te worden in een nieuw artikel 12 dat de uitvoeringsbepaling bevat.

Bijlagen

Naast het feit dat alle bijlagen een opschrift moeten krijgen, moeten ze ook worden aangevuld met de gebruikelijke formule:

"Gezien om gevoegd te worden bij ons besluit... (datum en opschrift)" (4).

De griffier, De voorzitter,
Charles-Henri VAN HOVE Martine BAGUET

Nota's

1 Betreffende die richtlijn, en in het bijzonder artikel 25 ervan, zie de opmerking die wordt gemaakt over het (nieuwe) artikel 1.

2 Om de redenen die in opmerking 1 betreffende de voorafgaande vormvereisten zijn aangehaald.

3 Bepaling in de wet van 1 juli 2011 ingevoegd bij artikel 75 van de wet van 7 april 2019.

4 Beginselen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten, www.raadvst-consetat.be, tab "Wetgevingstechniek", aanbeveling 172 en formule F 4 8 1.

12 JUILLET 2019. — Arrêté royal portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les articles 6, 1°, 2°, 7, 10, 31, § 1er, 36 et 39, § 1er;

Vu l'article 3, 3°, f), inséré par la loi du 7 avril 2019, l'article 24, § 2, alinéa 1er, et l'article 31 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques;

Vu l'avis de l'Inspecteur des Finances, donné le 18 mars 2019;

Vu l'accord de la Ministre du Budget, donné le 30 avril 2019;

Vu les avis sur l'article 11 du présent arrêté royal, rendus par la Banque nationale de Belgique, l'Autorité des services et marchés financiers et l'Institut belge des services postaux et des télécommunications;

Vu l'avis de l'Autorité de protection des données, rendu le 5 juin 2019;

Vu l'avis 66.225/4 du Conseil d'Etat, donné le 22 mai 2019 sur base de l'article 84, § 1er, alinéa 1er, 3°, des lois coordonnées sur le Conseil d'Etat;

Sur la proposition du Premier Ministre, du Ministre de la Sécurité et de l'Intérieur et de l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

CHAPITRE 1er. Objet

Article 1er. Le présent arrêté vise à transposer la directive européenne (EU) 2016/1148 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 (la « directive NIS »).

CHAPITRE 2. Définitions

Art. 2. Pour l'application du présent arrêté royal, il faut entendre par :

1° « loi » : la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

2° « CCB » : le Centre pour la Cybersécurité Belgique créé par l'arrêté royal du 10 octobre 2014;

12 JULI 2019. — Koninklijk besluit tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, de artikelen 6, 1°, 2°, 7, 10, 31, § 1, 36 en 39, § 1;

Gelet op artikel 3, 3°, f), ingevoegd bij de wet van 7 april 2019, artikel 24, § 2, eerste lid, en artikel 31 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;

Gelet op het advies van de Inspecteur van Financiën, gegeven op 18 maart 2019;

Gelet op de akkoordbevinding van de Minister van Begroting, gegeven op 30 april 2019;

Gelet op de adviezen over artikel 11 van dit koninklijk besluit, uitgebracht door de Nationale Bank van België, de Autoriteit voor Financiële Diensten en Markten en het Belgisch Instituut voor postdiensten en telecommunicatie;

Gelet op het advies van de Gegevensbeschermingsautoriteit, gegeven op 5 juni 2019;

Gelet op het advies 66.225/4 van de Raad van State, gegeven op 22 mei 2019 op basis van artikel 84, § 1, eerste lid, 3°, van de gecoördineerde wetten op de Raad van State;

Op de voordracht van de Eerste Minister en de Minister van Veiligheid en Binnenlandse Zaken, en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij :

HOOFDSTUK 1. Onderwerp

Artikel 1. Dit besluit voorziet in de omzetting van de Europese richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (de "NIS-richtlijn").

HOOFDSTUK 2. Definities

Art. 2. Voor de toepassing van dit koninklijk besluit wordt verstaan onder:

1° "wet": de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

2° "CCB": het Centrum voor Cybersecurity België opgericht bij het koninklijk besluit van 10 oktober 2014;

3° « DGCC » : la Direction générale Centre de Crise du Service public fédéral Intérieur, créée par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise;

4° « plate-forme de notification » : la plate-forme de notification d'incidents visée à l'article 31 de la loi.

CHAPITRE 3. Autorités compétentes

Art. 3. § 1er. Le CCB est désigné comme l'autorité visée à l'article 7, § 1er, et à l'article 10, § 1er, de la loi.

Le CCB est désigné comme le CSIRT national visé à l'article 7, § 2, de la loi.

§ 2. La DGCC est désignée comme l'autorité visée à l'article 7, § 4, de la loi.

§ 3. Les autorités sectorielles visées à l'article 7, § 3, de la loi sont désignées à l'annexe 1.

§ 4. Les services d'inspection visés à l'article 7, § 5, de la loi sont désignés à l'annexe 2.

Art. 4. § 1er. Pour les infrastructures critiques du secteur de la santé, l'autorité sectorielle visée à l'article 3, 3°, f), de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques est désignée à l'annexe 1, point c).

§ 2. Pour les infrastructures critiques du secteur de la santé, le service d'inspection visé à l'article 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques est désigné à l'annexe 2, point a).

CHAPITRE 4. Notification et traitement des incidents

Section 1re. Champ d'application et plate-forme de notification

Art. 5. Le présent chapitre s'applique aux notifications d'incidents visés par les articles 24, 26, § 1er, 27, 31 et 35 de la loi du 7 avril 2019.

Art. 6. Une plate-forme sécurisée de notification est créée afin de faciliter :

1° l'envoi par les opérateurs de services essentiels et les fournisseurs de service numérique au CSIRT national, à l'autorité sectorielle ou son CSIRT sectoriel, et à la DGCC, des notifications d'incidents de sécurité effectuées en vertu de la loi du 7 avril 2019;

2° la possibilité d'envoi, par les opérateurs de services essentiels et les fournisseurs de service numérique, d'une notification de violations de données à caractère personnel à une autorité de contrôle des données à caractère personnel, telle que prévue par l'article 31, § 1er, alinéa 2, et par l'article 36, § 2, de la loi.

Art. 7. La plate-forme visée à l'article 6 est accessible par le biais d'Internet pour les opérateurs de services essentiels et les fournisseurs de service numérique au moyen d'une connexion sécurisée et l'utilisation d'une clé d'identification unique à chaque opérateur de services essentiels ou fournisseur de service numérique.

Section 2. Notifications

Art. 8. § 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.

La notification contient toutes les informations disponibles permettant de déterminer la nature, les causes, les effets et les conséquences de l'incident.

§ 2. Lorsque l'opérateur de services essentiels ou le fournisseur de service numérique n'est pas en mesure de fournir toutes les informations reprises dans le formulaire à l'aide des éléments en sa possession, il complète la notification initiale via la plate-forme de notification dès que les informations manquantes sont disponibles.

§ 3. Il fait de même lorsque de nouvelles informations sont connues ou lorsque des développements importants surviennent.

§ 4. A la demande du CSIRT national, de la DGGC, de l'autorité sectorielle ou de son CSIRT sectoriel, l'opérateur de services essentiels ou le fournisseur de service numérique notifie via la plate-forme de notification une mise à jour du formulaire de notification retraçant la gestion de l'incident de sa découverte à sa clôture et reprenant toutes les informations reprises dans le formulaire de notification.

Art. 9. En cas d'indisponibilité de la plate-forme de notification visée à l'article 6, le CSIRT national informe les opérateurs de services essentiels et les fournisseurs de service numérique des modalités opérationnelles de notification à utiliser.

3° "ADCC": de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, opgericht bij het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering;

4° "meldingsplatform": het platform voor de melding van incidenten bedoeld in artikel 31 van de wet.

HOOFDSTUK 3. Bevoegde autoriteiten

Art. 3. § 1. Het CCB wordt aangewezen als de autoriteit bedoeld in artikel 7, § 1, en artikel 10, § 1, van de wet.

Het CCB wordt aangewezen als het nationale CSIRT bedoeld in artikel 7, § 2, van de wet.

§ 2. De ADCC wordt aangewezen als de autoriteit bedoeld in artikel 7, § 4, van de wet.

§ 3. De sectorale overheden bedoeld in artikel 7, § 3, van de wet worden aangewezen in bijlage 1.

§ 4. De inspectiediensten bedoeld in artikel 7, § 5, van de wet worden aangewezen in bijlage 2.

Art. 4. § 1. Voor de kritieke infrastructuren van de sector gezondheidszorg wordt de sectorale overheid bedoeld in artikel 3, 3°, f), van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren aangewezen in bijlage 1, punt c).

§ 2. Voor de kritieke infrastructuren van de sector gezondheidszorg wordt de inspectiedienst bedoeld in artikel 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren aangewezen in bijlage 2, punt a).

HOOFDSTUK 4. Melding en verwerking van incidenten

Afdeling 1. Toepassingsgebied en meldingsplatform

Art. 5. Dit hoofdstuk is van toepassing op de meldingen van incidenten bedoeld in de artikelen 24, 26, § 1, 27, 31 en 35 van de wet van 7 april 2019.

Art. 6. Een beveiligd meldingsplatform wordt opgericht met het oog op:

1° het melden van beveiligingsincidenten door aanbieders van essentiële diensten en digitaledienstverleners aan het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de ADCC, krachtens de wet van 7 april 2019;

2° het eventueel melden van inbreuken in verband met persoonsgegevens door aanbieders van essentiële diensten en digitaledienstverleners aan een toezichthoudende autoriteit persoonsgegevens, zoals bepaald in artikel 31, § 1, tweede lid, en in artikel 36, § 2, van de wet.

Art. 7. De aanbieders van essentiële diensten en digitaledienstverleners hebben via internet toegang tot het in artikel 6 bedoelde platform door middel van een beveiligde verbinding en een voor elke aanbieder van essentiële diensten of digitaledienstverlener unieke identificatiesleutel.

Afdeling 2. Meldingen

Art. 8. § 1. De melding gebeurt via het meldingsplatform met behulp van het formulier voor het melden van incidenten dat is opgesteld door het nationale CSIRT.

De melding omvat alle beschikbare informatie die toelaat de aard, de oorzaken, de effecten en de gevolgen van het incident te bepalen.

§ 2. Wanneer de aanbieder van essentiële diensten of digitaledienstverlener niet alle in het formulier gevraagde informatie kan verstrekken met behulp van de gegevens waarover hij beschikt, vult hij de oorspronkelijke melding via het meldingsplatform aan zodra de ontbrekende informatie beschikbaar is.

§ 3. Hij doet dit eveneens in geval van nieuwe informatie of belangrijke ontwikkelingen.

§ 4. Op verzoek van het nationale CSIRT, de ADCC, de sectorale overheid of haar sectorale CSIRT meldt de aanbieder van essentiële diensten of digitaledienstverlener via het meldingsplatform een actualisering van het meldingsformulier waarin hij de behandeling van het incident beschrijft vanaf het ontdekken tot het afsluiten ervan en alle informatie van het meldingsformulier overneemt.

Art. 9. Indien het meldingsplatform bedoeld in artikel 6 niet beschikbaar is, informeert het nationale CSIRT de aanbieders van essentiële diensten en digitaledienstverleners over de te gebruiken operationele meldingsmodaliteiten.

Section 3. Traitement de l'incident

Art. 10. § 1er. Le CSIRT national, l'autorité sectorielle ou son CSIRT sectoriel ou la DGCC peuvent demander à l'opérateur de services essentiels ou au fournisseur de service numérique des informations complémentaires sur les notifications qu'il a effectuées.

§ 2. Lorsque les circonstances le permettent, le CSIRT national fournit à l'opérateur de services essentiels, ou au fournisseur de service numérique qui est à l'origine de la notification toutes les informations utiles au suivi de sa notification, et le cas échéant toutes les informations qui pourraient contribuer à une gestion efficace de l'incident.

§ 3. Sans préjudice des règles applicables à la gestion de crise en cas de cyberincidents visée à l'article 3, 5°, de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, le CSIRT national assure la coordination du traitement des notifications au niveau national et international.

Section 4. Protocole d'accord

Art. 11. Le CSIRT national, les autorités sectorielles et la DGCC concluent un protocole d'accord pour fixer les modalités opérationnelles :

1° de gestion de la plate-forme de notification;

2° du traitement des notifications visées à l'article 8, § 3;

3° des demandes d'information complémentaire à l'opérateur de services essentiels ou au fournisseur de service numérique visées à l'article 6, § 4.

CHAPITRE 5. Les notifications volontaires

Art. 12. § 1er. Les notifications volontaires visées à l'article 30 de la loi sont adressées directement au CSIRT national.

§ 2. Les modalités opérationnelles de cette notification sont déterminées par le CSIRT national et publiées sur son site internet.

§ 3. Le CSIRT national transmet les informations relatives à ces notifications à la DGCC et aux autorités sectorielles ou CSIRT sectoriels potentiellement intéressés.

CHAPITRE 6. Dérogations

Art. 13. Il est dérogé aux chapitres IV et V pour les notifications de violations de données à caractère personnel, qui suivent les règles légales ou imposées par l'autorité de contrôle des données à caractère personnel visée à l'article 6, 4°, de la loi du 7 avril 2019.

CHAPITRE 7. Les organismes d'évaluation de la conformité

Art. 14. Les organismes d'évaluation de la conformité qui souhaitent être accrédités pour l'audit externe et la certification des opérateurs de services essentiels, visés aux articles 22, § 2, et 38, § 2, de la loi, ou l'audit externe de fournisseurs de service numérique, doivent introduire une demande auprès de l'autorité nationale d'accréditation ou d'une institution qui est co-signataire des accords de reconnaissance du« European Cooperation for Accreditation ».

Les conditions auxquelles l'organisme d'évaluation de la conformité doit répondre pour être accrédité à cette fin sont les suivantes :

1° satisfaire, à tout moment, aux critères d'accréditation prévus par les normes ISO/IEC 17021 ou ISO/IEC 17065, lesquelles spécifient (a) les exigences génériques et spécifiées applicables aux organismes procédant à l'audit et à la certification des systèmes de management et; (b) les exigences visant à garantir que les organismes de certification exploitent des programmes de certification avec compétence, cohérence et impartialité;

2° satisfaire aux procédures de fonctionnement du système d'accréditation qui sont applicables aux organismes accrédités.

Afdeling 3. Verwerking van het incident

Art. 10. § 1. Het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, of de ADCC kunnen de aanbieder van essentiële diensten of digitaledienstverlener bijkomende informatie vragen over diens meldingen.

§ 2. Wanneer de omstandigheden dit toelaten, verstrekt het nationale CSIRT de aanbieder van essentiële diensten of digitaledienstverlener die de melding heeft ingediend, alle informatie die nuttig is voor de opvolging van diens melding, en, in voorkomend geval, alle informatie die kan bijdragen tot een doeltreffende behandeling van het incident.

§ 3. Onverminderd de regels die van toepassing zijn op het crisisbeheer bij cyberincidenten, bedoeld in artikel 3, 5°, van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, coördineert het nationale CSIRT de verwerking van de meldingen op nationaal en internationaal niveau.

Afdeling 4. Protocolakkoord

Art. 11. Het nationale CSIRT, de sectorale overheden en de ADCC sluiten een protocolakkoord om de operationele modaliteiten vast te leggen voor:

1° het beheer van het meldingsplatform;

2° de verwerking van meldingen bedoeld in artikel 8, § 3;

3° de verzoeken om bijkomende informatie gericht aan de aanbieder van essentiële diensten of digitaledienstverlener bedoeld in artikel 6, § 4.

HOOFDSTUK 5. Vrijwillige meldingen

Art. 12. § 1. De vrijwillige meldingen bedoeld in artikel 30 van de wet worden rechtstreeks naar het nationale CSIRT gestuurd.

§ 2. De operationele modaliteiten van deze melding worden bepaald door het nationale CSIRT en op zijn website bekendgemaakt.

§ 3. Het nationale CSIRT bezorgt de informatie over deze meldingen aan de ADCC en aan de mogelijk belanghebbende sectorale overheden of sectorale CSIRT's.

HOOFDSTUK 6. Afwijkingen

Art. 13. Er wordt afgeweken van hoofdstuk IV en V voor de melding van inbreuken in verband met persoonsgegevens, die onderworpen blijft aan de wettelijke regels of de regels opgelegd door de toezichthoudende autoriteit persoonsgegevens bedoeld in artikel 6, 4°, van de wet van 7 april 2019.

HOOFDSTUK 7. Instellingen voor de conformiteitsbeoordeling

Art. 14. De instellingen voor de conformiteitsbeoordeling die geaccrediteerd wensen te worden voor de externe audit en certificering van aanbieders van essentiële diensten, bedoeld in de artikelen 22, § 2, en 38, § 2, van de wet, of voor de externe audit van digitaledienstverleners, moeten een aanvraag indienen bij de nationale accreditatie-autoriteit of bij een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft.

Om daarvoor te worden geaccrediteerd, moet de instelling voor de conformiteitsbeoordeling de volgende voorwaarden vervullen:

1° op ieder ogenblik voldoen aan de accreditatiecriteria van de normen ISO/IEC 17021 of ISO/IEC 17065. Deze normen specificeren (a) de algemene en specifieke eisen die gelden voor instellingen die audits en certificering van managementsystemen uitvoeren en; (b) voorschriften om ervoor te zorgen dat certificeringsinstellingen certificeringsregelingen op competente, consistente en onpartijdige wijze uitvoeren;

2° voldoen aan de werkingsprocedures van het accreditatiesysteem die van toepassing zijn op de geaccrediteerde instellingen.

CHAPITRE 8. Dispositions finales

Art. 15. Le présent arrêté entre en vigueur le jour de sa publication au *Moniteur belge*.

Art. 16. Le Premier Ministre et le Ministre ayant la sécurité et l'Intérieur dans ses attributions sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Donné à Bruxelles, le 12 juillet 2019.

PHILIPPE

Par le Roi :

Le Premier Ministre,
CH. MICHEL

Le Ministre de la Sécurité et de l'Intérieur,
P. DE CREM

Annexe 1 à l'arrêté royal du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

Les autorités sectorielles désignées par Nous:

a) pour le secteur de l'énergie : le Ministre fédéral ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur);

b) pour le secteur des transports :

- En ce qui concerne le secteur du transport, à l'exception du transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour le Transport, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur);

- En ce qui concerne le transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour la Mobilité maritime, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur);

c) pour le secteur de la santé : le Ministre fédéral ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur);

d) pour le secteur des fournisseurs de service numérique : le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).

Vu pour être annexé à Notre arrêté du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

PHILIPPE

Par le Roi :

Le Premier Ministre,
Ch. MICHEL

Le Ministre de la Sécurité et de l'Intérieur,
P. DE CREM

Annexe 2 à l'arrêté royal du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

HOOFDSTUK 8. Slotbepalingen

Art. 15. Dit besluit treedt in werking de dag waarop het in het *Belgisch Staatsblad* wordt bekendgemaakt.

Art. 16. De Eerste Minister en de Minister bevoegd voor veiligheid en binnenlandse zaken zijn, ieder wat hem betreft, belast met de uitvoering van dit besluit.

Gegeven te Brussel, 12 juli 2019.

FILIP

Van Koningswege :

De Eerste Minister,
CH. MICHEL

De Minister van Veiligheid en Binnenlandse Zaken,
P. DE CREM

Bijlage 1 bij het koninklijk besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

De door Ons aangewezen sectorale overheden :

a) voor de sector energie: de federale Minister bevoegd voor Energie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de Minister per deelsector een andere gemachtigde aanwijzen);

b) voor de sector vervoer:

- Voor wat betreft de sector vervoer, met uitzondering van het vervoer over wateren toegankelijk voor zeeschepen: de federale Minister bevoegd voor Vervoer of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de Minister per deelsector een andere gemachtigde aanwijzen);

- Voor wat betreft het vervoer over wateren toegankelijk voor zeeschepen: de federale Minister bevoegd voor Maritieme Mobiliteit of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de Minister per deelsector een andere gemachtigde aanwijzen);

c) voor de sector gezondheidszorg: de federale Minister bevoegd voor Volksgezondheid of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de Minister per deelsector een andere gemachtigde aanwijzen);

d) voor de sector digitaledienstverleners: de federale Minister bevoegd voor Economie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de Minister per deelsector een andere gemachtigde aanwijzen).

Gezien om te worden gevoegd bij Ons besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

FILIP

Van Koningswege :

De Eerste Minister,
Ch. MICHEL

De Minister van Veiligheid en Binnenlandse Zaken,
P. DE CREM

Bijlage 2 bij het koninklijk besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

Les services d'inspection désignés par Nous :

a) pour le secteur de la santé: le service public fédéral Santé publique;

b) pour le secteur de l'énergie à l'exception des éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité : le service public fédéral Economie;

c) pour le secteur des fournisseurs de service numérique : le service public fédéral Economie.

Vu pour être annexé à Notre arrêté du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

PHILIPPE

Par le Roi :

Le Premier Ministre,
Ch. MICHEL

Le Ministre de la Sécurité et de l'Intérieur,
P. DE CREM

De door Ons aangewezen inspectiediensten :

a) voor de sector gezondheidszorg: de Federale Overheidsdienst Volksgezondheid;

b) voor de sector energie, met uitzondering van de elementen van een nucleaire installatie, bestemd voor de industriële productie van elektriciteit, die dienen voor de transmissie van de elektriciteit: de Federale Overheidsdienst Economie;

c) voor de sector digitaledienstverleners: de Federale Overheidsdienst Economie.

Gezien om te worden gevoegd bij Ons besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

FILIP

Van Koningswege :

De Eerste Minister,
Ch. MICHEL

De Minister van Veiligheid en Binnenlandse Zaken,
P. DE CREM

SERVICE PUBLIC FEDERAL INTERIEUR

[C − 2019/13569]

6 DECEMBRE 2018. — Accord de coopération entre l'État fédéral, la Région wallonne, la Région flamande, la Région de Bruxelles-Capitale et la Communauté germanophone portant exécution à l'accord de coopération du 2 février 2018 entre l'Etat fédéral, la Région wallonne, la Région flamande, la Région de Bruxelles-Capitale et la Communauté germanophone portant sur la coordination des politiques d'octroi d'autorisations de travail et d'octroi du permis de séjour, ainsi que les normes relatives à l'emploi et au séjour des travailleurs étrangers

RAPPORT AU ROI

Sire,

I. COMMENTAIRE GENERAL

1. Objectif de l'accord

Suite à la loi spéciale relative à la sixième réforme de l'Etat du 6 janvier 2014 (*M.B.*, 31 janvier 2014), laquelle est entrée en vigueur le 1er juillet 2014, les compétences en matière d'occupation des travailleurs étrangers ont été transférées aux entités fédérées. Toutefois, la réglementation relative à l'accès à l'emploi en fonction de la situation de séjour des personnes concernées de même que les normes relatives à l'accès au territoire, au séjour, à l'établissement et à l'éloignement des étrangers restent une compétence fédérale.

L'article 92*bis* de la loi spéciale du 8 août 1980 de réformes institutionnelles (ci-après dénommée : « LSRI »), dans ses paragraphes 1er et 3, *c)* impose à l'Autorité fédérale et aux Régions la conclusion d'un accord de coopération pour la coordination des politiques d'octroi du permis de travail et d'octroi du permis de séjour, ainsi que les normes relatives à l'emploi de travailleurs étrangers.

En outre, l'article 92*bis*, paragraphe 1er, alinéa 3 de la LSRI permet à un accord de coopération, qui a reçu les assentiments requis, de prévoir que sa mise en œuvre sera assurée par des accords d'exécution ayant effet sans que l'assentiment parlementaire ne soit exigé.

Le 2 février 2018, l'Etat fédéral, les Régions et la Communauté germanophone ont conclu un accord de coopération portant sur la coordination des politiques d'octroi d'autorisations de travail et d'octroi du permis de séjour, ainsi que les normes relatives à l'emploi et au séjour des travailleurs étrangers (ci-après dénommé « l'accord de coopération du 2 février 2018 »). Cet accord transpose partiellement la directive 2011/98/UE du Parlement européen et du Conseil du 13 décembre 2011 établissant une procédure de demande unique en vue de la délivrance d'un permis unique autorisant les ressortissants de pays tiers à résider et à travailler sur le territoire d'un État membre et établissant un socle commun de droits pour les travailleurs issus de pays tiers qui résident légalement dans un État membre (ci-après dénommée « la directive 2011/98/UE »). Par ailleurs, il s'applique à

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[C − 2019/13569]

6 DECEMBER 2018. — Samenwerkingsakkoord tussen de Federale Staat, het Waals Gewest, het Vlaams Gewest, het Brussels-Hoofdstedelijk Gewest en de Duitstalige Gemeenschap houdende uitvoering van het samenwerkingsakkoord van 2 februari 2018 tussen de Federale Staat, het Waals Gewest, het Vlaams Gewest, het Brussels-Hoofdstedelijk Gewest en de Duitstalige Gemeenschap met betrekking tot de coördinatie tussen het beleid inzake de toelatingen tot arbeid en het beleid inzake de verblijfsvergunningen en inzake de normen betreffende de tewerkstelling en het verblijf van buitenlandse arbeidskrachten

VERSLAG AAN DE KONING

Sire,

I. ALGEMENE COMMENTAAR

1. Doelstelling van het akkoord

Ingevolge de bijzondere wet met betrekking tot de zesde staatshervorming van 6 januari 2014 (*B.S.*, 31 januari 2014), die in werking trad op 1 juli 2014, zijn de bevoegdheden inzake de tewerkstelling van buitenlandse werknemers overgedragen aan de deelstaten. De reglementering inzake de toegang tot werk naar gelang van de verblijfssituatie van de betrokken personen en ook de regels inzake de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen blijven evenwel een federale bevoegdheid.

Artikel 92*bis* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen (hierna: "BWHI"), verplicht in zijn paragrafen 1 en 3, *c)*, de Federale Overheid en de Gewesten een samenwerkingsakkoord af te sluiten voor het coördineren van het beleid inzake de toelatingen tot arbeid en het beleid inzake de verblijfsvergunningen en inzake de normen betreffende de tewerkstelling van buitenlandse arbeidskrachten.

Bovendien staat artikel 92*bis*, paragraaf 1, derde lid, van de BWHI toe, dat een samenwerkingsakkoord, dat de vereiste instemming heeft gekregen, bepaalt dat zijn toepassing wordt gegarandeerd door uitvoeringsbesluiten die uitwerking hebben zonder dat de parlementaire instemming is vereist.

Op 2 februari 2018 hebben de Federale Staat, de Gewesten en de Duitstalige Gemeenschap een samenwerkingsakkoord gesloten over het coördineren van het beleid inzake arbeidsvergunningen en het beleid inzake verblijfsvergunningen en inzake de regels betreffende de tewerkstelling van buitenlandse werknemers (hierna: "samenwerkingsakkoord van 2 februari 2018"). Dit akkoord is een gedeeltelijke omzetting van richtlijn 2011/98/EU van het Europees Parlement en de Raad van 13 december 2011 betreffende de gecombineerde aanvraagprocedure voor een gecombineerde vergunning voor onderdanen van derde landen om te verblijven en te werken op het grondgebied van een lidstaat, alsmede inzake een gemeenschappelijk pakket rechten voor werknemers uit derde landen die legaal in een lidstaat verblijven (hierna: "richtlijn 2011/98/EU"). Het is overigens van toepassing op