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

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[C − 2024/005260]

9 JUNI 2024. — Koninklijk besluit tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de Grondwet, artikel 108;

Gelet op de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, de artikelen 15, §§ 1 en 2, eerste lid, 17, 7° en 10°, 39, eerste lid, 40, § 1, eerste lid, 41, 47, § 1, 50, § 2, 63, §§ 1 en 2, en 75;

Gelet op 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 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 30 oktober 2023;

Gelet op de akkoordbevinding van de Staatssecretaris voor Begroting, gegeven op 7 november 2023;

Gelet op de adviesaanvraag binnen dertig dagen, die op 19 april 2024 bij de Raad van State is ingediend, met toepassing van artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Overwegende dat het advies niet is meegedeeld binnen die termijn;

Gelet op artikel 84, § 5, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Overwegende het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België;

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

Hebben Wij besloten en besluiten Wij :

HOOFDSTUK 1 — *Voorwerp en definities*

Artikel 1. Dit besluit voorziet in de omzetting van de Europese richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148.

Art. 2. Voor de toepassing van dit besluit zijn de definities bedoeld in artikel 8 van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid van toepassing.

Voor de toepassing van dit besluit, moet worden verstaan onder:

1° "NIS2-wet" : de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

2° "conformiteitsbeoordeling": de beoordeling bedoeld in artikel 2, punt 12 van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93;

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[C − 2024/005260]

9 JUIN 2024. — Arrêté royal exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

Vu la Constitution, l'article 108 ;

Vu la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les articles 15, §§ 1er et 2, alinéa 1er, 17, 7° et 10°, 39, alinéa 1er, 40, § 1er, alinéa 1er, 41, 47, § 1er, 50, § 2, 63, §§ 1er et 2, et 75;

Vu 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;

Vu l'avis de l'Inspecteur des Finances, donné le 30 octobre 2023;

Vu l'accord de la Secrétaire d'État au Budget, donné le 7 novembre 2023;

Vu la demande d'avis dans un délai de trente jours, adressée au Conseil d'État le 19 avril 2024, en application de l'article 84, § 1er, alinéa 1er, 2°, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973;

Considérant l'absence de communication de l'avis dans ce délai;

Vu l'article 84, § 5, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973;

Considérant l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique;

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

Nous avons arrêté et arrêtons :

CHAPITRE 1er — *Objet et définitions*

Article 1er. Le présent arrêté vise à transposer la directive européenne (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.

Art. 2. Pour l'application du présent arrêté, les définitions visées à l'article 8 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique sont d'application.

Pour l'application du présent arrêté, il faut entendre par :

1° « loi NIS2 » : la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

2° « évaluation de la conformité » : évaluation visée à l'article 2, point 12 du Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil;

3° "conformiteitsattest": afgifte van een bevestiging van conformiteit gebaseerd op een beslissing die de naleving van de gespecifieerde eisen aantoont. Het document kan het resultaat bevatten van een verificatie of certificering;

4° "verificatie": bevestiging van een verklaring door middel van objectieve bewijzen, dat aan de gespecifieerde einsen is voldaan;

5° "verklaring": door de entiteit verklaarde informatie.

HOOFDSTUK 2 — *Aanwijzing van de bevoegde autoriteiten*

Art. 3. § 1. Het Centrum voor Cybersecurity België, opgericht bij het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, wordt aangewezen als nationale cyberbeveiligingsautoriteit.

§ 2. De volgende autoriteiten worden aangewezen als sectorale overheden:

1° 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);

2° voor de sector vervoer:

- wat betreft de sector vervoer, met uitzondering van het vervoer over water: 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);

- wat betreft het vervoer over water: 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);

3° voor de sector gezondheidszorg:

- wat betreft entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen zoals gedefinieerd in artikel 1, punt 2, van Richtlijn 2001/83/EG van het Europees Parlement en de Raad van 6 november 2001 tot vaststelling van een communautair wetboek betreffende geneesmiddelen voor menselijk gebruik; entiteiten die farmaceutische basisproducten en farmaceutische bereidingen vervaardigen als bedoeld in bijlage I, sectie C, afdeling 21, van Verordening (EG) nr. 1893/2006 van het Europees Parlement en de Raad van 20 december 2006 tot vaststelling van de statistische classificatie van economische activiteiten NACE Rev. 2 en tot wijziging van Verordening (EEG) nr. 3037/90 en enkele EG-verordeningen op specifieke statistische gebieden; en entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd ("de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") in de zin van artikel 22 van Verordening (EU) 2022/123 van het Europees Parlement en de Raad van 25 januari 2022 betreffende een grotere rol van het Europees Geneesmiddelenbureau inzake crisisparaatheid en -beheersing op het gebied van geneesmiddelen en medische hulpmiddelen: het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten opgericht door de wet van 20 juli 2006 betreffende de oprichting en de werking van het federaal Agentschap voor geneesmiddelen en gezondheidsproducten;

- wat betreft de andere soorten entiteiten van de sector gezondheidszorg: de federale minister bevoegd voor Volksgezondheid of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;

4° voor de sector digitale infrastructuur, alleen voor wat betreft de verleners van vertrouwensdiensten: de federale minister bevoegd voor Economie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;

5° voor de sector digitale aanbieders: de federale minister bevoegd voor Economie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;

6° voor de sector ruimtevaart en de sector onderzoek: de federale minister van Wetenschapsbeleid of bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;

3° « attestation de conformité » : délivrance d'une affirmation de conformité basée sur une décision indiquant que le respect des exigences spécifiées a été démontré. Le document peut contenir le résultat d'une vérification ou certification;

4° « vérification » : confirmation d'une déclaration, par des preuves objectives, que les exigences spécifiées ont été satisfaites;

5° « déclaration » : informations déclarées par l'entité.

CHAPITRE 2 — *Désignation des autorités compétentes*

Art. 3. § 1er. Le Centre pour la Cybersécurité Belgique, créé par l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, est désigné comme autorité nationale de cybersécurité.

§ 2. Les autorités suivantes sont désignées comme autorités sectorielles :

1° 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);

2° pour le secteur des transports :

- en ce qui concerne le secteur du transport, à l'exception du transport par eau : 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 eau: 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);

3° pour le secteur de la santé :

- en ce qui concerne les entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain; les entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de l'annexe I, section C, division 21 du Règlement (CE) n° 1893/2006 du Parlement européen et du Conseil du 20 décembre 2006 établissant la nomenclature statistique des activités économiques NACE Rév. 2 et modifiant le règlement (CEE) n° 3037/90 du Conseil ainsi que certains règlements (CE) relatifs à des domaines statistiques spécifiques; et les entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux : l'Agence fédérale des médicaments et des produits de santé créée par la loi du 20 juillet 2006 relative à la création et au fonctionnement de l'Agence fédérale des médicaments et des produits de santé;

- en ce qui concerne les autres types d'entités du 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;

4° pour le secteur de l'infrastructure numérique, uniquement en ce qui concerne les prestataires de services de confiance : le ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration;

5° pour le secteur des fournisseurs numériques : le ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration;

6° pour les secteurs de l'espace et de la recherche : le ministre fédéral de la Politique scientifique ou par délégation de celui-ci, un membre dirigeant du personnel de son administration;

7° voor de deelsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek, van de sector vervaardiging: het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten.

HOOFDSTUK 3 — *Referentiekaders voor de regelmatige conformiteitsbeoordeling*

Art. 4. § 1. De nationale cyberbeveiligingsautoriteit zorgt, in overleg met de relevante belanghebbenden, voor de uitwerking, actualisering en openbaarmaking, met name via haar website, van een referentiekader. Dit kader bevat de praktische modaliteiten voor de beoordeling van de in artikel 30, § 3, van de NIS2-wet, bedoelde minimale maatregelen voor het beheer van cyberbeveiligingsrisico's.

Overeenkomstig de internationale regels met betrekking tot conformiteitsbeoordelingsschema's zijn de in het eerste lid bedoelde relevante belanghebbenden ten minste de autoriteiten vermeld in artikel 15 van de NIS2-wet, de geaccrediteerde instanties en de organisaties die het referentiekader het eerste lid gebruiken.

§ 2. Het referentiekader beschrijft, op evenredige wijze, ten minste de volgende zekerheidsniveaus: basis, belangrijk en essentieel.

Art. 5. § 1. In het kader van de in artikel 39 van de NIS2-wet bedoelde conformiteitsbeoordeling en rekening houdend met de relevante methoden voor risicoanalyse, kiezen essentiële entiteiten één of meer referentiekaders waarvan het toepassingsgebied alle netwerk- en informatiesystemen van de entiteit omvat uit een van de volgende referentiekaders:

1° het in artikel 4 bedoelde referentiekader; of

2° de norm NBN EN ISO/IEC 27001.

§ 2. In het kader van de vrijwillige conformiteitsbeoordeling bedoeld in artikel 41 van de NIS2-wet kiezen belangrijke entiteiten een van de in paragraaf 1 bedoelde referentiekaders.

HOOFDSTUK 4 — *Modaliteiten van de regelmatige conformiteitsbeoordeling van essentiële entiteiten*

Art. 6. In het kader van de conformiteitsbeoordeling door een conformiteitsbeoordelingsinstantie die overeenkomstig hoofdstuk 6 erkend is door de nationale cyberbeveiligingsautoriteit en op basis van het in artikel 4 bedoelde referentiekader, verkrijgen essentiële entiteiten een certificering voor het niveau "essentieel" van voornoemd referentiekader.

Art. 7. In afwijking van artikel 6 kunnen essentiële entiteiten, indien zij dit motiveren, een verificatie verkrijgen die uitgevoerd wordt door een conformiteitsbeoordelingsinstantie die overeenkomstig hoofdstuk 6 erkend is door de nationale cyberbeveiligingsautoriteit, voor een lager niveau van het in artikel 4 bedoelde referentiekader, indien het resultaat van hun risicoanalyse bedoeld in artikel 30, § 5, eerste lid, van de NIS2-wet dit rechtvaardigt.

Het gebruik van de in het eerste lid bedoelde afwijking valt onder de verantwoordelijkheid van de essentiële entiteit en wordt als zodanig niet beoordeeld door een conformiteitsbeoordelingsinstantie.

Art. 8. In het kader van de conformiteitsbeoordeling op basis van het referentiekader bedoeld in artikel 5, § 1, 2°, verkrijgen essentiële entiteiten een certificering via een procedure van regelmatige audits uitgevoerd door een conformiteitsbeoordelingsinstantie die overeenkomstig hoofdstuk 6 erkend is door de nationale cyberbeveiligingsautoriteit.

Art. 9. Ongeacht het gekozen referentiekader bezorgen essentiële entiteiten hun conformiteitsattest en de risicoanalyse bedoeld in artikel 30, § 5, eerste lid, van de NIS2-wet elektronisch aan de nationale cyberbeveiligingsautoriteit.

Daartoe creëert en actualiseert de nationale cyberbeveiligingsautoriteit een beveiligd platform dat voor de entiteiten toegankelijk is via internet.

Art. 10. In het kader van artikel 39, eerste lid, 2°, van de NIS2-wet vindt de regelmatige conformiteitsbeoordeling door de inspectiedienst van de nationale cyberbeveiligingsautoriteit niet meer dan één keer per jaar plaats.

7° pour le sous-secteur de la fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro, du secteur de la fabrication : l'Agence fédérale des médicaments et des produits de santé.

CHAPITRE 3 — *Cadres de référence pour l'évaluation périodique de la conformité*

Art. 4. § 1er. L'autorité nationale de cybersécurité élabore, en concertation avec les parties prenantes concernées, maintient à jour et met à disposition du public, notamment sur son site internet, un cadre de référence reprenant les modalités pratiques d'évaluation des mesures minimales de gestion des risques en matière de cybersécurité visées à l'article 30, § 3, de la loi NIS2.

Conformément aux règles internationales en matière de schémas d'évaluation de la conformité, les parties prenantes concernées au sens de l'alinéa 1er sont au moins les autorités visées à l'article 15 de la loi NIS2, les organismes accrédités et les organisations qui utilisent le référentiel visé à l'alinéa 1er.

§ 2. Le cadre de référence contient, de manière proportionnée, au minimum les niveaux d'assurance suivants : basique, important et essentiel.

Art. 5. § 1er. Dans le cadre de l'évaluation de la conformité visée à l'article 39 de la loi NIS2 et en tenant compte des méthodologies d'analyse des risques pertinentes, les entités essentielles choisissent un ou plusieurs cadres de référence dont le champ d'application couvre l'ensemble des réseaux et systèmes d'information de l'entité parmi les cadres de référence suivants :

1° le cadre de référence visé à l'article 4; ou

2° la norme NBN EN ISO/IEC 27001.

§ 2. Dans le cadre de l'évaluation volontaire de la conformité visée à l'article 41 de la loi NIS2, les entités importantes choisissent un cadre de référence parmi les cadres de référence visés au paragraphe 1er.

CHAPITRE 4 — *Modalités de l'évaluation périodique de la conformité des entités essentielles*

Art. 6. Dans le cadre de l'évaluation de la conformité effectuée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité conformément au chapitre 6 et sur base du cadre de référence visé à l'article 4, les entités essentielles obtiennent une certification au niveau essentiel du cadre de référence précité.

Art. 7. Par dérogation à l'article 6, les entités essentielles peuvent, de manière motivée, obtenir une vérification, effectuée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité conformément au chapitre 6, à un niveau inférieur du cadre de référence visé à l'article 4 si le résultat de leur analyse des risques visée à l'article 30, § 5, alinéa 1er, de la loi NIS2 le justifie.

L'usage de la dérogation visée à l'alinéa 1er relève de la responsabilité de l'entité essentielle et ne fait pas, en tant que tel, l'objet d'une évaluation de la part d'un organisme d'évaluation de la conformité.

Art. 8. Dans le cadre de l'évaluation de la conformité effectuée sur base du cadre de référence visé à l'article 5, § 1er, 2°, les entités essentielles obtiennent une certification au travers d'une procédure d'audits réguliers effectués par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité conformément au chapitre 6.

Art. 9. Quel que soit le cadre de référence choisi, les entités essentielles communiquent leur attestation de conformité ainsi que l'analyse des risques visée à l'article 30, § 5, alinéa 1er, de la loi NIS2, à l'autorité nationale de cybersécurité, de manière électronique.

A cette fin, l'autorité nationale de cybersécurité crée, maintient à jour et met à disposition des entités une plateforme sécurisée accessible par le biais d'internet.

Art. 10. Dans le cadre de l'article 39, alinéa 1er, 2°, de la loi NIS2, l'évaluation périodique de la conformité par le service d'inspection de l'autorité nationale de cybersécurité est effectuée au maximum une fois par an.

HOOFDSTUK 5 — *Modaliteiten van de regelmatige vrijwillige conformiteitsbeoordeling van belangrijke entiteiten door een conformiteitsbeoordelingsinstantie*

Art. 11. § 1. Wanneer belangrijke entiteiten opteren voor een regelmatige conformiteitsbeoordeling op basis van het in artikel 4 bedoelde referentiekader, verkrijgen zij een verificatieverklaring van minstens het niveau belangrijk van voornoemd referentiekader.

§ 2. In het kader van de in paragraaf 1 bedoelde regelmatige vrijwillige conformiteitsbeoordeling verrichten belangrijke entiteiten elk jaar een zelfbeoordeling die wordt geverifieerd door een conformiteitsbeoordelingsinstantie die overeenkomstig hoofdstuk 6 erkend is door de nationale cyberbeveiligingsautoriteit.

De erkende conformiteitsbeoordelingsinstantie bezorgt de betrokken entiteit een verificatieverslag dat al dan niet een verificatieverklaring bevat, overeenkomstig het in artikel 4 bedoelde referentiekader.

Art. 12. In het kader van de conformiteitsbeoordeling op basis van het referentiekader bedoeld in artikel 5, § 1, 2°, verkrijgen belangrijke entiteiten indien gewenst een certificering via een procedure van regelmatige audits uitgevoerd door een conformiteitsbeoordelingsinstantie die overeenkomstig hoofdstuk 6 erkend is door de nationale cyberbeveiligingsautoriteit.

Art. 13. Belangrijke entiteiten die opteren voor de in artikel 41 van de NIS2-wet bedoelde conformiteitsbeoordeling, bezorgen de nationale cyberbeveiligingsautoriteit, ongeacht het gekozen referentiekader, hun conformiteitsattest en de risicoanalyse bedoeld in artikel 30, § 5, eerste lid, van de NIS2-wet op de in artikel 9, eerste lid, bedoelde wijze.

Daartoe krijgen belangrijke entiteiten toegang tot het platform bedoeld in artikel 9, tweede lid.

HOOFDSTUK 6 — *Erkenningsvoorwaarden*

Art. 14. § 1. Onverminderd hoofdstuk 8 erkent de nationale cyberbeveiligingsautoriteit conformiteitsbeoordelingsinstanties die de erkenningsvoorwaarden van dit hoofdstuk naleven:

1° hetzij in het kader van de toepassing van de artikelen 39 en 41 van de NIS2-wet,

2° hetzij in het kader van de conformiteitsbeoordeling op basis van het in artikel 4 bedoelde referentiekader.

§ 2. Wanneer de inspectiedienst van de nationale cyberbeveiligingsautoriteit een inbreuk op de in dit hoofdstuk bedoelde erkenningsvoorwaarden vaststelt, kan deze inspectiedienst, via de procedure bedoeld in afdeling 1 van hoofdstuk 2 van titel 4 van de NIS2-wet, de conformiteitsbeoordelingsinstantie aanmanen om een einde te maken aan de inbreuk. Zo niet kan de nationale cyberbeveiligingsautoriteit de in paragraaf 1 bedoelde erkenning opschorten of intrekken.

Art. 15. § 1. Om te worden erkend, moet de conformiteitsbeoordelingsinstantie vooraf beschikken over een accreditatie van een nationale accreditatie-instantie voor het uitvoeren van de certificering en/of van de verificatie als conformiteitsbeoordelingsactiviteiten voor een of meer van de referentiekaders bedoeld in artikel 5, § 1, 1° en/of 2°. De erkenning is beperkt tot de referentiekaders waarvoor de conformiteitsbeoordelingsinstantie geaccrediteerd is.

§ 2. Wanneer er sprake is van een belangenconflict tussen de conformiteitsbeoordelingsinstantie of haar uitvoeringsinstanties en een entiteit waarvoor de verplichtingen van de NIS2-wet gelden, kan voor die entiteit geen erkenning worden verleend.

Om de in het eerste lid bedoelde situaties op te sporen, maakt de nationale cyberbeveiligingsautoriteit de toekenning van de erkenning afhankelijk van het verstrekken van alle nodige informatie.

Indien de in het eerste lid bedoelde situatie zich voordoet na de toekenning van de erkenning, moet de conformiteitsbeoordelingsinstantie de nationale cyberbeveiligingsautoriteit zo snel mogelijk op de hoogte brengen en afzien van de beoordeling van de betrokken entiteiten.

CHAPITRE 5 — *Modalités de l'évaluation périodique volontaire de la conformité des entités importantes par un organisme d'évaluation de la conformité*

Art. 11. § 1er. Lorsque les entités importantes choisissent de réaliser une évaluation périodique de la conformité sur base du cadre de référence visé à l'article 4, elles obtiennent un avis de vérification au moins au niveau important du cadre de référence précité.

§ 2. Dans le cadre de l'évaluation périodique volontaire de la conformité visée au paragraphe 1er, les entités importantes réalisent chaque année une auto-évaluation qui est vérifiée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité conformément au chapitre 6.

L'organisme d'évaluation de la conformité agréé délivre à l'entité concernée un rapport de vérification portant un avis de vérification, ou non, conformément au cadre de référence visé à l'article 4.

Art. 12. Dans le cadre de l'évaluation de la conformité effectuée sur base du cadre de référence visé à l'article 5, § 1er, 2°, les entités importantes qui le désirent obtiennent une certification au travers d'une procédure d'audits réguliers effectués par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité conformément au chapitre 6.

Art. 13. Les entités importantes qui choisissent d'effectuer l'évaluation de la conformité visée à l'article 41 de la loi NIS2, quel que soit le cadre de référence choisi, communiquent leur attestation de conformité ainsi que l'analyse des risques visée à l'article 30, § 5, alinéa 1er, de la loi NIS2, à l'autorité nationale de cybersécurité, de la manière visée à l'article 9, alinéa 1er.

A cette fin, les entités importantes ont accès à la plateforme visée à l'article 9, alinéa 2.

CHAPITRE 6 — *Conditions d'agrément*

Art. 14. § 1er. Sans préjudice du chapitre 8, l'autorité nationale de cybersécurité agrée les organismes d'évaluation de la conformité qui respectent les conditions d'agréation du présent chapitre :

1° soit dans le cadre de l'application des articles 39 et 41 de la loi NIS2,

2° soit dans le cadre de l'évaluation de la conformité sur base du référentiel visé à l'article 4.

§ 2. Lorsque le service d'inspection de l'autorité nationale de cybersécurité constate une violation des conditions d'agrément visées au présent chapitre, ce service d'inspection peut, au travers de la procédure visée à la section 1re du chapitre 2 du titre 4 de la loi NIS2, mettre en demeure l'organisme d'évaluation de la conformité de mettre fin à la violation, faute de quoi l'autorité nationale de cybersécurité peut suspendre ou retirer l'agrément visé au paragraphe 1er.

Art. 15. § 1er. Pour être agréé, l'organisme d'évaluation de la conformité doit disposer au préalable d'une accréditation délivrée par un organisme national d'accréditation pour réaliser la certification et/ou la vérification en tant qu'activités d'évaluation de la conformité d'un ou plusieurs cadres de référence visés à l'article 5, § 1er, 1° et/ou 2°. L'agrément se limite aux cadres de référence pour lesquels l'organisme d'évaluation de la conformité est accrédité.

§ 2. Lorsqu'il existe un conflit d'intérêts entre l'organisme d'évaluation de la conformité ou ses agents d'exécution et une entité soumise aux obligations de la loi NIS2, l'agrément ne peut valoir pour cette entité.

Afin de détecter les situations visées à l'alinéa 1er, l'autorité nationale de cybersécurité conditionne l'octroi de l'agrément à la fourniture de toutes les informations nécessaires.

Si la situation visée à l'alinéa 1er apparaît après l'octroi de l'agrément, l'organisme d'évaluation de la conformité doit en informer dans les plus brefs délais l'autorité nationale de cybersécurité et s'abstenir de participer à l'évaluation des entités concernées.

§ 3. Erkende conformiteitsbeoordelingsinstanties moeten de nationale cyberbeveiligingsautoriteit jaarlijks een verslag bezorgen volgens de modaliteiten bepaald door deze autoriteit. Dit verslag bevat minstens de volgende gegevens over entiteiten die tot het toepassingsgebied van de NIS2-wet behoren:

1° een lijst van de uitgereikte conformiteitsattesten;

2° een lijst van de geweigerde en geschorste conformiteitsattesten;

3° een lijst van de ontvangen klachten en van het gevolg dat hieraan werd gegeven.

De conformiteitsbeoordelingsinstantie wordt geacht op elk ogenblik samen te werken met de nationale cyberbeveiligingsautoriteit, onder meer door haar verzoeken om informatie te beantwoorden.

HOOFDSTUK 7 — *Bepalingen betreffende de inspectiedienst*

Art. 16. § 1. De beëdigde leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit beschikken over een legitimatiekaart waarvan het model in bijlage is opgenomen.

§ 2. De in paragraaf 1 bedoelde legitimatiekaart is rechthoekig, 85,6 mm lang en 53,98 mm breed, en geplastificeerd.

HOOFDSTUK 8 — *Conformiteitsbeoordelingsinstantie voor de federale overheidssector*

Art. 17. De Federale Interneauditdienst, opgericht bij artikel 3 van het koninklijk besluit van 4 mei 2016 tot oprichting van de Federale Interneauditdienst, wordt aangewezen als conformiteitsbeoordelingsinstantie voor de instanties bedoeld in artikel 1 van dat besluit, wat het in artikel 5, § 1, 1°, bedoelde referentiekader betreft.

Art. 18. De nationale cyberbeveiligingsautoriteit erkent de als conformiteitsbeoordelingsinstantie aangewezen autoriteit wanneer zij de erkenningsvoorwaarden van dit hoofdstuk naleeft, evenals de artikelen 14, § 2, en 15, § 3.

Art. 19. Om te worden erkend en regelmatige conformiteitsbeoordelingen te kunnen verrichten op basis van het in artikel 5, § 1, 1°, bedoelde referentiekader, moet een als conformiteitsbeoordelingsinstantie aangewezen autoriteit over de technische bekwaamheid beschikken voor het uitvoeren van certificeringsaudits en verificaties in het kader van de conformiteitsbeoordeling.

HOOFDSTUK 9 — *Retributies voor regelmatige conformiteitsbeoordelingen uitgevoerd door de inspectiedienst*

Art. 20. § 1. Er is voorzien in een retributie voor inspectieprestaties die de essentiële entiteit gekozen heeft in het kader van artikel 39, eerste lid, 2°, van de NIS2-wet.

Deze retributie wordt bepaald op basis van de duur van de in uren berekende prestaties en vermenigvuldigd met het in paragraaf 2, tweede lid, bedoelde uurtarief.

§ 2. De duur van de prestaties wordt bepaald door de methodologie van het in artikel 5 bedoelde referentiekader.

Het uurtarief bedraagt 150 euro.

§ 3. De in dit artikel bedoelde bedragen zijn gekoppeld aan het indexcijfer van de consumptieprijzen van november 2023 en worden jaarlijks op 1 januari aangepast aan de schommelingen van dit indexcijfer.

§ 4. Retributies worden gedetailleerd gefactureerd.

Gefactureerde bedragen moeten uiterlijk op de laatste dag van de maand na de factuurdatum worden betaald. Als dit niet gebeurt, wordt een herinnering gestuurd naar de betrokken entiteit.

Bij niet-betaling binnen twee maanden na de herinnering wordt een aangetekende ingebrekestelling verstuurd naar de betrokken entiteit.

§ 5. De in paragraaf 1 bedoelde retributie is niet van toepassing op entiteiten die deel uitmaken van de overheidssector bedoeld in bijlage I van de NIS2-wet, voor zover deze niet zijn vermeld in artikel 1 van het koninklijk besluit van 4 mei 2016 tot oprichting van de Federale Interneauditdienst.

HOOFDSTUK 10 — *Opheffings- en slotbepalingen*

Art. 21. 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 de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren wordt opgeheven, met uitzondering van artikel 4, bijlage I, punt *c)*, en bijlage II, punt *a)*, van voornoemd koninklijk besluit waarvan de draagwijdte beperkt is tot de uitvoering van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

§ 3. Les organismes d'évaluation de la conformité agréés fournissent chaque année à l'autorité nationale de cybersécurité, selon les modalités fixées par cette autorité, un rapport contenant au minimum les données suivantes en ce qui concerne les entités qui relèvent du champ d'application de la loi NIS2 :

1° une liste des attestations de conformité délivrées;

2° une liste des attestations de conformité refusées ou suspendues;

3° une liste des plaintes reçues et des suites données à celles-ci.

L'organisme d'évaluation de la conformité collabore à tout moment avec l'autorité nationale de cybersécurité, notamment en répondant à ses demandes d'information.

CHAPITRE 7 — *Dispositions relatives au service d'inspection*

Art. 16. § 1er. Les membres assermentés du service d'inspection de l'autorité nationale de cybersécurité sont dotés d'une carte de légitimation dont le modèle est repris à l'annexe.

§ 2. La carte de légitimation visée au paragraphe 1er a une forme rectangle de 85,6 mm de longueur et 53,98 mm de largeur et est plastifiée.

CHAPITRE 8 — *Organisme d'évaluation de la conformité du secteur public fédéral*

Art. 17. Le Service fédéral d'audit interne, créé par l'article 3 de l'arrêté royal du 4 mai 2016 portant création du Service fédéral d'audit interne, est désigné comme organisme d'évaluation de la conformité des entités visées à l'article 1er dudit arrêté, pour le cadre de référence visé à l'article 5, § 1er, 1°.

Art. 18. L'autorité nationale de cybersécurité agrée l'autorité désignée comme organisme d'évaluation de la conformité lorsqu'elle respecte les conditions d'agrément du présent chapitre ainsi que les articles 14, § 2 et 15, § 3.

Art. 19. Pour être agréée et effectuer les évaluations périodiques de la conformité sur base du cadre de référence visé à l'article 5, § 1er, 1°, une autorité désignée comme organisme d'évaluation de la conformité doit disposer des capacités techniques pour effectuer les audits de certification et les vérifications dans le cadre de l'évaluation de la conformité.

CHAPITRE 9 — *Rétributions relatives aux évaluations périodiques de la conformité effectuées par le service d'inspection*

Art. 20. § 1er. Une rétribution est prévue pour les prestations d'inspection choisies par l'entité essentielle dans le cadre de l'article 39, alinéa 1er, 2°, de la loi NIS2.

Cette rétribution est déterminée sur base de la durée des prestations calculées en heures, multipliée par le taux horaire visé au paragraphe 2, alinéa 2.

§ 2. La durée des prestations est fixée par la méthodologie du cadre de référence visé à l'article 5.

Le taux horaire est fixé à 150 euro.

§ 3. Les montants visés au présent article sont rattachés à l'indice des prix à la consommation de novembre 2023 et sont adaptés annuellement le 1er janvier en fonction des fluctuations de cet indice.

§ 4. Les rétributions font l'objet d'une facturation détaillée.

Les montants facturés doivent être versés au plus tard le dernier jour du mois qui suit la date de la facture. A défaut, un rappel est adressé à l'entité concernée.

En cas de non-paiement dans les deux mois suivant le rappel, une mise en demeure est adressée par recommandé à l'entité concernée.

§ 5. La rétribution visée au paragraphe 1er n'est pas applicable pour les entités faisant partie du secteur de l'administration publique visées à l'annexe I de la loi NIS2, pour autant qu'elles ne soient pas visées à l'article 1er de l'arrêté royal du 4 mai 2016 portant création du Service fédéral d'audit interne.

CHAPITRE 10 — *Dispositions abrogatoires et finales*

Art. 21. 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 est abrogé, à l'exception de l'article 4, de l'annexe I, point *c)*, et de l'annexe II, point *a)*, de l'arrêté royal précité, dont la portée est réduite à l'exécution de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

Art. 22. § 1. Indien essentiële entiteiten opteren voor de certificering op basis van een van de in artikel 5 bedoelde referentiekaders, moeten zij binnen 18 maanden na de inwerkingtreding van de NIS2-wet of na de datum van de identificatie bedoeld in artikel 11 van de NIS2-wet, minstens voldoen aan de volgende verplichtingen:

1° een verificatie verkrijgen die uitgevoerd wordt door een conformiteitsbeoordelingsinstantie die overeenkomstig hoofdstuk 6 erkend is door de nationale cyberbeveiligingsautoriteit, voor het niveau basis of belangrijk van het in artikel 4 bedoelde referentiekader, naargelang het resultaat van hun risicoanalyse bedoeld in artikel 30, § 5, eerste lid, van de NIS2-wet, indien de entiteit opteert voor het in artikel 4 bedoelde referentiekader; of

2° het toepassingsgebied en de toepasselijkheidsverklaring bezorgen indien de entiteit opteert voor het referentiekader bedoeld in artikel 5, paragraaf 1, 2°.

§ 2. Indien essentiële entiteiten opteren voor de certificering op basis van een van de in artikel 5 bedoelde referentiekaders, verkrijgen zij binnen 30 maanden na de inwerkingtreding van de NIS2-wet of na de datum van de identificatie bedoeld in artikel 11 van de NIS2-wet en naargelang de keuze gemaakt overeenkomstig § 1:

1° een certificering overeenkomstig artikel 6, onverminderd artikel 7; of

2° een certificering overeenkomstig artikel 8.

Art. 23. § 1. Indien essentiële entiteiten opteren voor toezicht door een inspectiedienst bedoeld in artikel 39, eerste lid, 2°, van de NIS2-wet op basis van een van de in artikel 5 bedoelde referentiekaders, moeten zij binnen 18 maanden na de inwerkingtreding van de NIS2-wet of na de datum van de identificatie bedoeld in artikel 11 van de NIS2-wet, minstens voldoen aan de volgende verplichtingen:

1° een zelfbeoordeling van niveau "basis" of "belangrijk" bezorgen indien zij opteren voor het referentiekader bedoeld in artikel 4;

2° het I.B.B., het toepassingsgebied en de toepasselijkheidsverklaring bezorgen, indien zij opteren voor het referentiekader bedoeld in artikel 5, paragraaf 1, 2°.

§ 2. Indien essentiële entiteiten opteren voor toezicht door een inspectiedienst bedoeld in artikel 39, eerste lid, 2°, van de NIS2-wet op basis van een van de in artikel 5 bedoelde referentiekaders, bezorgen zij een stand van zaken van de voortgang van het conformiteitsproces binnen 30 maanden na de inwerkingtreding van de NIS2-wet of na de datum van de identificatie bedoeld in artikel 11 van de NIS2-wet en naargelang de keuze die overeenkomstig § 1 is gemaakt.

§ 3. Ongeacht de gemaakte keuze moeten essentiële en belangrijke entiteiten een continue verbetering aantonen.

Art. 24. De Eerste Minister en de Minister bevoegd voor Binnenlandse Zaken zijn, ieder wat hem of haar betreft, belast met de uitvoering van dit besluit.

Gegeven te Brussel, 9 juni 2024.

FILIP

Van Koningswege :

De Eerste Minister,
A. DE CROO

De Minister van Binnenlandse Zaken,
A. VERLINDEN

Bijlage

Bijlage bij het koninklijk besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Bijlage – Legitimatiekaart

Art. 22. § 1er. Lorsque les entités essentielles font le choix de la certification sur base de l'un des cadres de référence visés à l'article 5, elles doivent au minimum, dans les 18 mois après l'entrée en vigueur de la loi NIS2 ou la date de l'identification visée à l'article 11 de la loi NIS2, remplir les obligations suivantes :

1° obtenir une vérification, effectuée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité conformément au chapitre 6, au niveau basique ou important du cadre de référence visé à l'article 4, selon le résultat de leur analyse des risques visée à l'article 30, § 5, alinéa 1er, de la loi NIS2 lorsque l'entité choisit le cadre de référence visé à l'article 4; ou

2° transmettre le champ d'application et la déclaration d'applicabilité lorsque l'entité choisit le cadre de référence visé à l'article 5, paragraphe 1, 2°.

§ 2. Lorsque les entités essentielles font le choix de la certification sur base de l'un des cadres de référence visés à l'article 5, dans les 30 mois suivant l'entrée en vigueur de la loi NIS2 ou la date de l'identification visée à l'article 11 de la loi NIS2 et selon le choix effectué conformément au § 1er, les entités essentielles :

1° obtiennent une certification conformément à l'article 6, sans préjudice de l'article 7; ou

2° obtiennent une certification conformément à l'article 8.

Art. 23. § 1er. Lorsque les entités essentielles font le choix de la supervision par un service d'inspection visée à l'article 39, alinéa 1er, 2° de la loi NIS2 sur base de l'un des cadres de référence visés à l'article 5, elles doivent au minimum, dans les 18 mois après l'entrée en vigueur de la loi NIS2 ou la date de l'identification visée à l'article 11 de la loi NIS2, remplir les obligations suivantes :

1° transmettre une auto-évaluation du niveau basique ou important lorsqu'elles choisissent le cadre de référence visé à l'article 4;

2° transmettre la P.S.I., le champ d'application et la déclaration d'applicabilité, lorsqu'elles choisissent le cadre de référence visé à l'article 5, paragraphe 1er, 2°.

§ 2. Lorsque les entités essentielles font le choix de la supervision par un service d'inspection visée à l'article 39, alinéa 1er, 2° de la loi NIS2 sur base de l'un des cadres de référence visés à l'article 5, dans les 30 mois suivant l'entrée en vigueur de la loi NIS2 ou la date de l'identification visée à l'article 11 de la loi NIS2 et selon le choix effectué conformément au § 1er, elles transmettent une état de l'avancement de la mise en conformité.

§ 3. Quel que soit le choix effectué, les entités essentielles et les entités importantes démontrent une amélioration continue.

Art. 24. Le Premier Ministre et le Ministre qui a l'Intérieur dans ses attributions sont chargés, chacun en ce qui les concerne, de l'exécution du présent arrêté.

Donné à Bruxelles, le 9 juin 2024.

PHILIPPE

Par le Roi :

Le Premier Ministre,
A. DE CROO

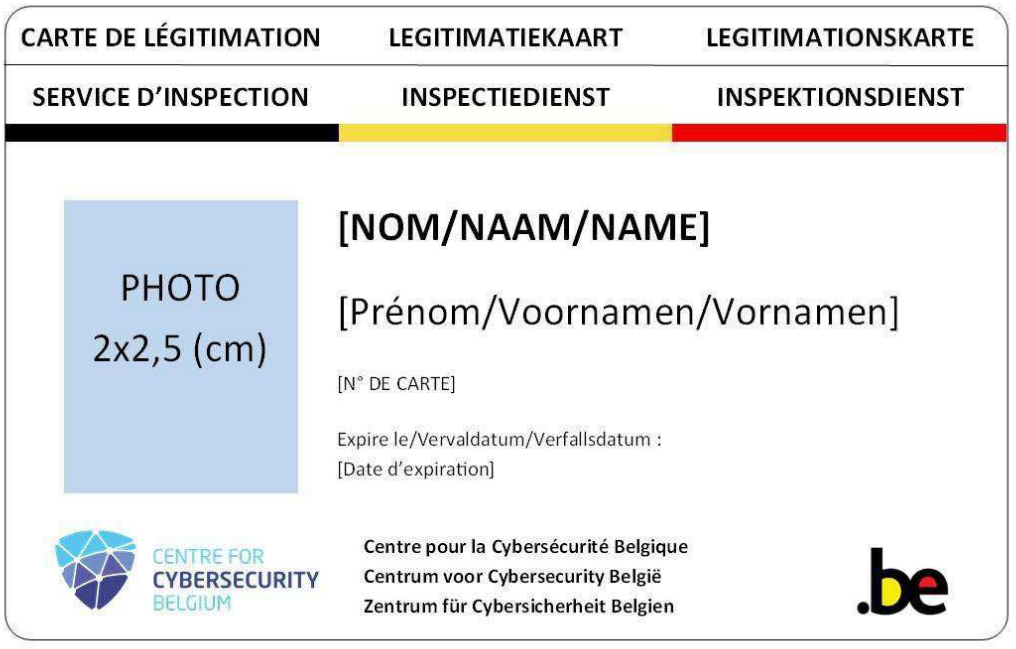
La Ministre de l'Intérieur,
A. VERLINDEN

Annexe

Annexe à l'arrêté royal du 9 juin 2024 exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Annexe – Carte de légitimation

Recto Voorzijde



Verso Achterzijde

Gezien om te worden gevoegd bij Ons besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

FILIP

Van Koningswege :

De Eerste Minister,
A. DE CROO

De Minister van Binnenlandse Zaken,
A. VERLINDEN

Vu pour être annexé à Notre arrêté du 9 juin 2024 exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

PHILIPPE

Par le Roi :

Le Premier Ministre,
A. DE CROO

La Ministre de l'Intérieur,
A. VERLINDEN