

Avant-projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité

CHAPITRE 1^{er}. - Définitions et dispositions générales

Section 1^{re}. - Objet et champ d'application

Sous-section 1^{re}. - Objet

Art. 1^{er}. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. La présente loi met en œuvre partiellement le Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013.

Sous-section 2. - Champ d'application

Art. 3. § 1^{er}. La présente loi s'applique à la certification européenne volontaire de cybersécurité des produits TIC, services TIC et processus TIC visée par le Règlement sur la cybersécurité.

§ 2. Les chapitres 1 à 4 et 7, ainsi que les articles 21 et 22, s'appliquent également à une certification européenne de cybersécurité rendue obligatoire.

Lors de la mise en œuvre des articles 21 et 22 dans le cadre d'une telle certification, les articles 19 et 26 sont applicables.

Le Roi peut, par arrêté délibéré en Conseil des Ministres, rendre applicables, en tout ou en partie, les chapitres 5 et 6 dans le cadre d'une telle certification.

§ 3. La présente loi ne porte pas préjudice aux mesures adoptées en droit belge pour protéger la sécurité publique, la défense, la sécurité nationale et les activités dans le domaine du droit pénal.

§ 4. La présente loi est sans préjudice des compétences de rendre obligatoire une certification de cybersécurité et d'en assurer le contrôle dont disposent les autorités publiques, notamment les autorités de surveillance de marché ou les autorités sectorielles au sens de l'article 6, § 1^{er} 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 (« loi NIS »), de l'article 3, 3^e la loi du 1^{er} juillet 2011 relative à la protection et la sécurité des infrastructures critiques et de l'article 2, 1^o de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

Dans le respect des dispositions légales applicables et du paragraphe 2, les autorités précitées et les services

Voorontwerp van wet inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit

HOOFDSTUK 1. - Definities en algemene bepalingen

Afdeling 1. - Onderwerp en toepassingsgebied

Onderafdeling 1. - Onderwerp

Art. 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2. Deze wet geeft gedeeltelijk uitvoering aan Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013.

Onderafdeling 2. – Toepassingsgebied

Art. 3. § 1. Deze wet is van toepassing op de vrijwillige Europese certificering van de cyberbeveiliging van ICT-producten, -diensten en -processen zoals bedoeld in de Cyberbeveiligingsverordening.

§ 2. De hoofdstukken 1 tot 4 en 7, alsook de artikelen 21 en 22, zijn ook van toepassing op een Europese cyberbeveiligingscertificering die wordt opgelegd.

Bij de uitvoering van artikel 21 en 22 in het kader van een dergelijke certificering zijn artikel 19 en 26 van toepassing.

De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, de hoofdstuk 5 en 6 volledig of gedeeltelijk toepasselijk maken in het kader van deze certificering.

§ 3. Deze wet doet geen afbreuk aan de maatregelen die in het Belgisch recht worden genomen ter bescherming van de openbare veiligheid, defensie, de nationale veiligheid en de activiteiten op het gebied van het strafrecht.

§ 4. Deze wet doet geen afbreuk aan de bevoegdheden om een cyberbeveiligingscertificering op te leggen en er toezicht op uit te oefenen waarover de overheden beschikken, met name de markttoezichtautoriteiten of de sectorale overheden als bedoeld in artikel 6, § 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 ("NIS-wet"), in artikel 3, 3^e, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur en in artikel 2, 1^o, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuur in de deelsector van het luchtvervoer.

d'inspection compétents assurent le contrôle et les sanctions des certifications européennes de cybersécurité rendues obligatoires.

§ 5. L'article 5, §§ 2 à 4 n'est applicable ni à la Banque nationale de Belgique visée par la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique ni à la FSMA visée par la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ni au SPF Economie visé au Code de droit économique.

Section 2. – Définitions

Art. 4. Pour l'application de la présente loi, il faut entendre par :

1° "Règlement sur la cybersécurité" : le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 ;

2° "autorité nationale de certification de cybersécurité" : l'autorité visée à l'article 58 du Règlement sur la cybersécurité et désignée par le Roi conformément à l'article 5, § 1^{er} ;

3° "GECC" : Groupe européen de certification de cybersécurité visé à l'article 62 du Règlement sur la cybersécurité ;

4° "autorité nationale d'accréditation" : l'organisme créé par le Roi en exécution de l'article VIII.30 du Code de droit économique et visée à l'article 2, 16° du Règlement sur la cybersécurité ;

5° "autorité publique" : l'autorité publique au sens de l'article 5 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

6° "service d'inspection" : le service d'inspection visé à l'article 13, § 1^{er}.

CHAPITRE 2. - Autorités compétentes et coopération au niveau national

Section 1^{re}. Autorités compétentes

Art. 5. § 1^{er}. Le Roi désigne l'autorité qui est chargée, en tant qu'autorité nationale de certification de cybersécurité, des tâches et missions visées par le Règlement sur la cybersécurité et par la présente loi.

§ 2. En fonction de l'objet du schéma de certification concerné et à la demande de l'autorité publique concernée, le Roi peut, par dérogation, confier, par arrêté délibéré en

Met inachtneming van de toepasselijke wettelijke bepalingen en van paragraaf 2 zorgen de voornoemde overheden en de bevoegde inspectiediensten voor het toezicht op en de sancties met betrekking tot verplichte Europese cyberbeveiligingscertificeringen.

§ 5. Artikel 5, §§ 2 tot 4, zijn niet van toepassing op de Nationale Bank van België bedoeld in de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, noch op de FSMA bedoeld in de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten noch op de FOD Economie bedoeld in het Wetboek van Economisch recht.

Afdeling 2. – Definities

Art. 4. Voor de toepassing van deze wet moet worden verstaan onder:

1° "Cyberbeveiligingsverordening": verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013;

2° "nationale cyberbeveiligingscertificeringsautoriteit": de overheid bedoeld in artikel 58 van de Cyberbeveiligingsverordening en aangewezen door de Koning overeenkomstig artikel 5, § 1;

3° "EGC": Europese Groep voor cyberbeveiligingscertificering bedoeld in artikel 62 van de Cyberbeveiligingsverordening;

4° "nationale accrediteringsautoriteit": instelling die door de Koning is opgericht in uitvoering van artikel VIII.30 van het Wetboek van economisch recht;

5° "overheid": de overheid als bedoeld in artikel 5 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

6° "inspectiedienst": de inspectiedienst bedoeld in artikel 13, § 1.

HOOFDSTUK 2. - Bevoegde autoriteiten en samenwerking op nationaal niveau

Afdeling 1. Bevoegde autoriteiten

Art. 5. § 1. De Koning wijst de autoriteit aan die, als nationale cyberbeveiligingscertificeringsautoriteit, belast is met de taken en opdrachten bedoeld in de Cyberbeveiligingsverordening en in deze wet.

§ 2. Naargelang het voorwerp van de betrokken certificeringsregeling en op verzoek van de betrokken overheid kan de Koning, bij wijze van afwijking en bij besluit

Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6 de l'autorité visée à l'article 5, § 1^{er} à une autre autorité publique, à l'exception des articles 21 et 22.

Le Roi veille à tenir compte de l'expertise de l'autorité publique concernée lors de l'attribution éventuelle de tâches de contrôle.

§ 3. Dans l'hypothèse visée au paragraphe 2, le Roi sollicite l'avis et se consulte au préalable avec l'autorité visée à l'article 5, § 1^{er} et l'autorité publique concernée.

§ 4. Dans l'exercice de ces missions confiées par le Roi et sans préjudice de ses compétences légales en matière de contrôle et de sanctions, l'autorité publique concernée dispose des mêmes droits et obligations que ceux visés aux chapitres 5 et 6.

Section 2. - Coopération au niveau national

Art. 6. § 1^{er}. L'autorité visée à l'article 5, § 1^{er} et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 accomplissent leurs tâches en concertation avec les autorités publiques. En fonction de l'objet précis du schéma de certification, l'autorité visée à l'article 5, § 1^{er} et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 peuvent également consulter les acteurs privés concernés par la certification en matière de cybersécurité.

§ 2. Les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne communiquent à l'autorité visée à l'article 5, § 1^{er} ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2 toute information dont elle a besoin pour l'exécution de ses tâches.

§ 3. L'autorité visée à l'article 5, § 1^{er} et les autorités publiques visées au paragraphe 1^{er} s'échangent les informations nécessaires à l'application du Règlement sur la cybersécurité, de la présente loi ou d'autres dispositions légales, notamment en matière de délivrance de certificat, de contrôle, de sanction et de réclamation. Les informations échangées se limitent à ce qui est pertinent et proportionnée à l'objectif de cet échange, notamment dans le respect du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Les modalités d'échange d'informations préservent la confidentialité des informations concernées.

§ 4. Les personnes dépositaires, par état ou par profession, des secrets ou informations confidentielles qu'on leur confie sont autorisées à faire connaître ces secrets ou ces

constatés na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6 van de autoriteit bedoeld in artikel 5, § 1, volledig of gedeeltelijk toevertrouwen aan een andere overheid, met uitzondering van artikel 21 en 22.

De Koning houdt rekening met de expertise van de betrokken overheid bij de eventuele toekenning van toezichtstaken.

§ 3. In het in paragraaf 2 bedoelde geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, en de betrokken overheid.

§ 4. Bij de uitoefening van deze door de Koning toevertrouwde opdrachten en onverminderd haar wettelijke toezichts- en sanctiebevoegdheden beschikt de betrokken overheid over dezelfde rechten en verplichtingen als die bedoeld in hoofdstuk 5 en 6.

Afdeling 2. - Samenwerking op nationaal niveau

Art. 6. § 1. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, voeren hun taken uit in overleg met de overheden. Naargelang het specifieke voorwerp van de certificeringsregeling kunnen de autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, ook de private actoren raadplegen die betrokken zijn bij de cyberbeveiligingscertificering.

§ 2. Conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen verstrekken de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, alle informatie die zij nodig heeft voor de uitvoering van haar taken.

§ 3. De autoriteit bedoeld in artikel 5, § 1, en de overheden bedoeld in paragraaf 1 wisselen onderling de informatie uit die nodig is voor de toepassing van de Cyberbeveiligingsverordening, van deze wet of van andere wettelijke bepalingen, met name wat betreft de afgifte van certificaten, het toezicht, sancties en klachten. De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van deze uitwisseling, met name overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad 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 en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). De modaliteiten van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.

§ 4. Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen of vertrouwelijke informatie die hun zijn toevertrouwd, mogen deze geheimen of vertrouwelijke informatie bekendmaken aan de autoriteit bedoeld in artikel

informations confidentielles à l'autorité visée à l'article 5, § 1^{er}, ainsi qu'éventuellement à d'autres autorités publiques lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.

Il s'agit notamment des informations nécessaires en matière de délivrance de certificat, de contrôle, de sanction et de réclamation. Les informations échangées se limitent à ce qui est pertinent et proportionnée à l'objectif de cet échange, notamment dans le respect du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Les modalités d'échange d'informations préservent la confidentialité des informations concernées.

Art. 7. Dans le cadre des missions et pouvoirs qui leur sont attribués par la loi, les autorités publiques peuvent assister l'autorité visée à l'article 5, § 1^{er} dans ses missions de contrôle visées par la présente loi.

CHAPITRE 3. - Autorité nationale de certification de cybersécurité

Section 1^{re}. - Représentation au Groupe européen de certification de cybersécurité

Art. 8. § 1^{er}. L'autorité visée à l'article 5, § 1^{er} représente la Belgique au sein du GECC.

§ 2. Dans le cadre de sa mission de représentation de la Belgique au sein du GECC, l'autorité visée à l'article 5, § 1^{er} se concerta avec les autres autorités publiques désignées par le Roi, en particulier en ce qui concerne la préparation et l'adoption d'un avis sur un schéma de certification candidat au sens de l'article 49 du Règlement sur la cybersécurité.

§ 3. D'autres autorités publiques peuvent assister avec l'autorité visée à l'article 5, § 1^{er} aux travaux et réunions du GECC.

Section 2. - Indépendance

Art. 9. § 1^{er}. L'autorité visée à l'article 5, § 1^{er} prend les mesures nécessaires afin d'assurer l'indépendance des membres de son personnel, de prévenir, d'identifier et de résoudre efficacement les conflits d'intérêts lors de l'exécution de ses tâches de contrôle ou de certification en matière de cybersécurité, afin d'éviter des distorsions de concurrence et de garantir l'égalité de traitement de tous.

La notion de conflit d'intérêts vise au moins les situations dans lesquelles un membre du personnel de l'autorité visée à l'article 5, § 1^{er} chargé de la certification ou du contrôle a, directement ou indirectement, un intérêt financier, économique ou un autre intérêt personnel qui pourrait être

5, § 1, aussi éventuellement à d'autres autorités publiques lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.

Het gaat met name om noodzakelijke informatie met betrekking tot de afgifte van certificaten, het toezicht, sancties en klachten. De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van deze uitwisseling, met name overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad 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 en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). De modaliteiten van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.

Art. 7. De overheden mogen, in het kader van de opdrachten en bevoegdheden die hun zijn toevertrouwd door de wet, de autoriteit bedoeld in artikel 5, § 1, bijstaan bij de in deze wet bedoelde toezichtsoopdrachten.

HOOFDSTUK 3. - Nationale cyberbeveiligingscertificeringsautoriteit

Afdeling 1. - Vertegenwoordiging in de Europese Groep voor cyberbeveiligingscertificering

Art. 8. § 1. De autoriteit bedoeld in artikel 5, § 1, vertegenwoordigt België in de EGC.

§ 2. In het kader van haar opdracht om België in de EGC te vertegenwoordigen overlegt de autoriteit bedoeld in artikel 5, § 1, met de andere door de Koning aangewezen overheden, met name bij de voorbereiding en goedkeuring van een advies over een potentiële certificeringsregeling als bedoeld in artikel 49 van de Cyberbeveiligingsverordening.

§ 3. Andere overheden kunnen, samen met de autoriteit bedoeld in artikel 5, § 1, de werkzaamheden en vergaderingen van de EGC bijwonen.

Afdeling 2. - Onafhankelijkheid

Art. 9. § 1. De autoriteit bedoeld in artikel 5, § 1, neemt de nodige maatregelen om, bij de uitvoering van haar toezichts- of certificeringstaken op het gebied van cyberbeveiliging, de onafhankelijkheid van haar personeelsleden te garanderen, belangenconflicten doeltreffend te voorkomen, te identificeren en op te lossen, teneinde vertekening van de mededinging te vermijden en de gelijke behandeling van allen te waarborgen.

Het begrip "belangenconflict" heeft minstens betrekking op situaties waarin een met de certificering of het toezicht belast personeelslid van de autoriteit bedoeld in artikel 5, § 1, rechtstreeks of onrechtstreeks financiële, economische of

perçu comme compromettant son impartialité et son indépendance dans le cadre de sa mission ou de ses fonctions.

§ 2. Les membres du personnel de l'autorité visée à l'article 5, § 1^{er} ne reçoivent ni ne cherchent dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne.

Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au troisième degré ont un intérêt personnel ou direct.

Le Roi peut également désigner d'autres situations comme étant des conflits d'intérêts.

CHAPITRE 4. - Délivrance des certificats européens

Section 1^{re}. - Certificats de cybersécurité européens attestant d'un niveau d'assurance "élémentaire" ou "substantiel"

Art. 10. § 1^{er}. Les organismes d'évaluation de la conformité accrédités par l'autorité nationale d'accréditation délivrent les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élémentaire" ou "substantiel".

§ 2. Lorsque le schéma européen de certification de cybersécurité l'impose, la délivrance de tels certificats est réservée à l'autorité visée à l'article 5, § 1^{er}.

§ 3. En fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1^{er} peut néanmoins déléguer en tout ou en partie la délivrance d'un certificat visé au paragraphe 2 à un organisme public accrédité par l'autorité nationale d'accréditation en tant qu'organisme d'évaluation de la conformité.

Section 2. - Certificats de cybersécurité européens attestant d'un niveau d'assurance "élevé"

Art. 11. § 1^{er}. L'autorité visée à l'article 5, § 1^{er} délivre les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élevé".

§ 2. En fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1^{er} peut toutefois déléguer en tout ou en partie cette tâche à un organisme d'évaluation de la conformité accrédité par l'autorité nationale d'accréditation.

Section 3. - Réclamation en cas de refus de délivrance

andere persoonlijke belangen heeft die geacht kunnen worden zijn onpartijdigheid en onafhankelijkheid in het kader van zijn opdracht of functie in het gedrang te brengen.

§ 2. De personeelsleden van de autoriteit bedoeld in artikel 5, § 1, krijgen, noch vragen binnen de grenzen van hun bevoegdheden op directe of indirecte wijze van niemand instructies.

Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarin zij een persoonlijk of rechtstreeks belang hebben of waarin hun bloed- of aanverwanten tot en met de derde graad een persoonlijk of rechtstreeks belang hebben.

De Koning kan ook andere situaties benoemen als belangenconflicten.

HOOFDSTUK 4. - Afgifte van Europese certificaten

Afdeling 1. - Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel"

Art. 10. § 1. De conformiteitsbeoordelingsinstanties die door de nationale accreditatieautoriteit geaccrediteerd zijn, geven de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel" af.

§ 2. Indien vereist door de Europese cyberbeveiligingscertificeringsregeling is de afgifte van deze certificaten voorbehouden aan de autoriteit bedoeld in artikel 5, § 1.

§ 3. Naargelang de technische vereisten van de certificeringsregeling en na voorafgaande delegatie kan de - autoriteit bedoeld in artikel 5, § 1, de afgifte van een certificaat bedoeld in paragraaf 2 niettemin volledig of gedeeltelijk delegeren aan een overheidsinstelling die door de nationale accreditatieautoriteit als conformiteitsbeoordelingsinstantie geaccrediteerd is.

Afdeling 2. - Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog"

Art. 11. § 1. De autoriteit bedoeld in artikel 5, § 1, geeft de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog" af.

§ 2. Naargelang de technische vereisten van de certificeringsregeling en na voorafgaande delegatie kan de - autoriteit bedoeld in artikel 5, § 1, deze taak echter volledig of gedeeltelijk delegeren aan een conformiteitsbeoordelingsinstantie die door de nationale accreditatieautoriteit geaccrediteerd is.

Afdeling 3. - Klacht ingeval de afgifte geweigerd wordt

Art. 12. En cas de refus de délivrance du certificat, le demandeur peut introduire une réclamation devant l'autorité visée à l'article 5, § 1^{er} selon les modalités prévues au chapitre 7.

CHAPITRE 5. - Contrôle

Art. 13. § 1^{er}. L'autorité visée à l'article 5, § 1^{er} dispose d'un service d'inspection qui peut à tout moment réaliser des contrôles du respect par les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens volontaires et les émetteurs de déclarations de conformité de l'Union européenne des règles imposées par le Règlement sur la cybersécurité, les schémas européens de certification de cybersécurité, la présente loi ou ses arrêtés d'exécution.

Dans l'exécution de ses tâches de contrôle, le service d'inspection agit de manière indépendante des autres services de l'autorité visée à l'article 5, § 1^{er}, notamment du service chargé de la délivrance des certificats de cybersécurité.

§ 2. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection mentionne la finalité de la demande et précise le délai dans lequel les informations ou preuves doivent être fournies.

§ 3. En fonction des caractéristiques propres à chaque schéma européen de certification de cybersécurité, le service d'inspection peut faire appel à des experts, lesquels sont soumis aux règles de l'article 17.

Les frais de recours à des experts peuvent être mis à charge des organismes d'évaluation de la conformité, des titulaires de certificat de cybersécurité européen ou des émetteurs de déclaration de conformité de l'Union européenne.

Art. 14. Lorsqu'un organisme d'évaluation de la conformité, un titulaire de certificat de cybersécurité européen volontaire ou un émetteur de déclaration de conformité de l'Union européenne est situé en dehors du territoire belge, le service d'inspection peut solliciter la coopération et l'assistance des autorités nationales de certification de cybersécurité compétentes de ces autres Etats.

Art. 15. § 1^{er}. Les membres assermentés du service d'inspection sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi.

§ 2. Les membres assermentés du service d'inspection ou les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les organismes d'évaluation de la conformité, titulaires de certificat de cybersécurité européen ou émetteurs de déclaration de conformité de l'Union européenne qu'ils sont chargés de contrôler, susceptible de compromettre leur

Art. 12. Ingeval de afgifte van een certificaat geweigerd wordt, kan de aanvrager een klacht indienen bij de autoriteit bedoeld in artikel 5, § 1, volgens de in hoofdstuk 7 bepaalde modaliteiten.

HOOFDSTUK 5. - Toezicht

Art. 13. § 1. De autoriteit bedoeld in artikel 5, § 1, beschikt over een inspectiedienst die op elk ogenblik controles kan uitvoeren om na te gaan of de conformiteitsbeoordelingsinstanties, de houders van vrijwillige Europese cyberbeveiligingscertificaten en de afgevers van EU-conformiteitsverklaringen de regels naleven die zijn opgelegd door de Cyberbeveiligingsverordening, de Europese cyberbeveiligingscertificeringsregelingen, deze wet of de uitvoeringsbesluiten ervan.

Bij de uitvoering van zijn toezichtstaken handelt de inspectiedienst onafhankelijk van de andere diensten van de autoriteit bedoeld in artikel 5, § 1, met name van de dienst belast met de afgifte van cyberbeveiligingscertificaten.

§ 2. Bij het formuleren van een verzoek om informatie of bewijzen vermeldt de inspectiedienst het doel van het verzoek en de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt.

§ 3. Naargelang de specifieke kenmerken van elke Europese cyberbeveiligingscertificeringsregeling kan de inspectiedienst een beroep doen op experts, die onderworpen zijn aan de regels van artikel 17.

De kosten om een beroep te doen op experts kunnen ten laste worden gelegd van de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen.

Art. 14. Wanneer een conformiteitsbeoordelingsinstantie, een houder van een vrijwillig Europees cyberbeveiligingscertificaat of een afgever van een EU-conformiteitsverklaring zich buiten het Belgische grondgebied bevindt, kan de inspectiedienst de bevoegde nationale cyberbeveiligingscertificeringsautoriteiten van deze andere landen om samenwerking en bijstand verzoeken.

Art. 15. § 1. De beëdigde leden van de inspectiedienst beschikken over een legitimatiekaart waarvan het model door de Koning wordt bepaald.

§ 2. De beëdigde leden van de inspectiedienst of de experts die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou

objectivité. Ils prêtent serment auprès du fonctionnaire dirigeant de leur service.

§ 3. Sans préjudice des attributions des officiers de police judiciaire visées à l'article 8 du Code d'instruction criminelle, les membres assermentés du service d'inspection disposent, à tout moment, des compétences de contrôle suivantes dans l'exercice de leur mission :

1° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen ou l'émetteur de déclaration de conformité de l'Union européenne; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction;

2° prendre connaissance sur place et obtenir une copie du certificat ou de la déclaration de conformité de l'Union européenne, ainsi que de tout acte, tout document et toute autre source d'informations nécessaires à l'exercice de leur mission;

3° procéder à tout examen, contrôle et audition, et requérir toutes les informations qu'ils estiment nécessaires à l'exercice de leur mission;

4° relever et vérifier l'identité des personnes qui se trouvent sur les lieux utilisés par l'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen ou l'émetteur de déclaration de conformité de l'Union européenne et dont ils estiment l'audition nécessaire pour l'exercice de leur mission. A cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification;

5° requérir l'assistance des services de la police fédérale ou locale.

§ 4. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du personnel du service d'inspection adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes :

1° l'identification des espaces habités auxquels les membres du personnel du service d'inspection souhaitent avoir accès;

2° les infractions présumées qui font l'objet du contrôle;

3° la législation qui donne lieu au contrôle pour lequel les inspecteurs estiment nécessaire d'obtenir une autorisation de visite;

4° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire;

5° la proportionnalité et la subsidiarité à l'égard de tout autre devoir d'enquête.

Le juge d'instruction décide dans un délai de 48 heures maximum après réception de la demande. La décision du juge d'instruction est motivée. En l'absence de décision dans

un délai de 48 heures, la demande est considérée comme rejetée. Ze leggen de eed af bij de leidend ambtenaar van hun dienst.

§ 3. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de inspectiedienst op elk ogenblik over de volgende toezichtbevoegdheden bij de uitoefening van hun opdracht:

1° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle plaatsen betreden die de conformiteitsbeoordelingsinstantie, de houder van een Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring gebruikt; zij hebben slechts toegang tot bewoonde lokalen mits vooraf een machtiging is uitgereikt door de onderzoeksrechter;

2° ter plaatse kennisnemen van het certificaat of de EU-conformiteitsverklaring, alsook van alle bescheiden, documenten en andere informatiebronnen die nodig zijn voor de uitoefening van hun opdracht en hiervan een kopie verkrijgen;

3° overgaan tot elk onderzoek, elke controle en elk verhoor, alsook alle inlichtingen inwinnen die zij nodig achten voor de uitoefening van hun opdracht;

4° de identiteit opnemen en controleren van de personen die zich bevinden op de plaatsen die de conformiteitsbeoordelingsinstantie, de houder van een Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring gebruikt en van wie ze het verhoor nodig achten voor de uitoefening van hun opdracht. Daartoe kunnen ze van deze personen eisen dat ze officiële identificatiedocumenten voorleggen;

5° de bijstand vorderen van de federale of lokale politiediensten.

§ 4. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de personeelsleden van de inspectiedienst een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

1° de identificatie van de bewoonde ruimten waartoe de personeelsleden van de inspectiedienst toegang wensen te hebben;

2° de vermoedelijke inbreuken die het voorwerp zijn van de controle;

3° de wetgeving die aanleiding geeft tot de controle waarvoor de inspecteurs een machtiging tot bezoek menen nodig hebben;

4° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is;

5° de proportionaliteit en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

le délai prescrit, la visite des lieux est réputée être refusée. Le service d'inspection peut introduire un recours contre la décision de refus ou l'absence de décision devant la chambre des mises en accusation dans les quinze jours de la notification de la décision ou de l'expiration du délai.

Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une heures par au moins deux membres assermentés du service d'inspection agissant conjointement.

§ 5. Au début de toute audition, il est communiqué à la personne interrogée :

1° que ses déclarations peuvent être utilisées comme preuve en justice;

2° qu'elle peut demander que toutes les questions qui lui sont posées et les réponses qu'elle donne soient actées dans les termes utilisés;

3° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition.

L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui interviennent lors de l'audition ou à une partie de celle-ci.

A la fin de l'audition, la personne interrogée a le droit de relire celle-ci ou de demander que lecture lui en soit faite. Elle peut demander à ce que ses déclarations soient corrigées ou complétées.

Les membres du personnel du service d'inspection qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.

§ 6. Les membres du service d'inspection peuvent consulter tous les supports d'information et les données qu'ils contiennent. Ils peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme lisible et intelligible qu'ils ont demandée.

S'il n'est pas possible de prendre des copies sur place, les membres du service d'inspection peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

§ 7. Pour étendre les recherches dans un système informatique ou une partie de celui-ci, entamées sur la base du paragraphe 6, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, le service d'inspection peut

De onderzoeksrechter beslist binnen een termijn van maximum 48 uur na ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed. Bij gebrek aan een beslissing binnen de voorgeschreven termijn wordt het plaatsbezoek geacht te zijn geweigerd. De inspectiedienst kan beroep instellen tegen de weigeringsbeslissing of het gebrek aan een beslissing bij de kamer van inbeschuldigingstelling binnen vijftien dagen na de kennisgeving van de beslissing of het verstrijken van de termijn.

Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee beëdigde leden van de inspectiedienst die samen optreden.

§ 5. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld:

1° dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;

2° dat hij kan vragen dat alle vragen die hem worden gesteld en de antwoorden die hij geeft, worden genoteerd in de gebruikte bewoordingen;

3° dat hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Elke ondervraagde persoon mag de documenten in zijn bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij mag tijdens het verhoor of later vragen om die documenten bij het verhoor te voegen.

Het verhoor vermeldt nauwkeurig het tijdstip waarop het wordt aangevat, eventueel onderbroken en hervat, alsook beëindigd. Het vermeldt de identiteit van de personen die tussenkomen tijdens het verhoor of een deel ervan.

Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen of het te laten voorlezen. Hij mag zijn verklaringen laten verbeteren of er iets aan laten toevoegen.

De personeelsleden van de inspectiedienst die een persoon ondervragen, delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.

§ 6. De leden van de inspectiedienst mogen alle informatiedragers en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen in een door hen gevraagde leesbare en verstaanbare vorm.

Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst, tegen een ontvangstbewijs dat een inventaris bevat, het

solliciter l'autorisation d'un juge d'instruction, selon les mêmes conditions que celles prévues au paragraphe 4.

§ 8. Lorsque cela s'avère nécessaire, les membres du service d'inspection disposent d'une habilitation de sécurité correspondant au niveau de classification, au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, des informations auxquelles ils doivent avoir accès afin de réaliser leur contrôle.

Art. 16. § 1^{er}. A la fin des inspections, un rapport est dressé par le service d'inspection ou par l'autorité publique désignée par le Roi en vertu de l'article 5, § 2. Une copie de ce rapport est transmise à l'organisme d'évaluation de la conformité, au titulaire de certificat de cybersécurité européen ou à l'émetteur de déclaration de conformité de l'Union européenne inspecté.

§ 2. A sa demande et pour autant que cela poursuive l'accomplissement de ses missions légales, une autre autorité publique peut recevoir une copie du rapport prévu au § 1^{er}.

§ 3. Par dérogation au paragraphe 2, l'autorité visée à l'article 5, § 1^{er} ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2 transmet une copie du rapport prévu au paragraphe 1^{er} à l'autorité sectorielle compétente lorsque celui-ci est lié à un contrôle effectué auprès d'une infrastructure critique, d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques, 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 ou de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

Art. 17. § 1^{er}. Le service d'inspection limite l'accès aux informations relatives à l'exécution de ses missions aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec la présente loi ou d'autres dispositions légales.

§ 2. Les membres du personnel du service d'inspection sont tenus au secret professionnel en ce qui concerne les informations en rapport à l'exécution de la présente loi.

§ 3. A sa demande et pour autant que cela poursuive l'accomplissement de ses missions légales, une autre autorité publique peut recevoir une copie d'un procès-verbal

informatiquesystème en de erin opgenomen gegevens in beslag nemen.

§ 7. Om de zoekactie in een informatiesysteem of een deel hiervan die op basis van paragraaf 6 werd opgestart, uit te breiden naar een informatiesysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiedienst de toestemming vragen van een onderzoeksrechter, volgens dezelfde voorwaarden als die bedoeld in paragraaf 4.

§ 8. Indien nodig beschikken de leden van de inspectiedienst over een veiligheidsmachtiging die overeenstemt met het classificatieniveau, als bedoeld in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, van de informatie waar zij toegang toe moeten hebben om hun controle uit te voeren.

Art. 16. § 1. Na afloop van de inspecties stelt de inspectiedienst of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een verslag op waarvan een kopie wordt bezorgd aan de geïnspecteerde conformiteitsbeoordelingsinstantie, houder van een Europees cyberbeveiligingscertificaat of afgever van een EU-conformiteitsverklaring.

§ 2. Op haar verzoek en voor zover dit nodig is voor het vervullen van haar wettelijke opdrachten kan een andere overheid een kopie krijgen van het verslag bedoeld in § 1.

§ 3. In afwijking van paragraaf 2 bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een kopie van het verslag bedoeld in paragraaf 1 aan de bevoegde sectorale overheid indien dit betrekking heeft op een controle bij een kritieke infrastructuur, een aanbieder van essentiële diensten of een digitaaldienstverlener als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid of het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.

Art. 17. § 1. De inspectiedienst beperkt de toegang tot de informatie betreffende de uitvoering van zijn opdrachten tot de personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met deze wet of andere wettelijke bepalingen.

§ 2. De personeelsleden van de inspectiedienst zijn gebonden aan het beroepsgeheim wat de informatie in verband met de uitvoering van deze wet betreft.

§ 3. Op haar verzoek en voor zover dit nodig is voor het vervullen van haar wettelijke opdrachten kan een andere

ainsi que de toutes les informations complémentaires liées à un contrôle effectué par l'autorité visée à l'article 5, § 1^{er} ou par l'autorité publique désignée par le Roi en vertu de l'article 5, § 2.

§ 4. L'autorité visée à l'article 5, § 1^{er} ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2 transmet à l'autorité sectorielle compétente une copie complète du procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué auprès d'une infrastructure critique, d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou 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.

§ 5. Dans l'exercice de leurs fonctions, les membres du personnel du service d'inspection peuvent :

1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne leur est pas destinée personnellement;

2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu;

3° prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne.

Art. 18. § 1^{er}. L'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen volontaire ou l'émetteur de déclaration de conformité de l'Union européenne apporte son entière collaboration aux membres du service d'inspection ou aux experts appelés à participer à l'inspection dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes.

Si nécessaire, l'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen volontaire ou l'émetteur de déclaration de conformité de l'Union européenne met à disposition des membres du service d'inspection et des experts appelés à participer à l'inspection le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections.

§ 2. Après avis de l'autorité visée à l'article 5, § 1^{er}, le Roi peut déterminer des rétributions relatives à la délivrance et aux prestations d'inspections réalisées dans le cadre du recours volontaire à des certifications et déclarations de conformité visées par le Règlement sur la cybersécurité.

Ces rétributions sont à charge des organismes d'évaluation de la conformité, titulaires de certificat de cybersécurité européen volontaire et des émetteurs de déclaration de

overheid een kopie krijgen van het proces-verbaal en van alle bijkomende informatie in verband met een controle uitgevoerd door de autoriteit bedoeld in artikel 5, § 1, of door de overheid die door de Koning is aangewezen krachtens artikel 5, § 2.

§ 4. De autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, bezorgt de bevoegde sectorale overheid een volledige kopie van het proces-verbaal en van alle bijkomende informatie in verband met een controle bij een kritieke infrastructuur, aanbieder van essentiële diensten of digitaal dienstverlener als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of 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.

§ 5. Bij de uitoefening van hun functie mogen de personeelsleden van de inspectiedienst:

1° met opzet kennisnemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hen bestemd is;

2° met opzet de personen identificeren die bij de overdracht van de informatie en de inhoud ervan betrokken zijn;

3° met opzet kennisnemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon.

Art. 18. § 1. De conformiteitsbeoordelingsinstantie, de houder van een vrijwillig Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring verleent zijn volledige medewerking aan de leden van de inspectiedienst of de experts die deelnemen aan de inspectie bij de uitoefening van hun functie, met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen.

Indien nodig stelt de conformiteitsbeoordelingsinstantie, de houder van een vrijwillig Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring het nodige materiaal ter beschikking van de leden van de inspectiedienst en de experts die deelnemen aan de inspectie, zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties.

§ 2. Na advies van de autoriteit bedoeld in artikel 5, § 1, kan de Koning retributies bepalen voor de afgifte en de inspectieprestaties die geleverd worden in het kader van het vrijwillige gebruik van certificeringen en conformiteitsverklaringen bedoeld in de Cyberbeveiligingsverordening.

Deze retributies zijn ten laste van de conformiteitsbeoordelingsinstanties, de houders van vrijwillige Europese cyberbeveiligingscertificaten en de

conformité de l'Union européenne. Le Roi fixe les modalités de calcul et de paiement.

CHAPITRE 6. - Sanctions

Section 1^{re}. - Procédure

Art. 19. § 1^{er}. Lorsqu'un ou plusieurs manquements aux exigences imposées par le Règlement sur la cybersécurité, la présente loi ou ses arrêtés d'exécution ou aux exigences de schémas de certification volontaire de cybersécurité sont constatés, le service d'inspection met en demeure le contrevenant de se conformer, dans un délai raisonnable qu'il fixe, aux obligations qui lui incombent.

Le délai est déterminé en tenant compte des conditions de fonctionnement du contrevenant et des mesures à mettre en œuvre.

§ 2. Au préalable, le service d'inspection informe, de manière motivée, le contrevenant de son intention de lui adresser une mise en demeure et lui fait part de son droit, dans les quinze jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant son envoi par le service d'inspection.

Art. 20. § 1^{er}. Lorsque le service d'inspection constate que le contrevenant n'a pas respecté les obligations découlant de la loi ou du Règlement sur la cybersécurité, les faits sont constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection.

§ 2. Le fait pour quiconque d'empêcher ou entraver volontairement l'exécution d'un contrôle effectué par les membres du service d'inspection, de refuser de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou de communiquer sciemment des informations inexactes ou incomplètes est constaté par les membres assermentés du service d'inspection dans un procès-verbal.

§ 3. Les procès-verbaux rédigés par les membres assermentés du service d'inspection font foi jusqu'à preuve du contraire.

Section 2. - Retrait d'un certificat

Art. 21. L'autorité visée à l'article 5, § 1^{er} retire un certificat de cybersécurité lorsque le bénéficiaire ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité.

Section 3. - Limitation, suspension ou retrait d'une autorisation ou d'une délégation

Art. 22. L'autorité visée à l'article 5, § 1^{er} limite, suspend ou retire les autorisations ainsi que les délégations qu'elle a

afgevers van EU-conformiteitsverklaringen. De Koning bepaalt de nadere regels inzake berekening en betaling.

HOOFDSTUK 6. - Sancties

Afdeling 1. - Procedure

Art. 19. § 1. Wanneer een of meer inbreuken op de voorschriften van de Cyberbeveiligingsverordening, deze wet of de uitvoeringsbesluiten ervan of op de voorschriften van vrijwillige cyberbeveiligingscertificeringsregelingen worden vastgesteld, maant de inspectiedienst de overtreder aan om zijn verplichtingen na te komen binnen een door hem vastgestelde redelijke termijn.

De termijn wordt bepaald rekening houdend met de werkingsomstandigheden van de overtreder en de te nemen maatregelen.

§ 2. De inspectiedienst deelt de overtreder vooraf, op een met redenen omklede wijze, mee dat hij van plan is hem een ingebrekestelling te sturen en laat hem weten dat hij het recht heeft om, binnen vijftien dagen na ontvangst van deze informatie, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending ervan door de inspectiedienst.

Art. 20. § 1. Als de inspectiedienst vaststelt dat de overtreder de verplichtingen van de wet of de Cyberbeveiligingsverordening niet is nagekomen, worden de feiten opgetekend in een proces-verbaal door de beëdigde leden van de inspectiedienst.

§ 2. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst opzettelijk verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of bewust foutieve of onvolledige informatie verstrekt, wordt opgetekend in een proces-verbaal door de beëdigde leden van de inspectiedienst.

§ 3. De processen-verbaal opgesteld door de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.

Afdeling 2. - Intrekking van een certificaat

Art. 21. De autoriteit bedoeld in artikel 5, § 1, trekt een cyberbeveiligingscertificaat in als de begunstigde de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft.

Afdeling 3. - Beperken, opschorten of intrekken van een toelating of een delegatie

Art. 22. De autoriteit bedoeld in artikel 5, § 1, voorziet in de beperking, opschorting of intrekking van toelatingen alsook

accordées aux organismes d'évaluation de la conformité, lorsque le bénéficiaire de l'autorisation ou de la délégation ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité.

Section 4. - Amendes administratives

Art. 23. § 1^{er}. Toute infraction au Règlement sur la cybersécurité, à la présente loi ou ses arrêtés d'exécution peut faire l'objet d'une sanction administrative.

§ 2. Est puni d'une amende de 500 à 75 000 euros quiconque ne répond pas à une demande d'information de l'autorité visée à l'article 5, § 1^{er}.

§ 3. Est puni d'une amende de 500 à 100 000 euros le fabricant ou fournisseur de produits TIC, services TIC ou processus TIC qui ne se conforme pas aux dispositions relatives à l'autoévaluation de la conformité visées à l'article 53 du Règlement sur la cybersécurité.

§ 4. Est également puni d'une amende de 500 à 100 000 euros le titulaire d'un certificat de cybersécurité européen attestant du niveau d'assurance dit "élémentaire" qui ne se conforme pas aux obligations émanant du schéma européen de certification de cybersécurité correspondant.

§ 5. Est puni d'une amende de 500 à 125 000 euros le titulaire d'un certificat de cybersécurité européen attestant du niveau d'assurance dit "substantiel" ou "élevé" qui ne se conforme pas aux obligations émanant du schéma européen de certification de cybersécurité correspondant.

§ 6. Est puni d'une amende de 500 à 150 000 euros quiconque ne coopère pas lors d'un contrôle, par exemple en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle.

§ 7. Est puni d'une amende de 500 à 200 000 euros quiconque communique sciemment des informations inexactes ou incomplètes ou se rend coupable de tout autre acte ou omission frauduleuse dans le cadre de l'exécution du Règlement sur la cybersécurité, de la présente loi et de ses arrêtés d'exécution.

Art. 24. § 1^{er}. La décision d'imposer une amende administrative est motivée. Elle mentionne également le montant de l'amende administrative et les infractions visées.

§ 2. L'autorité visée à l'article 5, § 1^{er} informe au préalable le contrevenant de sa proposition motivée de sanction administrative et lui fait part de son droit, dans les quinze jours de la réception de la proposition, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. La proposition est présumée reçue par le contrevenant le

van delegaties die ze aan conformiteitsbeoordelingsinstanties heeft verleend, als de begunstigde van de toelating of delegatie de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft.

Afdeling 4. - Administratieve geldboetes

Art. 23. § 1. Elke inbreuk op de Cyberbeveiligingsverordening, op deze wet of op de uitvoeringsbesluiten ervan kan aanleiding geven tot een administratieve sanctie.

§ 2. Wordt gestraft met een geldboete van 500 tot 75 000 euro: eenieder die niet reageert op een verzoek om informatie van de autoriteit bedoeld in artikel 5, § 1, van de wet.

§ 3. Wordt gestraft met een geldboete van 500 tot 100 000 euro: de fabrikant of aanbieder van ICT-producten, -diensten of -processen die niet voldoet aan de bepalingen inzake conformiteitszelfbeoordeling bedoeld in artikel 53 van de Cyberbeveiligingsverordening.

§ 4. Wordt eveneens gestraft met een geldboete van 500 tot 100 000 euro: de houder van een Europees cyberbeveiligingscertificaat voor zekerheidsniveau "basis" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling.

§ 5. Wordt gestraft met een geldboete van 500 tot 125 000 euro: de houder van een Europees cyberbeveiligingscertificaat voor zekerheidsniveau "substantieel" of "hoog" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling.

§ 6. Wordt gestraft met een geldboete van 500 tot 150 000 euro: eenieder die weigert mee te werken tijdens een inspectie, bijvoorbeeld door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken.

§ 7. Wordt gestraft met een boete van 500 tot 200 000 euro: eenieder die bewust onjuiste of onvolledige informatie verstrekt of zich schuldig maakt aan enige andere frauduleuze handeling of nalatigheid in het kader van de uitvoering van de Cyberbeveiligingsverordening, deze wet en de uitvoeringsbesluiten ervan.

Art. 24. § 1. De beslissing om een administratieve geldboete op te leggen wordt met redenen omkleed. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§ 2. De autoriteit bedoeld in artikel 5, § 1, bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen vijftien dagen na ontvangst van het voorstel, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. Het voorstel wordt geacht te

sixième jour suivant son envoi par de l'autorité visée à l'article 5, § 1^{er}.

§ 3. En tenant compte des moyens de défense invoqués dans le délai visé au paragraphe 2 ou en l'absence de réaction du contrevenant dans ce même délai, l'autorité visée à l'article 5, § 1^{er} peut adopter une sanction administrative visée à l'article 23.

§ 4. L'amende administrative est proportionnelle à la gravité, la durée, les moyens utilisés, les dommages causés et les circonstances des faits.

L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois ans.

§ 5. Le concours de plusieurs infractions peut donner lieu à une amende administrative unique proportionnelle à la gravité de l'ensemble des faits.

Art. 25. La décision est notifiée par envoi recommandé au contrevenant.

Une invitation à acquitter l'amende dans un délai d'un mois est jointe à la décision.

Art. 26. Le contrevenant peut contester la décision prise en vertu du chapitre 6 par l'autorité visée à l'article 5, § 1^{er} devant la Cour des marchés visée à l'article 101 du Code judiciaire.

La Cour des marchés est saisie du fond du litige et dispose d'une compétence de pleine juridiction.

La demande est introduite par requête contradictoire introduite, à peine de déchéance, dans les soixante jours de la notification de la décision de l'autorité visée à l'article 5, § 1^{er}.

La cause est traitée selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire.

Ce recours ne suspend pas l'exécution de la décision.

Art. 27. § 1^{er}. Lorsque le contrevenant reste en défaut de payer l'amende administrative dans le délai imparti, la décision d'infliger une amende administrative a force exécutoire et l'autorité visée à l'article 5, § 1^{er} peut décerner une contrainte.

La contrainte est décernée par le représentant légal de l'autorité visée à l'article 5, § 1^{er} ou par un membre du personnel habilité à cette fin.

§ 2. La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un commandement de payer dans les vingt-quatre heures, à peine d'exécution par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.

zijn ontvangen door de overtreder de zesde dag na de verzending ervan door de autoriteit bedoeld in artikel 5, § 1.

§ 3. Rekening houdend met de verweermiddelen die zijn aangevoerd binnen de in paragraaf 2 bedoelde termijn of bij gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de autoriteit bedoeld in artikel 5, § 1, een in artikel 23 bedoelde administratieve sanctie opleggen.

§ 4. De administratieve geldboete staat in verhouding tot de ernst, de duur, de gebruikte middelen, de veroorzaakte schade en de omstandigheden van de feiten.

De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jaar.

§ 5. De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

Art. 25. De beslissing wordt bij aangetekende zending ter kennis gebracht van de overtreder.

Een verzoek tot betaling van de geldboete binnen een maand wordt bij de beslissing gevoegd.

Art. 26. De overtreder kan de beslissing die de autoriteit bedoeld in artikel 5, § 1, krachtens hoofdstuk 6 heeft genomen, betwisten bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek.

De grond van de zaak wordt voorgelegd aan het Marktenhof, dat uitspraak doet met volle rechtsmacht.

De vordering wordt ingesteld bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen zestig dagen na kennisgeving van de beslissing van de autoriteit bedoeld in artikel 5, § 1, wordt ingediend.

De zaak wordt behandeld zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek.

Dit beroep schorst de uitvoering van de beslissing niet.

Art. 27. § 1. Als de overtreder de administratieve geldboete niet betaalt binnen de toegestane termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de autoriteit bedoeld in artikel 5, § 1, een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door de wettelijke vertegenwoordiger van de autoriteit bedoeld in artikel 5, § 1, of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaardersexploit betekend. De betekening bevat een bevel om te betalen binnen vierentwintig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 3. Le contrevenant peut former opposition à la contrainte devant le juge des saisies.

L'opposition est motivée à peine de nullité. Elle est formée au moyen d'une citation à l'autorité visée à l'article 5, § 1^{er} par exploit d'huissier dans les quinze jours à partir de la signification de la contrainte.

Les dispositions du chapitre VIII de la première partie du Code judiciaire sont applicables à ce délai, y compris les prorogations prévues à l'article 50, alinéa 2, et l'article 55 de ce Code.

L'exercice de l'opposition à la contrainte suspend l'exécution de la contrainte, ainsi que la prescription des créances contenues dans la contrainte, jusqu'à ce qu'il ait été statué sur son bien-fondé. Les saisies déjà pratiquées antérieurement conservent leur caractère conservatoire.

§ 4. L'autorité visée à l'article 5, § 1^{er} peut faire pratiquer la saisie conservatoire et exécuter la contrainte en usant des voies d'exécution prévues à la cinquième partie du Code judiciaire.

Les paiements partiels effectués en suite de la signification d'une contrainte ne font pas obstacle à la continuation des poursuites.

§ 5. Les frais de signification de la contrainte de même que les frais de l'exécution ou des mesures conservatoires sont à charge du contrevenant.

Ils sont déterminés suivant les règles établies pour les actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 28. L'autorité visée à l'article 5, § 1^{er} ne peut imposer d'amende administrative à l'échéance d'un délai de trois ans, à compter du jour où le fait a été commis.

CHAPITRE 7. - Réclamations

Section 1^{re}. - Saisine de l'autorité nationale de certification de cybersécurité

Art. 29. L'autorité visée à l'article 5, § 1^{er} reçoit et traite les réclamations des personnes en rapport avec un certificat de cybersécurité européen, le refus de délivrance d'un certificat ou une déclaration de conformité de l'Union européenne.

Art. 30. Le dépôt d'une réclamation par toute personne physique ou morale au sens de l'article 63 du Règlement sur la cybersécurité est sans frais.

Art. 31. § 1^{er}. L'autorité compétente examine si la réclamation est recevable.

§ 2. Une réclamation est recevable lorsqu'elle :

§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het dient gedaan te worden door middel van een dagvaarding van de autoriteit bedoeld in artikel 5, § 1, van de wet bij deurwaardersexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.

De uitoefening van verzet tegen het dwangbevel schorst de tenuitvoerlegging van het dwangbevel, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak is gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.

§ 4. De autoriteit bedoeld in artikel 5, § 1, mag bewarend beslag laten leggen en het dwangbevel uitvoeren met gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§ 5. De betekeningkosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder.

Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 28. De autoriteit bedoeld in artikel 5, § 1, kan geen administratieve geldboete opleggen na het verstrijken van een termijn van drie jaar, te rekenen vanaf de dag waarop het feit werd gepleegd.

HOOFDSTUK 7. - Klachten

Afdeling 1. - Aanhangigmaking bij de nationale cyberbeveiligingscertificeringsautoriteit

Art. 29. De autoriteit bedoeld in artikel 5, § 1, ontvangt en behandelt klachten van personen over een Europees cyberbeveiligingscertificaat, de weigering om een certificaat af te geven of een EU-conformiteitsverklaring.

Art. 30. De indiening van een klacht door iedere natuurlijke of rechtspersoon als bedoeld in artikel 63 van de Cyberbeveiligingsverordening is kosteloos.

Art. 31. § 1. De bevoegde autoriteit gaat na of de klacht ontvankelijk is.

§ 2. Een klacht is ontvankelijk wanneer zij:

- est rédigée dans l'une des langues nationales;
- contient un exposé des faits et les indications nécessaires pour identifier le certificat de cybersécurité européen, le refus de délivrance d'un certificat ou la déclaration de conformité de l'Union européenne sur laquelle elle porte;
- relève de la compétence de l'autorité visée à l'article 5, § 1^{er} en vertu du Règlement sur la cybersécurité.

§ 3. L'autorité compétente peut inviter l'auteur de la réclamation à préciser sa réclamation.

Art. 32. L'affaire est traitée dans la langue nationale de la réclamation.

Art. 33. La décision portant sur la recevabilité de la réclamation est portée à la connaissance de l'auteur de la réclamation.

Si l'autorité visée à l'article 5, § 1^{er} conclut à l'irrecevabilité de la réclamation, l'auteur de la réclamation en est informé par décision motivée.

Art. 34. Si l'autorité visée à l'article 5, § 1^{er} conclut à la recevabilité de la réclamation, elle peut exercer les pouvoirs qui lui sont conférés conformément aux articles 11, 12, 21 et 22.

L'autorité visée à l'article 5, § 1^{er} peut délivrer elle-même la certification demandée.

Section 2. Recours

Art. 35. Le réclamant peut contester la décision prise en vertu du chapitre 7 par l'autorité visée à l'article 5, § 1^{er} devant la Cour des marchés visée à l'article 101 du Code judiciaire.

La Cour des marchés est saisie du fond du litige et dispose d'une compétence de pleine juridiction.

La demande est introduite par requête contradictoire introduite, à peine de déchéance, dans les soixante jours de la notification de la décision de l'autorité visée à l'article 5, § 1^{er}.

La cause est traitée selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire.

Ce recours ne suspend pas l'exécution de la décision.

CHAPITRE 8. - Dispositions finales

Section 1^{re}. - Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

- opgesteld is in een van de landstalen;
- een uiteenzetting van de feiten bevat, alsook de nodige indicaties voor de identificatie van het Europees cyberbeveiligingscertificaat, de weigering om een certificaat af te geven of de EU-conformiteitsverklaring waarop zij betrekking heeft;
- behoort tot de bevoegdheid van de autoriteit bedoeld in artikel 5, § 1, krachtens de Cyberbeveiligingsverordening.

§ 3. De bevoegde autoriteit kan de klager verzoeken zijn klacht toe te lichten.

Art. 32. De zaak wordt behandeld in de landstaal van de klacht.

Art. 33. De beslissing inzake de ontvankelijkheid van de klacht wordt ter kennis gebracht van de klager.

Indien de autoriteit bedoeld in artikel 5, § 1, de klacht onontvankelijk verklaart, wordt de klager hierover ingelicht door een met redenen omklede beslissing.

Art. 34. Indien de autoriteit bedoeld in artikel 5, § 1, de klacht ontvankelijk verklaart, kan zij de bevoegdheden uitoefenen die haar overeenkomstig de artikelen 11, 12, 21 en 22 zijn verleend.

De autoriteit bedoeld in artikel 5, § 1, kan zelf de gevraagde certificering afgeven.

Afdeling 2. Beroepen

Art. 35. De klager kan de beslissing die de autoriteit bedoeld in artikel 5, § 1, krachtens hoofdstuk 7 heeft genomen, betwisten bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek.

De grond van de zaak wordt voorgelegd aan het Marktenhof, dat uitspraak doet met volle rechtsmacht.

De vordering wordt ingesteld bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen zestig dagen na kennisgeving van de beslissing van de autoriteit bedoeld in artikel 5, § 1, wordt ingediend.

De zaak wordt behandeld zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek.

Dit beroep schorst de uitvoering van de beslissing niet.

HOOFDSTUK 8. - Slotbepalingen

Afdeling 1. - Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecomunicatiesector

Art. 36. L'article 14, § 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, est complété par un 7° rédigé comme suit :

« 7° L'Institut exerce les missions de contrôle et de sanctions qui lui sont confiées par l'arrêté royal visant à exécuter l'article 5, § 2, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. »

Art. 37. Dans l'article 14, § 2, 3°, g) de la même loi, inséré par la loi du 10 juillet 2012 portant des dispositions diverses en matière de communications électroniques (cité comme : loi Télécom), les mots « en ce compris la sécurité des réseaux et des systèmes d'information, » sont insérés entre les mots « sécurité publique, » et « ou de sécurité et protection civile ».

Section 2. - Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 38. L'article 45 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers est complété par un paragraphe 6, rédigé comme suit :

« § 6. A la demande de la FSMA et en fonction de l'objet du schéma de certification de cybersécurité concerné, le Roi peut, à condition qu'elle dispose de l'expertise requise à ces fins, confier à la FSMA, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. Dans cette hypothèse, le Roi sollicite l'avis et se consulte au préalable avec l'autorité visée à l'article 5, § 1^{er} de la loi précitée et la FSMA. La FSMA exerce ces missions de contrôle uniquement vis-à-vis des entités sur lesquelles elle exerce le contrôle en vertu du paragraphe 1^{er}, 2° du présent article et des lois particulières qui régissent le contrôle des établissements financiers. »

Art. 39. L'article 75, § 1 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, est complété par un 26°, rédigé comme suit :

« 26° à l'autorité visée à l'article 5, § 1^{er} de la loi du [...] relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de

Art. 36. Artikel 14, § 1, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector wordt aangevuld met een punt 7°, luidende:

“7° Het Instituut oefent de toezichts- en sanctieopdrachten uit die hem zijn toevertrouwd bij het koninklijk besluit dat voorziet in de uitvoering van artikel 5, § 2, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit].”

Art. 37. In artikel 14, § 2, 3°, g), van dezelfde wet, ingevoegd bij de wet van 10 juli 2012 houdende diverse bepalingen inzake elektronische communicatie (aangehaald als: wet Telecom), worden de woorden “met inbegrip van de beveiliging van netwerk- en informatiesystemen,” ingevoegd tussen de woorden “openbare veiligheid,” en “of civiele veiligheid en bescherming”.

Afdeling 2. - Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 38. Artikel 45 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten wordt aangevuld met een paragraaf 6, luidende:

“§ 6. Op verzoek van de FSMA en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling kan de Koning, op voorwaarde dat eerstgenoemde over de daarvoor vereiste expertise beschikt, bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], volledig of gedeeltelijk aan de FSMA toevertrouwen. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de FSMA. De FSMA vervult die toezichtopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens paragraaf 1, 2°, van dit artikel en de bijzondere wetten die het toezicht op de financiële instellingen regelen.”

Art. 39. Artikel 75, § 1, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten wordt aangevuld met een punt 26°, luidende:

« 26° aan de autoriteit bedoeld in artikel 5, § 1, van de wet van [...] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit of

cybersécurité ou aux autorités désignées par le Roi en vertu de l'article 5, § 2 de la même loi. »

Section 3. - Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique

Art. 40. Dans le Chapitre IV/4 de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, inséré par la loi du 7 avril 2019 et modifié en dernier lieu par la loi du [date], il est inséré un article 36/48/1 rédigé comme suit :

« Art. 36/48/1. A la demande de la Banque et en fonction de l'objet du schéma de certification de cybersécurité concerné, le Roi peut, à condition qu'elle dispose de l'expertise requise à ces fins, confier à la Banque, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. Dans cette hypothèse, le Roi sollicite l'avis et se consulte au préalable avec l'autorité visée à l'article 5, § 1^{er} de la loi précitée et la Banque. La Banque exerce ces missions de contrôle uniquement vis-à-vis des entités sur lesquelles elle exerce le contrôle en vertu des articles 8 et 12*bis* et des lois particulières qui régissent le contrôle des établissements financiers. »

Art. 41. Dans l'article 36/14 de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, modifié en dernier lieu par la loi du 20 juillet 2020, il est inséré un 20°/2 rédigé comme suit :

« 20°/2 dans les limites du droit de l'Union européenne, à l'autorité visée à l'article 5, § 1^{er} de la loi du [...] relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité, ou aux autorités désignées par le Roi en vertu de l'article 5, § 2 de la même loi ; »

Section 4. – Modification du Code de droit économique

Art. 42. L'article I.20 du Code de droit économique, inséré par la loi du 17 juillet 2013 et modifié par les lois du 1^{er} décembre 2016 et du 15 avril 2018, est complété par un 9° rédigé comme suit :

“9° Règlement sur la cybersécurité : Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013.”.

aan de door de Koning aangewezen overheden krachtens artikel 5, § 2, van dezelfde wet.”

Afdeling 3. - Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 40. In Hoofdstuk IV/4 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, ingevoegd bij de wet van 7 april 2019 en het laatst gewijzigd bij de wet van [datum], wordt een artikel 36/48/1 ingevoegd, luidende:

“Art. 36/48/1. Op verzoek van de Bank en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling kan de Koning, op voorwaarde dat eerstgenoemde over de daarvoor vereiste expertise beschikt, bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], volledig of gedeeltelijk aan de Bank toevertrouwen. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de Bank. De Bank vervult die toezichtopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens de artikelen 8 en 12*bis* en de bijzondere wetten die het toezicht op de financiële instellingen regelen.”

Art. 41. In artikel 36/14 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, het laatst gewijzigd bij de wet van 20 juli 2020, wordt een punt 20°/2 ingevoegd, luidende:

“20° /2 binnen de grenzen van het recht van de Europese Unie, aan de autoriteit bedoeld in artikel 5, § 1, van de wet van [...] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, of aan de door de Koning krachtens artikel 5, § 2, van dezelfde wet aangewezen overheden;”

Afdeling 4. - Wijzigingen van het Wetboek van Economisch recht

Art. 42. Artikel I.20 van het Wetboek van Economisch recht, ingevoegd bij de wet van 17 juli 2013 en gewijzigd bij de wetten van 1 december 2016 en 15 april 2018, wordt aangevuld met een bepaling onder 9°, luidende:

“9° Cyberbeveiligingsverordening: Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en

communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013. ”.

Art. 43. Dans le livre XV, titre Ier, chapitre 2, du même Code, inséré par la loi du 18 avril 2017, il est inséré une section 10 intitulée « Section 10.Certification de cybersécurité ».

Art. 43. In boek XV, titel 1, hoofdstuk 2, van hetzelfde Wetboek, ingevoegd bij de wet van 18 april 2017, wordt een afdeling 10 ingevoegd, luidende “Afdeling 10 Certificering van de cyberbeveiliging”.

Art. 44. Dans la section 10, inséré par l’article 43, il est inséré une sous-section 1^{ère} intitulée « Sous-section 1^{ère}. Certification de cybersécurité volontaire ».

Art. 44. In afdeling 10, ingevoegd bij artikel 43, wordt een onderafdeling 1 ingevoegd, luidende “Onderafdeling 1. Vrijwillige cyberbeveiligingscertificering”.

Art. 45. Dans la sous-section 1^{ère}, inséré par l’article 44, il est inséré un article XV.30/3, rédigé comme suit :

Art. 45. In onderafdeling 1, ingevoegd bij artikel 44, wordt een artikel XV.30/3 ingevoegd, luidende als volgt:

Art. XV.30/3. En matière de certification de cybersécurité volontaire, à la demande du SPF Economie, le Roi peut, par arrêté délibéré en Conseil des ministres, confier certaines missions visées aux chapitres 5 et 6, à l’exception des articles 21 et 22, de la loi du [date] [relative à la certification de la cybersécurité des technologies de l’information et des communications et portant désignation d’une autorité nationale de certification de cybersécurité], à certains agents du SPF Economie, à condition que le SPF Economie dispose de l’expertise requise à ces fins. Dans cette hypothèse, le Roi sollicite l’avis et se consulte au préalable avec l’autorité visée à l’article 5, § 1^{er} de la loi précitée et avec le SPF Economie. Le SPF Economie exerce ces missions de contrôle uniquement sur les produits ou entités réglementés par le présent Code, ses arrêtés d’exécution ou les règlements de l’Union européenne relatifs aux matières qui, conformément aux livres VI, VII, IX et XII du présent Code, relèvent du pouvoir réglementaire du Roi.

Art. XV. 30/3. Op het gebied van vrijwillige cyberbeveiligingscertificering, op verzoek van de FOD Economie, kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van de artikelen 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], aan bepaalde ambtenaren van de FOD Economie toevertrouwen, op voorwaarde dat de FOD Economie over de daarvoor vereiste expertise beschikt. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de FOD Economie. De FOD Economie vervult die toezichtopdrachten enkel ten aanzien van producten of entiteiten die gereguleerd zijn door dit Wetboek, de uitvoeringsbesluiten ervan of verordeningen van de Europese Unie betreffende aangelegenheden die, overeenkomstig de boeken VI, VII, IX en XII van dit Wetboek, tot de regelgevende bevoegdheid van de Koning behoren.

Art. 46. Dans la section 10, inséré par l’article 43, il est inséré une sous-section 2 intitulée « Sous-section 2. Certification de cybersécurité obligatoire ».

Art. 46. In afdeling 10, ingevoegd bij artikel 43, wordt een onderafdeling 2 ingevoegd, luidende “Onderafdeling 2. Verplichte cyberbeveiligingscertificering”.

Art. 47. Par dérogation au paragraphe 2 de l’article 3 de la présente loi, il est inséré dans la sous-section 2, inséré par l’article 46, un article XV.30/4, rédigé comme suit :

Art. 47. In afwijking van paragraaf 2 van artikel 3 van deze wet, wordt in onderafdeling 2, ingevoegd bij artikel 46, een artikel XV.30/4 ingevoegd, luidende als volgt:

« **Art. XV.30/4. § 1.** En matière de certification européenne de cybersécurité rendue obligatoire en vertu du droit de l’Union ou du droit national, à la demande du SPF Economie et après avis de l’autorité nationale de certification de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, confier certaines missions en matière de contrôle relatives au règlement sur la cybersécurité ou relatives à la loi du [date] relative à la certification de cybersécurité des technologies de l’information et des communications et portant désignation d’une autorité nationale de certification de cybersécurité, à certains agents du SPF Economie, à

“**Art. XV.30/4. § 1.** Met betrekking tot de Europese cyberbeveiligingscertificering die verplicht is op grond van de Europese of nationale wetgeving, op verzoek van de FOD Economie en na advies van de nationale cyberbeveiligingscertificeringsautoriteit, kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde toezichtopdrachten in verband met de Cyberbeveiligingsverordening of in verband met de wet van [datum] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit,

condition que ce dernier dispose de l'expertise requise à ces fins.

§ 2. Les missions en matière de contrôle visées au paragraphe 1^{er}, y compris la recherche, la constatation, la poursuite et la sanction des infractions, s'effectuent conformément aux dispositions du présent livre.

Art. 48. Dans le livre XV, titre 3, chapitre 2, section 11/3, du même Code, insérée par la loi du 18 avril 2017, sont insérés les articles XV.125/7 et XV.125/8, rédigés comme suit :

« **Art. XV.125/7.** Dans le cadre de la surveillance visé à l'article [XV.30/4], sont punis d'une sanction de niveau 2:

- 1° le titulaire d'un certificat de cybersécurité rendu obligatoire en vertu du droit de l'Union ou du droit national attestant du niveau d'assurance dit "élémentaire" qui ne se conforme pas aux obligations émanant du schéma de certification de cybersécurité correspondant ;
- 2° quiconque ne coopère pas lors d'un contrôle, par exemple en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle.

Art. XV.125/8. Dans le cadre de la surveillance visé à l'article [XV.30/4], sont punis d'une sanction de niveau 3 :

- 1° le titulaire d'un certificat de cybersécurité rendu obligatoire en vertu du droit de l'Union ou du droit national attestant du niveau d'assurance dit "substantiel" ou "élevé" qui ne se conforme pas aux obligations émanant du schéma de certification de cybersécurité correspondant ;
- 2° quiconque communique sciemment des informations inexacts ou incomplètes ou se rend coupable de tout autre acte ou omission frauduleuse dans le cadre de l'exécution du Règlement sur la cybersécurité. ».

Section 5. - Entrée en vigueur et dispositions transitoires

Art. 49. La présente loi entre en vigueur le jour de sa publication au Moniteur belge.

Donné à

Par le Roi :

toevertrouwen aan bepaalde ambtenaren van de FOD Economie, op voorwaarde dat die laatste over de voor deze doeleinden vereiste expertise beschikt.

§ 2. De in het eerste paragraaf bedoelde controletaken, met inbegrip van de opsporing, vaststelling, vervolging en bestraffing van inbreuken, worden uitgeoefend overeenkomstig de bepalingen van dit boek.

Art. 48. In boek XV, titel 3, hoofdstuk 2, afdeling 11/3, van hetzelfde Wetboek, ingevoegd bij de wet van 18 april 2017, worden de artikelen XV.125/7 en XV.125/8 ingevoegd, luidende:

“**Art. XV.125/7.** In het kader van het toezicht bedoeld in artikel [XV.30/4], wordt gestraft met een sanctie van niveau 2:

- 1° de houder van een cyberbeveiligingscertificaat die verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "basis" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling;
- 2° eenieder die weigert mee te werken tijdens een inspectie, bijvoorbeeld door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken.

Art. XV.125/8. In het kader van het toezicht bedoeld in artikel [XV.30/4], wordt gestraft met een sanctie van niveau 3:

- 1° de houder van een cyberbeveiligingscertificaat die verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "substantieel" of "hoog" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken cyberbeveiligingscertificeringsregeling;
- 2° eenieder die bewust onjuiste of onvolledige informatie verstrekt of zich schuldig maakt aan enige andere frauduleuze handeling of nalatigheid in het kader van de uitvoering van de Cyberbeveiligingsverordening.”.

Afdeling 5. - Inwerkingtreding en overgangsbepalingen

Art. 49. Deze wet treedt in werking de dag waarop ze in het Belgisch Staatsblad wordt bekendgemaakt.

Gegeven te

Van Koningswege :

Le Premier Ministre,

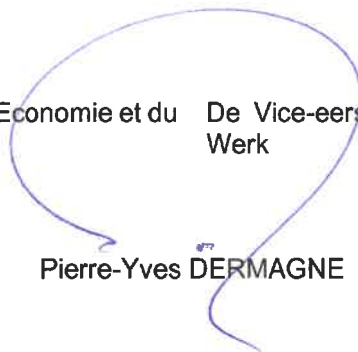
De Eerste Minister,



Alexander DE CROO

Le Vice-Premier Ministre et Ministre de l'Economie et du Travail,

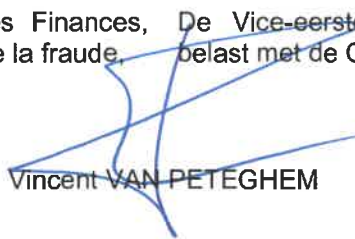
De Vice-eersteminister en minister van Economie en Werk



Pierre-Yves DERMAGNE

Le Vice-Premier Ministre et Ministre des Finances, chargé de la Coordination de la lutte contre la fraude,

De Vice-eersteminister en Minister van Financiën, belast met de Coördinatie van de fraudebestrijding,



Vincent VAN PETEGHEM

La Vice-Première Ministre et Ministre de la Fonction publique, des Entreprises publiques, des Télécommunications et de la Poste,

De Vice-eersteminister en Minister van Ambtenarenzaken, Telecommunicatie en Post,

en Minister van Overheidsbedrijven,

Petra DE SUTTER



EXPOSÉ DES MOTIFS	MEMORIE VAN TOELICHTING
MESDAMES, MESSIEURS,	MEVROUWEN, MIJNE HEREN,
CONSIDÉRATIONS GÉNÉRALES	ALGEMENE BESCHOUWINGEN
<p>Ce projet de loi vise à mettre en œuvre le Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013, désigné ci-après le « Règlement sur la cybersécurité ».</p> <p>Cette mise en œuvre exige, en effet, l'adoption de certaines dispositions légales en droit interne pour fixer notamment : les pouvoirs des services d'inspection, les règles de sanctions, les procédures de réclamations et de recours, les habilitations légales pour effectuer certaines délégations, les règles générales d'indépendance, etc.</p>	<p>Dit wetsontwerp geeft uitvoering aan Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013, hierna de "Cyberbeveiligingsverordening" genoemd.</p> <p>Deze uitvoering vereist immers de invoering van een aantal wettelijke bepalingen in het nationaal recht om met name de bevoegdheden van de inspectiediensten, de sanctieregels, de klachten- en beroepsprocedures, de wettelijke machtigingen voor bepaalde delegaties, de algemene onafhankelijkheidsregels, enz. vast te stellen.</p>
COMMENTAIRE DES ARTICLES	ARTIKELSGEWIJZE BESPREKING
CHAPITRE 1 ^{er} . - Définitions et dispositions générales	HOOFDSTUK 1. - Definities en algemene bepalingen
Section 1 ^{re} . - Objet et champ d'application	Afdeling 1. - Onderwerp en toepassingsgebied
Sous-section 1 ^{re} . - Objet	Onderafdeling 1. - Onderwerp
<p>Cette section précise le fondement légal et l'objet du projet de loi.</p> <p>L'autorité fédérale est compétente en cette matière car elle relève de la protection des consommateurs ainsi que de la sécurité publique, deux compétences fédérales.</p> <p>En effet, le Règlement sur la cybersécurité a, selon ses considérants 7 et 10, pour but de renforcer la confiance des consommateurs auprès des fournisseurs de services numériques et de faire en sorte que les consommateurs disposent d'informations précises sur le niveau d'assurance auquel la sécurité de leur produits TIC, services TIC et processus TIC a été certifiée. Pour rappel, la Cour constitutionnelle a jugé, dans son arrêt n°101/2013 du 9 juillet 2013 que « <i>L'autorité fédérale est habilitée à fixer les règles générales en matière de protection des consommateurs</i> » et ce, conformément à l'article 6, § 1er, VI, alinéa 4, 2°, de la loi spéciale du 8 août 1980 de réformes institutionnelles.</p> <p>De plus, le Règlement sur la cybersécurité a également pour objectif d'atténuer les risques liés à une numérisation et une connectivité accrue, rendant, selon le considérant 3, « <i>l'ensemble de la société plus vulnérable aux cybermenaces et [exacerbant] les dangers auxquels sont confrontés les individus, notamment les personnes vulnérables telles que les</i></p>	<p>Deze afdeling verduidelijkt de wettelijke grondslag en het onderwerp van het wetsontwerp.</p> <p>De federale overheid is bevoegd voor deze materie aangezien consumentenbescherming en openbare veiligheid twee federale bevoegdheden zijn.</p> <p>Volgens overwegingen 7 en 10 heeft de Cyberbeveiligingsverordening immers tot doel het vertrouwen van consumenten in digitaal dienstverleners te versterken en ervoor te zorgen dat consumenten over nauwkeurige informatie beschikken met betrekking tot het zekerheidsniveau waarop hun ICT-producten, -diensten en -processen zijn gecertificeerd. Ter herinnering, in zijn arrest nr. 101/2013 van 9 juli 2013 oordeelde het Grondwettelijk Hof het volgende: "<i>De federale overheid is ertoe gemachtigd de algemene regels inzake consumentenbescherming vast te stellen</i>" en dit overeenkomstig artikel 6, § 1, VI, vierde lid, 2°, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.</p> <p>Voorts heeft de Cyberbeveiligingsverordening tot doel de risico's te beperken die verbonden zijn aan de toenemende digitalisering en connectiviteit. Volgens overweging 3 leiden die risico's ertoe dat "<i>de maatschappij als geheel kwetsbaarder wordt voor cyberdreigingen en [...] de gevaren waaraan individuen, waaronder kwetsbare personen zoals</i></p>

<p><i>enfants</i> ». À cette fin, le Règlement entend « <i>prendre toutes les mesures nécessaires pour améliorer la cybersécurité dans l'Union afin que les réseaux et systèmes d'information, les réseaux de communication, les produits, services et appareils numériques utilisés par les citoyens, les organisations et les entreprises — depuis les petites et moyennes entreprises (PME), telles qu'elles sont définies dans la recommandation 2003/361/CE de la Commission, jusqu'aux opérateurs d'infrastructures critiques — soient mieux protégés contre les cybermenaces</i> », toujours selon le même considérant. Il en ressort clairement que le Règlement sur la cybersécurité porte sur la sécurité publique. Comme l'a rappelé la section de législation du Conseil d'Etat à plusieurs reprises, notamment dans ses avis n°35.678, 43.644/4 et 63.972/4, « <i>les règles relatives à la sécurité publique demeurent en principe de la compétence de l'autorité fédérale</i> ».</p>	<p><i>kinderen, zijn blootgesteld worden verergerd</i>”. Volgens dezelfde overweging wil de verordening daartoe “<i>alle noodzakelijke maatregelen [nemen] om de cyberbeveiliging in de Unie te versterken, zodat netwerk- en informatiesystemen, communicatienetwerken, digitale producten, diensten en toestellen die worden gebruikt door burgers, organisaties en bedrijven — van kleine en middelgrote ondernemingen in de zin van Aanbeveling 2003/361/EG van de Commissie tot exploitanten van cruciale infrastructuurvoorzieningen — beter beschermd worden tegen cyberdreigingen</i>”. Hieruit blijkt duidelijk dat de Cyberbeveiligingsverordening betrekking heeft op openbare veiligheid. De afdeling wetgeving van de Raad van State heeft er herhaaldelijk op gewezen, met name in zijn adviezen nrs 35.678, 43.644/4 en 63.972/4, dat “<i>de federale overheid in principe bevoegd blijft voor de regels inzake openbare veiligheid</i>” (vrije vertaling).</p>
Sous-section 2. - Champ d'application	Onderafdeling 2. - Toepassingsgebied
Article 3	Artikel 3
<p>Cet article précise que les certifications de cybersécurité prévues par la présente loi peuvent porter sur plusieurs types d'objet, définis à l'article 2, 12), 13), et 14) du Règlement sur la cybersécurité : un produit TIC (un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information), un service TIC (un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information) ou encore un processus TIC (un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance).</p> <p>En effet, les organisations, les fabricants ou les fournisseurs impliqués dans la conception et le développement de produits TIC, services TIC ou processus TIC devraient être encouragés à mettre en œuvre, aux stades les plus précoces de la conception et du développement, des mesures permettant de protéger au mieux la sécurité de ces produits, services et processus, de manière que la survenance de cyberattaques soit présumée et que leur incidence soit anticipée et minimisée. La sécurité devrait être prise en charge tout au long du cycle de vie du produit TIC, service TIC ou processus TIC par les processus de conception et de développement qui évoluent constamment pour réduire le risque de préjudice causé par une utilisation malveillante.</p> <p>A l'exception des articles 21 et 22, les chapitres 5 et 6 de la loi ne sont pas applicables aux certifications européennes rendues obligatoires en vertu du droit de l'Union ou du droit national. Les articles 21 et 22 visent, en effet, le retrait, la suspension ou la limitation d'un certificat, d'une autorisation ou d'une délégation. Il s'agit d'une prérogative de l'autorité nationale de certification de cybersécurité, que l'on soit dans une certification volontaire ou obligatoire.</p>	<p>Volgens dit artikel kunnen de in deze wet bedoelde cyberbeveiligingscertificeringen betrekking hebben op verschillende soorten zaken, bepaald in artikel 2, 12), 13) en 14), van de Cyberbeveiligingsverordening: een ICT-product (een element of groep elementen van een netwerk- of informatiesysteem), een ICT-dienst (een dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opvraging of verwerking van gegevens door middel van netwerk- en informatiesystemen) of een ICT-proces (een reeks activiteiten die wordt uitgevoerd om een ICT-product of ICT-dienst te ontwerpen, ontwikkelen, leveren of onderhouden).</p> <p>Organisaties, fabrikanten en aanbieders die betrokken zijn bij het ontwerp en de ontwikkeling van ICT-producten, -diensten en -processen moeten er immers toe worden aangespoord om al in de eerste fase van ontwerp en ontwikkeling maatregelen te treffen om ervoor te zorgen dat het beveiligingsniveau van deze producten, diensten en processen zo hoog mogelijk is, zodat cyberaanvallen zijn ingecalculeerd en de gevolgen daarvan zijn ingeschat en tot een minimum beperkt. Beveiliging moet tijdens de gehele levensduur van het ICT-product, de ICT-dienst of het ICT-proces worden gewaarborgd door middel van ontwerp- en ontwikkelingsprocessen die constant evolueren om het risico op schade door kwaadwillig gebruik te verminderen.</p> <p>Met uitzondering van de artikelen 21 en 22 zijn de hoofdstukken 5 en 6 van de wet niet van toepassing op Europese certificeringen die verplicht zijn op grond van de Europese of nationale wetgeving, worden opgelegd. Artikel 21 en 22 hebben immers betrekking op de intrekking, opschorting of beperking van een certificaat, een toelating of een delegatie. Dit is een bevoegdheid van de nationale cyberbeveiligingscertificeringsautoriteit, ongeacht of het om een vrijwillige of verplichte certificering gaat.</p>

<p>Le paragraphe 2, alinéa 2 prévoit que l'autorité nationale de certification de cybersécurité applique les dispositions relatives à la mise en demeure et au recours, lorsqu'elle compte faire usage des prérogatives prévues aux articles 21 et 22 dans le cadre de certification obligatoire.</p> <p>Les chapitres 5 et 6 (à l'exception des articles 21 et 22) ne sont pas applicables aux certifications obligatoires car ces dernières poursuivent, le cas échéant, un but plus spécifique justifiant des règles de contrôle et de sanctions différentes. En effet, dans le cadre de la certification de cybersécurité volontaire, le régime légal a pour but de renforcer, de manière générale, la confiance des consommateurs et la sécurité publique en proposant des certifications de cybersécurité auxquelles les personnes peuvent choisir de se soumettre. Lorsqu'une certification de cybersécurité est rendue obligatoire en vertu du droit de l'Union ou du droit national, le régime légal poursuit un but plus spécifique : imposer auprès de certaines entités l'obtention du certificat de cybersécurité concerné. A partir du moment où l'obtention d'un certificat de cybersécurité est considéré comme nécessaire et devient une obligation légale, des contrôles et des sanctions plus strictes peuvent se justifier.</p> <p>Le Roi peut néanmoins décider, à l'initiative de cette autorité publique et si cela s'avère nécessaire, de lui accorder les mêmes pouvoirs de contrôle et de sanctions que ceux attribués à l'autorité nationale de certification de cybersécurité, assortis des mêmes possibilités de recours pour les certifications volontaires et visés aux chapitres 5 et 6 de la loi.</p> <p>En effet, les autorités publiques qui souhaiteraient rendre obligatoire l'obtention d'un certificat de cybersécurité et qui ne bénéficieraient pas déjà de dispositions similaires en matière de contrôle et de sanction dans leurs lois sectorielles pourraient ainsi appliquer les chapitres 5 et 6 de la présente loi.</p> <p>Conformément à l'article 1, § 2 du Règlement sur la cybersécurité et à l'article 4, § 2 du Traité sur l'Union européenne, le paragraphe 3 rappelle que la présente loi ne porte pas préjudice à l'adoption de mesures nationales en matière de certification de cybersécurité pour protéger la sécurité publique, la défense, la sécurité nationale et les activités dans le domaine du droit pénal.</p> <p>De plus, le paragraphe 4 rappelle que la présente loi est sans préjudice des compétences des autorités publiques, notamment les autorités de surveillance de marché et les autorités sectorielles, de rendre obligatoire une certification de cybersécurité et d'en assurer le contrôle ainsi que, le cas échéant, les sanctions, en vertu de leurs compétences légales comme autorité de surveillance de marché, 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 (« loi NIS »), de la loi du 1er juillet 2011 relative à la protection et la sécurité des infrastructures critiques et de l'arrêté royal du 2 décembre 2011 concernant</p>	<p>Paragraaf 2, tweede lid, bepaalt dat de nationale cyberbeveiligingscertificeringsautoriteit de bepalingen betreffende de ingebrekestelling en het beroep toepast, indien ze van plan is gebruik te maken van de bevoegdheden bedoeld in artikel 21 en 22 in het kader van de verplichte certificering.</p> <p>De hoofdstukken 5 en 6 (met uitzondering van artikel 21 en 22) zijn niet van toepassing op verplichte certificeringen omdat die laatste in voorkomend geval een specifiek doel nastreven, dat andere toezicht- en sanctieregels rechtvaardigt. In het kader van de vrijwillige cyberbeveiligingscertificering heeft de wettelijke regeling immers tot doel om, in het algemeen, het consumentenvertrouwen te vergroten en de openbare veiligheid te verhogen door cyberbeveiligingscertificeringen aan te bieden waaraan personen zich vrijwillig kunnen onderwerpen. Indien een cyberbeveiligingscertificering krachtens het recht van de Unie of het nationale recht wordt opgelegd, streeft de wettelijke regeling een specifiek doel na: bij bepaalde entiteiten het verkrijgen van het betrokken cyberbeveiligingscertificaat opleggen. Vanaf het ogenblik dat het verkrijgen van een cyberbeveiligingscertificaat noodzakelijk wordt geacht en een wettelijke verplichting wordt, zijn strengere controles en sancties gerechtvaardigd.</p> <p>Niettemin kan de Koning, indien nodig, op initiatief van die overheid beslissen haar dezelfde toezichts- en sanctiebevoegdheden toe te kennen als die van de nationale cyberbeveiligingscertificeringsautoriteit, alsook dezelfde beroepsmogelijkheden, die in hoofdstuk 5 en 6 van de wet zijn vastgelegd voor vrijwillige certificeringen.</p> <p>Overheden die het verkrijgen van een cyberbeveiligingscertificaat verplicht willen maken en waarvan de sectorale wetten nog geen soortgelijke bepalingen inzake toezicht en sancties bevatten, kunnen zo immers hoofdstuk 5 en 6 van deze wet toepassen.</p> <p>Overeenkomstig artikel 1, lid 2, van de Cyberbeveiligingsverordening en artikel 4, lid 2, van het Verdrag betreffende de Europese Unie wijst paragraaf 3 erop dat deze wet geen afbreuk doet aan nationale maatregelen inzake cyberbeveiligingscertificering die worden genomen ter bescherming van de openbare veiligheid, defensie, de nationale veiligheid en de activiteiten op het gebied van het strafrecht.</p> <p>Bovendien herinnert paragraaf 4 eraan dat deze wet geen afbreuk doet aan de bevoegdheden van de overheden, met name de markttoezichtautoriteiten en sectorale overheden, om een cyberbeveiligingscertificering op te leggen en te zorgen voor het toezicht op en, in voorkomend geval, de sancties met betrekking tot deze certificering, krachtens hun wettelijke bevoegdheden als markttoezichtautoriteit, 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 ("NIS-wet"), de wet van 1 juli 2011 betreffende de beveiliging en de</p>
--	---

<p>les infrastructures critiques dans le sous-secteur du transport aérien.</p> <p>En tout état de cause, les autorités de surveillance de marché et les autorités sectorielles devront disposer des moyens humains et budgétaires suffisants pour contrôler les certifications obligatoires.</p> <p>Par ailleurs, un cinquième paragraphe exclut l'application des paragraphes 2 à 4 de l'article 5 à la Banque nationale de Belgique visée par la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, à la FSMA visée par la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ainsi qu'au Service Public Fédéral Economie visé au Code de droit économique. Les paragraphes 2 et 3 de l'article 5 habilite le Roi à confier, sous certaines conditions, à d'autres autorités administratives ou autorités administratives indépendantes que l'autorité nationale de certification de cybersécurité, des missions de contrôle normalement dévolues à cette dernière. Le paragraphe 4 prévoit que ces entités disposent des mêmes droits et obligations que celles de l'autorité nationale de certification de cybersécurité, sans préjudice de leurs compétences légales existantes.</p> <p>Cette exclusion s'explique par le fait que de nouvelles dispositions sont insérées dans les lois organiques de la Banque nationale de Belgique, de la FSMA ainsi que dans le Code de droit économique.</p>	<p>bescherming van de kritieke infrastructuur en het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuur in de deelsector van het luchtvervoer.</p> <p>De markttoezichtautoriteiten en sectorale overheden moeten in ieder geval over voldoende menselijke en budgettaire middelen beschikken om de verplichte certificeringen te controleren.</p> <p>Voorts sluit een vijfde paragraaf uit dat de paragrafen 2 tot 4 van artikel 5 worden toegepast op de Nationale Bank van België bedoeld in de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, op de FSMA bedoeld in de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten en op de Federale Overheidsdienst Economie bedoeld in het Wetboek van Economisch recht. . De paragrafen 2 en 3 van artikel 5 machtigen de Koning om, onder bepaalde voorwaarden, toezichtsoverdrachten waarmee normaal de nationale cyberbeveiligingscertificeringsautoriteit belast is, toe te vertrouwen aan andere administratieve overheden of onafhankelijke administratieve overheden. Paragraaf 4 bepaalt dat deze entiteiten dezelfde rechten en verplichtingen hebben als de nationale cyberbeveiligingscertificeringsautoriteit, onverminderd hun bestaande wettelijke bevoegdheden.</p> <p>Deze uitsluiting wordt verklaard door het feit dat nieuwe bepalingen worden ingevoegd in de organieke wetten van de Nationale Bank van België en de FSMA, alsook in het Wetboek van economisch recht.</p>
Section 2. - Définitions	Afdeling 2. - Definities
Article 4	Artikel 4
<p>L'article 4 donne quelques définitions utiles pour le projet de loi.</p> <p>La notion d'autorité publique vise de manière large toutes les autorités publiques du pays et reprend à cet effet la définition de l'article 5 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.</p>	<p>Artikel 4 bevat enkele nuttige definities voor het wetsontwerp.</p> <p>Het begrip "overheid" heeft, in ruime zin, betrekking op alle overheden van het land en neemt hiervoor de definitie over van artikel 5 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.</p>
CHAPITRE 2. - Autorités compétentes et coopération au niveau national	HOOFDSTUK 2. - Bevoegde autoriteiten en samenwerking op nationaal niveau
Section 1^{re}. Autorités compétentes	Afdeling 1. Bevoegde autoriteiten
Article 5	Artikel 5
<p>L'article 58 du Règlement sur la cybersécurité impose à chaque État membre de désigner une ou plusieurs autorités nationales de certification de cybersécurité sur son territoire. Le projet de loi dispose que le Roi désigne une seule autorité qui sera chargée, en tant qu'autorité nationale</p>	<p>Artikel 58 van de Cyberbeveiligingsverordening verplicht elke lidstaat om een of meer nationale cyberbeveiligingscertificeringsautoriteiten op zijn grondgebied aan te wijzen. Het wetsontwerp bepaalt dat de Koning één autoriteit aanwijst die, als nationale</p>

<p>de certification de cybersécurité, des tâches et missions visées par le Règlement sur la cybersécurité et la présente loi.</p> <p>La désignation d'une seule autorité nationale de certification de cybersécurité est recommandée afin de faciliter pour tous les acteurs intéressés (fabricants, fournisseurs de services, organismes d'évaluation de la conformité, consommateurs, États membres de l'Union européenne, etc.) l'accès aux informations nécessaires sur la certification de cybersécurité en Belgique.</p> <p>D'un point de vue organisationnel, il est également souhaitable qu'une seule autorité centrale garde une vue d'ensemble des différents schémas de certification en matière de cybersécurité. Cela est d'autant plus vrai que l'on ne sait pas exactement quels schémas de certification l'Union européenne mettra en place à l'avenir, ni à quels types de produits, services ou processus ils s'appliqueront.</p> <p>Lors de cette désignation, le Roi tiendra compte de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique (« CCB ») qui confie au CCB les missions légales suivantes : coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication, coordonner la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière.</p> <p>En vertu de l'article 60 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 (loi NIS) et de son arrêté d'exécution du 12 juillet 2019, le CCB assume également le rôle de centre national de réponse aux incidents de sécurité informatique (« CSIRT national »).</p> <p>Toutefois, le second paragraphe prévoit, à titre dérogatoire, que le Roi peut, par arrêté délibéré en Conseil des ministres, en fonction de l'objet du schéma de certification et à la demande d'une autre autorité publique, attribuer certaines missions de l'autorité nationale de certification de cybersécurité, en matière de contrôle (chapitre 5) et de sanctions (chapitre 6), à l'exception des articles 21 et 22, à cette autre autorité publique.</p> <p>L'objectif n'est pas que le Roi attribue les tâches de contrôle et de sanction de l'autorité nationale de certification de cybersécurité pour toutes les certifications à d'autres administrations mais de permettre, via une éventuelle décision du Roi prise en concertation avec l'administration concernée et l'autorité nationale de certification de cybersécurité, de confier légalement les tâches de contrôle et de sanction dans le cadre de la présente loi à une autre administration en raison de son expertise particulière par rapport au schéma de certification concerné. Il ne s'agit toutefois ici que d'une faculté pour le Roi afin d'éviter des doublons dans les inspections et d'assurer une coordination dans les contrôles. A cette occasion, le Roi veille à respecter les répartitions de compétences existantes prévues par la loi.</p>	<p>cyberbeveiligingscertificeringsautoriteit, belast is met de taken en opdrachten bedoeld in de Cyberbeveiligingsverordening en in deze wet.</p> <p>De aanwijzing van één nationale cyberbeveiligingscertificeringsautoriteit wordt aanbevolen om alle belanghebbenden (fabrikanten, dienstverleners, conformiteitsbeoordelingsinstanties, consumenten, lidstaten van de Europese Unie, enz.) gemakkelijker toegang te verlenen tot de nodige informatie over cyberbeveiligingscertificering in België.</p> <p>Uit organisatorisch oogpunt is het ook wenselijk dat één centrale autoriteit het overzicht behoudt van de verschillende cyberbeveiligingscertificeringsregelingen, te meer daar men niet precies weet welke certificeringsregelingen de Europese Unie in de toekomst zal invoeren, noch op welke soorten producten, diensten of processen deze van toepassing zullen zijn.</p> <p>Bij deze aanwijzing houdt de Koning rekening met het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België ("CCB"), dat het CCB de volgende wettelijke opdrachten toevertrouwt: coördineren van de evaluatie en certificatie van de veiligheid van informatie- en communicatiesystemen, coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberveiligheid, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak.</p> <p>Krachtens artikel 60 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 (NIS-wet) en het bijhorende uitvoeringsbesluit van 12 juli 2019 vervult het CCB ook de rol van nationaal computer security incident response team ("nationaal CSIRT").</p> <p>Bij wijze van afwijking bepaalt de tweede paragraaf echter dat de Koning, bij besluit vastgesteld na overleg in de Ministerraad, naargelang het voorwerp van de certificeringsregeling en op verzoek van een andere overheid, bepaalde opdrachten van de nationale cyberbeveiligingscertificeringsautoriteit inzake toezicht (hoofdstuk 5) en sancties (hoofdstuk 6), met uitzondering van artikel 21 en 22, kan toewijzen aan deze andere overheid.</p> <p>Het is niet de bedoeling dat de Koning de taken inzake toezicht en sancties van de nationale cyberbeveiligingscertificeringsautoriteit voor alle certificeringen aan andere administraties toewijst, maar dat, via een eventuele beslissing van de Koning genomen in overleg met de betrokken administratie en de nationale cyberbeveiligingscertificeringsautoriteit, de taken inzake toezicht en sancties in het kader van deze wet wettelijk kunnen worden toevertrouwd aan een andere administratie vanwege haar bijzondere expertise in verband met de betrokken certificeringsregeling. Het betreft hier echter</p>
---	---

<p>Il veille ainsi notamment à ce que les compétences de l'autorité qu'il charge d'assurer le contrôle en ce qui concerne une certification de cybersécurité s'étendent uniquement aux entreprises qui tombent déjà dans le champ des compétences de l'autorité concernée. Par ailleurs, le Roi veille à tenir compte de l'expertise de l'autorité concernée lors de l'attribution éventuelle de tâches de contrôle.</p> <p>Conformément aux articles 58, § 5 et 59, § 2 du Règlement sur la cybersécurité, toute autorité publique qui doit assurer des missions de contrôle doit disposer des moyens humains et budgétaires suffisants pour réaliser ses tâches.</p> <p>Le troisième paragraphe précise que le Roi doit, préalablement au fait de confier certaines tâches de contrôle à une autre autorité, se concerter avec celle-ci.</p> <p>Par ailleurs, le quatrième paragraphe prévoit que ces entités, auxquelles auront été attribuées certaines compétences de l'autorité nationale de certification de cybersécurité, disposent des mêmes droits et obligations que celles de l'autorité nationale de certification de cybersécurité visées au chapitre 5, sans préjudice de leurs compétences légales existantes. Cette disposition garantit le respect du principe d'égalité et de non-discrimination en imposant le respect des mêmes obligations à toute entité à laquelle serait attribuée une ou plusieurs compétences dévolues, en principe, à l'autorité nationale de certification de cybersécurité en vertu du Règlement sur la cybersécurité ou de la présente loi.</p>	<p>alleen een mogelijkheid voor de Koning teneinde dubbel inspectiewerk te voorkomen en ervoor te zorgen dat de controles gecoördineerd gebeuren. Bij deze gelegenheid ziet de Koning toe op de naleving van de in de wet bepaalde bestaande bevoegdheidsverdelingen. Hij zorgt er met name voor dat de bevoegdheden van de overheid die Hij belast met het toezicht in verband met een cyberbeveiligingscertificering, enkel betrekking hebben op ondernemingen die al onder de bevoegdheid van de betrokken overheid vallen. Verder houdt de Koning rekening met de expertise van de betrokken overheid bij de eventuele toekenning van toezichtstaken.</p> <p>Overeenkomstig de artikelen 58, lid 5, en 59, lid 2, van de Cyberbeveiligingsverordening moet elke overheid die toezichtsoopdrachten vervult over voldoende menselijke en budgettaire middelen beschikken om haar taken uit te voeren.</p> <p>Volgens de derde paragraaf moet de Koning, alvorens bepaalde toezichtstaken toe te vertrouwen aan een andere overheid, overleg plegen met die laatste.</p> <p>Voorts bepaalt de vierde paragraaf dat deze entiteiten, waaraan bepaalde bevoegdheden van de nationale cyberbeveiligingscertificeringsautoriteit zijn toegekend, dezelfde rechten en verplichtingen hebben als die van de nationale cyberbeveiligingscertificeringsautoriteit bedoeld in hoofdstuk 5, onverminderd hun bestaande wettelijke bevoegdheden. Deze bepaling waarborgt de naleving van het gelijkheids- en non-discriminatiebeginsel door dezelfde verplichtingen op te leggen aan elke entiteit waaraan een of meer bevoegdheden worden toegekend waarover de nationale cyberbeveiligingscertificeringsautoriteit in beginsel krachtens de Cyberbeveiligingsverordening of deze wet beschikt.</p>
<p>Section 2. - Coopération au niveau national</p>	<p>Afdeling 2. - Samenwerking op nationaal niveau</p>
<p>Article 6</p>	<p>Artikel 6</p>
<p>Cet article énonce que l'autorité nationale de certification de cybersécurité se concerte avec les autres autorités publiques. Il permet également à l'autorité nationale de certification de cybersécurité de consulter, par exemple, les fédérations professionnelles concernées par la certification en matière de cybersécurité.</p> <p>Le Règlement sur la cybersécurité prévoit notamment, en son article 58, § 7, h), que l'autorité nationale de certification de cybersécurité coopère, non seulement avec les autres autorités nationales de certification de cybersécurité, mais également avec d'autres autorités publiques. Ces autorités se partagent notamment, au travers de cette coopération, des informations en matière de contrôle du respect des exigences dudit règlement et du schéma de certification de cybersécurité.</p>	<p>Dit artikel vermeldt dat de nationale cyberbeveiligingscertificeringsautoriteit overleg pleegt met de andere overheden. Het laat de nationale cyberbeveiligingscertificeringsautoriteit ook toe om bijvoorbeeld de beroepsfederaties te raadplegen die betrokken zijn bij de cyberbeveiligingscertificering.</p> <p>Artikel 58, lid 7, h), van de Cyberbeveiligingsverordening bepaalt met name dat de nationale cyberbeveiligingscertificeringsautoriteit niet alleen samenwerkt met andere nationale cyberbeveiligingscertificeringsautoriteiten, maar ook met andere overheden. Via deze samenwerking wisselen deze overheden met name informatie uit over het toezicht op de naleving van de voorschriften van deze verordening en van de cyberbeveiligingscertificeringsregeling.</p>

<p>Le paragraphe 2 met en œuvre l'article 58, § 8, a) du Règlement sur la cybersécurité. Il s'agit d'une obligation de communication de toutes les informations utiles à l'exécution des tâches légales de l'autorité nationale de certification de cybersécurité à charge des organismes d'évaluation de la conformité, des titulaires de certificats de cybersécurité européens et des émetteurs de déclarations de conformité de l'Union européenne.</p> <p>Le non-respect de cette obligation peut conduire l'autorité nationale de certification de cybersécurité à prononcer des sanctions administratives, conformément au chapitre 6 de la présente loi.</p> <p>Conformément au paragraphe 3, l'autorité nationale de certification de cybersécurité et les autres autorités publiques en Belgique pourront s'échanger mutuellement toutes les informations nécessaires à l'application du Règlement sur la cybersécurité et de la présente loi, notamment en matière de délivrance de certificat, de contrôle, de sanction et de réclamation. Parmi les autres autorités publiques figurent notamment les autorités de surveillance de marché, les autorités sectorielles, les services de sécurité publique, les services de police, les services de renseignements, l'organe de coordination pour l'analyse de la menace et le ministère public.</p> <p>Ce partage d'information demeure néanmoins limité à ce qui est pertinent et proportionné à l'objectif de cet échange, notamment dans le respect d'autres dispositions légales nationales ou internationales.</p> <p>Pour définir les modalités pratiques de cette collaboration et des échanges d'informations, des protocoles entre administrations seraient alors conclus.</p> <p>Si la collaboration conduit à une transmission de données à caractère personnel entre autorités, il sera tenu compte des dispositions applicables à la protection des données à caractère personnel et notamment l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ainsi que des principes du Règlement (UE) 2016/679 (règlement général sur la protection des données), notamment la limitation du traitement à ce qui est nécessaire en vue de l'objectif poursuivi.</p> <p>Le paragraphe 4 autorise les personnes dépositaires, par état ou par profession, des secrets qu'on leur confie à faire connaître ces secrets à l'autorité nationale de certification de cybersécurité ou à une autre autorité lorsque cela est nécessaire à l'application de la présente loi ou du Règlement sur la cybersécurité.</p> <p>A titre d'exemple, cette disposition permet au service d'inspection de contrôler les réseaux et systèmes d'informations d'une entité qui regroupe des professionnels soumis à une obligation de secret professionnel. De même, les membres d'une autre autorité publique pourraient partager des informations nécessaires pour l'exécution de la</p>	<p>Paragraaf 2 geeft uitvoering aan artikel 58, lid 8, a), van de Cyberbeveiligingsverordening. Het betreft de verplichting voor conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen om alle informatie te verstrekken die nuttig is voor de uitvoering van de wettelijke taken van de nationale cyberbeveiligingscertificeringsautoriteit.</p> <p>Indien deze verplichting niet wordt nageleefd, kan de nationale cyberbeveiligingscertificeringsautoriteit administratieve sancties opleggen, overeenkomstig hoofdstuk 6 van deze wet.</p> <p>Overeenkomstig paragraaf 3 kunnen de nationale cyberbeveiligingscertificeringsautoriteit en de andere overheden in België onderling alle informatie uitwisselen die nodig is voor de toepassing van de Cyberbeveiligingsverordening en deze wet, met name wat betreft de afgifte van certificaten, het toezicht, sancties en klachten. De andere overheden omvatten met name de markttoezichtautoriteiten, de sectorale overheden, de openbare veiligheidsdiensten, de politiediensten, de inlichtingendiensten, het coördinatieorgaan voor de dreigingsanalyse en het openbaar ministerie.</p> <p>Deze informatie-uitwisseling blijft evenwel beperkt tot hetgeen relevant is voor en evenredig is met het doel van deze uitwisseling, met name overeenkomstig andere nationale of internationale wettelijke bepalingen.</p> <p>Om de praktische modaliteiten van deze samenwerking en informatie-uitwisseling te bepalen, zouden protocollen worden gesloten tussen de administraties.</p> <p>Indien de samenwerking leidt tot een overdracht van persoonsgegevens tussen overheden, wordt rekening gehouden met de bepalingen die van toepassing zijn op de bescherming van persoonsgegevens en met name met artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, alsook met de beginselen van Verordening (EU) 2016/679 (algemene verordening gegevensbescherming), met name de beperking van de verwerking tot hetgeen noodzakelijk is voor het nagestreefde doel.</p> <p>Paragraaf 4 staat toe dat personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, deze geheimen bekendmaken aan de nationale cyberbeveiligingscertificeringsautoriteit of aan een andere overheid indien dit nodig is voor de toepassing van deze wet of van de Cyberbeveiligingsverordening.</p> <p>Deze bepaling laat de inspectiedienst bijvoorbeeld toe om de netwerk- en informatiesystemen te controleren van een entiteit die beroepsbeoefenaars verenigt die aan het beroepsgeheim gebonden zijn. Ook kunnen leden van een andere overheid informatie die nodig is voor de uitvoering van de wet of van de Cyberbeveiligingsverordening delen met de nationale cyberbeveiligingscertificeringsautoriteit of</p>
---	--

<p>loi ou du Règlement sur la cybersécurité avec l'autorité nationale de certification de cybersécurité ou une autre administration, sans contradiction avec leur éventuelle obligation de secret professionnel.</p> <p>Le cas échéant, les professionnels soumis à un code de déontologie devront respecter ce dernier avant de procéder à la levée du secret professionnel.</p> <p>Bien entendu, cette disposition ne porte pas préjudice à l'application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Il s'agit d'un régime juridique distinct de celui du secret professionnel. Ce paragraphe ne permet donc pas de s'affranchir du respect des obligations légales relatives aux traitements d'éventuelles informations classifiées.</p>	<p>een andere administratie, zonder dat dit in strijd zou zijn met hun eventuele beroepsgeheim.</p> <p>In voorkomend geval moeten beroepsbeoefenaars die onderworpen zijn aan een deontologische code, deze naleven alvorens over te gaan tot de opheffing van het beroepsgeheim.</p> <p>Uiteraard doet deze bepaling geen afbreuk aan de toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Het betreft een andere juridische regeling dan die van het beroepsgeheim. Deze paragraaf laat dus niet toe de wettelijke verplichtingen met betrekking tot de verwerking van eventuele geclassificeerde informatie te veronachtzamen.</p>
Article 7	Artikel 7
<p>Sauf attribution par le Roi de certaines missions de contrôle à une autre autorité, le contrôle des certifications volontaires de cybersécurité est assuré par l'autorité nationale de certification de cybersécurité. Sur base de cet article, l'autorité nationale de certification de cybersécurité peut éventuellement solliciter la collaboration d'une autre autorité qui agirait dans le cadre de ses propres compétences légales de contrôle, afin de l'assister dans ses missions de contrôle.</p>	<p>Tenzij de Koning bepaalde toezichtsoopdrachten aan een andere overheid heeft toegewezen, wordt het toezicht op de vrijwillige cyberbeveiligingscertificeringen uitgeoefend door de nationale cyberbeveiligingscertificeringsautoriteit. Op basis van dit artikel kan de nationale cyberbeveiligingscertificeringsautoriteit eventueel een andere overheid verzoeken om haar voor haar toezichtsoopdrachten bij te staan, en dit in het kader van de eigen wettelijke toezichtsbevoegdheden van laatstgenoemde.</p>
CHAPITRE 3. - Autorité nationale de certification de cybersécurité	HOOFDSTUK 3. - Nationale cyberbeveiligingscertificeringsautoriteit
Section 1^{re}. - Représentation au Groupe européen de certification de cybersécurité	Afdeling 1. - Vertegenwoordiging in de Europese Groep voor cyberbeveiligingscertificering
Article 8	Artikel 8
<p>L'article précise que l'autorité nationale de certification de cybersécurité représentera la Belgique au sein du Groupe européen de certification de cybersécurité (ci-après « GECC ») visé à l'article 62 du Règlement sur la cybersécurité. Le GECC est chargé notamment de conseiller et d'assister la Commission en matière de certification de cybersécurité, d'adopter un avis sur les schémas candidats préparés par l'ENISA (l'agence européenne chargée de la cybersécurité), de demander à l'ENISA de préparer un schéma candidat et de faciliter la coopération entre les autorités nationales de certification de cybersécurité.</p> <p>Lors des discussions relatives à l'adoption d'actes d'exécution liés au Règlement sur la cybersécurité, l'autorité nationale de certification de cybersécurité représentera également la Belgique au cours des réunions visées par le Règlement n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États</p>	<p>Volgens dit artikel zal de nationale cyberbeveiligingscertificeringsautoriteit België vertegenwoordigen in de Europese Groep voor cyberbeveiligingscertificering (hierna "EGC") bedoeld in artikel 62 van de Cyberbeveiligingsverordening. De EGC heeft met name als taak advies en bijstand te verlenen aan de Commissie op het vlak van cyberbeveiligingscertificering, een advies uit te brengen over potentiële regelingen opgesteld door ENISA (het Europees agentschap voor cyberbeveiliging), ENISA te verzoeken potentiële regelingen op te stellen en de samenwerking tussen de nationale cyberbeveiligingscertificeringsautoriteiten te vergemakkelijken.</p> <p>De nationale cyberbeveiligingscertificeringsautoriteit zal België ook vertegenwoordigen tijdens besprekingen voor de vaststelling van uitvoeringshandelingen in verband met de Cyberbeveiligingsverordening op de vergaderingen bedoeld in Verordening nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de</p>

<p>membres de l'exercice des compétences d'exécution par la Commission.</p> <p>Les schémas européens de certification de cybersécurité ont vocation à contribuer à harmoniser les pratiques de cybersécurité au sein de l'Union. Ils doivent contribuer à augmenter le niveau de cybersécurité dans l'Union. La conception des schémas européens de certification de cybersécurité devrait également prendre en compte et permettre la mise au point d'innovations dans le domaine de la cybersécurité.</p> <p>Le deuxième paragraphe souligne que dans le cadre de sa mission de représentation de la Belgique au sein du GECC, l'autorité nationale de certification de cybersécurité se concertera avec les autres autorités publiques concernées (désignées par le Roi), en particulier en ce qui concerne la préparation et l'adoption d'un avis sur un schéma candidat de certification de cybersécurité.</p> <p>Il est, en effet, souhaitable que l'autorité nationale de certification de cybersécurité se concerte au préalable notamment avec les différentes autorités de surveillance du marché, les autorités sectorielles visées par la loi NIS, les entités fédérées ou d'autres autorités publiques qui pourraient être concernées par le schéma de certification européen proposé.</p> <p>La variété des objets sur lesquels pourront porter les propositions de schémas européens de certification de cybersécurité requiert, en outre, une structure flexible de concertation avec les acteurs concernés au niveau national, en fonction de chaque schéma précis.</p> <p>De plus, le paragraphe 3 prévoit que ces autres autorités publiques pourront assister avec l'autorité nationale de certification de cybersécurité aux travaux et réunions du GECC.</p>	<p>algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren.</p> <p>Met Europese cyberbeveiligingscertificeringsregelingen wordt beoogd bij te dragen aan de harmonisatie van cyberbeveiligingspraktijken in de Unie. Zij dienen bij te dragen tot een betere cyberbeveiliging binnen de Unie. Bij het ontwerp van de Europese cyberbeveiligingscertificeringsregelingen moet de ontwikkeling van innovaties op het gebied van cyberbeveiliging in aanmerking worden genomen en mogelijk zijn.</p> <p>De tweede paragraaf wijst erop dat de nationale cyberbeveiligingscertificeringsautoriteit, in het kader van haar opdracht om België in de EGC te vertegenwoordigen, met de andere betrokken (door de Koning aangewezen) overheden overlegt, met name bij de voorbereiding en goedkeuring van een advies over een potentiële cyberbeveiligingscertificeringsregeling.</p> <p>Het is immers wenselijk dat de nationale cyberbeveiligingscertificeringsautoriteit vooraf met name met de verschillende markttoezichtautoriteiten, de sectorale overheden bedoeld in de NIS-wet, de deelgebieden of andere overheden overlegt die betrokken kunnen zijn bij de voorgestelde Europese certificeringsregeling.</p> <p>De verscheidenheid van de zaken waarop voorstellen voor Europese cyberbeveiligingscertificeringsregelingen betrekking kunnen hebben, vereist bovendien een flexibele structuur voor het overleg met de betrokkenen op nationaal niveau, naargelang elke specifieke regeling.</p> <p>Verder bepaalt paragraaf 3 dat deze andere overheden, samen met de nationale cyberbeveiligingscertificeringsautoriteit, de werkzaamheden en vergaderingen van de EGC kunnen bijwonen.</p>
<p>Section 2. - Indépendance</p>	<p>Afdeling 2. - Onafhankelijkheid</p>
<p>Article 9</p>	<p>Artikel 9</p>
<p>Cet article met en œuvre l'article 58, § 3 du Règlement sur la cybersécurité qui impose que chaque autorité nationale de certification de cybersécurité soit indépendante des entités qu'elle surveille en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et son processus décisionnel.</p> <p>La disposition précise les situations de conflits d'intérêts que l'autorité nationale de certification de cybersécurité doit prévenir, identifier et résoudre lors de l'exécution de ses tâches de contrôle et de certification en matière de cybersécurité.</p>	<p>Dit artikel geeft uitvoering aan artikel 58, lid 3, van de Cyberbeveiligingsverordening waaruit blijkt dat elke nationale cyberbeveiligingscertificeringsautoriteit op het vlak van haar organisatie, financieringsbeslissingen, rechtsstructuur en besluitvorming onafhankelijk moet zijn van de entiteiten waarop zij toezicht houdt.</p> <p>De bepaling verduidelijkt welke situaties van belangenconflicten de nationale cyberbeveiligingscertificeringsautoriteit moet voorkomen, identificeren en oplossen bij de uitvoering van haar toezichts- en certificeringstaken op het gebied van cyberbeveiliging.</p>

CHAPITRE 4. - Délivrance des certificats européens	HOOFDSTUK 4. - Afgifte van Europese certificaten
Section 1 ^{re} . - Certificats de cybersécurité européens attestant d'un niveau d'assurance "élémentaire" ou "substantiel"	Afdeling 1. - Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel"
Article 10	Artikel 10
<p>En vertu de l'article 56, § 4 du Règlement sur la cybersécurité, les organismes d'évaluation de la conformité accrédités délivrent les certificats de cybersécurité européens attestant d'un niveau d'assurance dit « élémentaire » ou « substantiel ».</p> <p>Les schémas européens de certification de cybersécurité auront pour finalité de garantir que les produits TIC, services TIC et processus TIC certifiés selon de tels schémas respectent les exigences définies qui visent à protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées, transmises ou traitées, ou des fonctions connexes de ces produits, services et processus tout au long de leur cycle de vie, ou des services qu'ils offrent ou qui sont accessibles par leur intermédiaire.</p> <p>Comme le prévoit l'article 52, § 5 du Règlement sur la cybersécurité, le niveau d'assurance dit « élémentaire » offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels un certificat ou une déclaration de conformité de l'Union européenne est délivré(e) satisfont aux exigences de sécurité correspondantes, y compris les fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques élémentaires connus d'incidents et de cyberattaques.</p> <p>Quant au niveau d'assurance dit « substantiel », l'article 52, § 6 du Règlement sur la cybersécurité dispose qu'il offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels un certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques liés à la cybersécurité connus, et le risque d'incidents et de cyberattaques émanant d'acteurs aux aptitudes et aux ressources limitées.</p> <p>L'article 56, § 5 du même Règlement précise que la délivrance de tels certificats est néanmoins réservée à l'autorité nationale de certification de cybersécurité, lorsque le schéma de certification de cybersécurité l'exige. Pour ce faire et conformément à l'article 60, § 2, du Règlement sur la cybersécurité, l'autorité nationale de certification de cybersécurité devra disposer d'une accréditation délivrée par l'organisme national d'accréditation. L'autorité nationale de certification de cybersécurité peut toutefois déléguer en tout ou en partie cette tâche à un organisme public accrédité en tant qu'organisme d'évaluation de la conformité.</p> <p>L'éventuelle délégation prévue au troisième paragraphe est légalement admissible dès lors qu'elle n'octroie à l'organisme public accrédité en tant qu'organisme</p>	<p>Krachtens artikel 56, lid 4, van de Cyberbeveiligingsverordening geven de geaccrediteerde conformiteitsbeoordelingsinstanties de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel" af.</p> <p>Europese cyberbeveiligingscertificeringsregelingen moeten tot doel hebben te waarborgen dat ICT-producten, -diensten en -processen die door middel van een dergelijke regeling zijn gecertificeerd, voldoen aan gespecificeerde voorschriften met als doel de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die producten, diensten en processen worden aangeboden of toegankelijk zijn, gedurende de levenscyclus ervan te beschermen.</p> <p>Zoals bepaald in artikel 52, lid 5, van de Cyberbeveiligingsverordening biedt het zekerheidsniveau "basis" de zekerheid dat de ICT-producten, -diensten en -processen waarvoor een certificaat of EU-conformiteitsverklaring is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om de bekende basisrisico's van incidenten en cyberaanvallen tot een minimum te beperken.</p> <p>Volgens artikel 52, lid 6, van de Cyberbeveiligingsverordening biedt het zekerheidsniveau "substantieel" de zekerheid dat de ICT-producten, -diensten en -processen waarvoor een certificaat is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om de bekende cyberbeveiligingsrisico's, en het risico op incidenten en cyberaanvallen door actoren met beperkte vaardigheden en middelen, tot een minimum te beperken.</p> <p>Artikel 56, lid 5, van dezelfde Verordening verduidelijkt niettemin dat de afgifte van deze certificaten voorbehouden is aan de nationale cyberbeveiligingscertificeringsautoriteit indien de cyberbeveiligingscertificeringsregeling dit vereist. Overeenkomstig artikel 60, lid 2, van de Cyberbeveiligingsverordening moet de nationale cyberbeveiligingscertificeringsautoriteit daartoe beschikken over een accreditatie die wordt afgegeven door de nationale accreditatie-instantie. De nationale cyberbeveiligingscertificeringsautoriteit kan deze taak echter volledig of gedeeltelijk delegeren aan een</p>

<p>d'évaluation de la conformité aucun pouvoir réglementaire. De plus, cette délégation ne porte que sur une mission technique et spécifique, à savoir la délivrance de certificats de cybersécurité de niveau « élémentaire » ou « substantiel » sur base d'un schéma précis de certification européen.</p>	<p>overheidsinstelling die als conformiteitsbeoordelingsinstantie geaccrediteerd is.</p> <p>De in de derde paragraaf bedoelde eventuele delegatie is wettelijk toegestaan, aangezien ze geen regelgevende bevoegdheid verleent aan de overheidsinstelling die als conformiteitsbeoordelingsinstantie geaccrediteerd is. Bovendien betreft deze delegatie alleen een technische en specifieke opdracht, namelijk de afgifte van cyberbeveiligingscertificaten voor niveau "basis" of "substantieel", op basis van een specifieke Europese certificeringsregeling.</p>
<p>Section 2. - Certificats de cybersécurité européens attestant d'un niveau d'assurance "élevé"</p>	<p>Afdeling 2. - Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog"</p>
<p>Article 11</p>	<p>Artikel 11</p>
<p>En vertu de l'article 56, § 6 du Règlement sur la cybersécurité, une certification européenne de cybersécurité d'un niveau d'assurance dit «élevé» ne peut être délivrée que par l'autorité nationale de certification de cybersécurité ou, éventuellement, en cas de délégation, par un organisme d'évaluation de la conformité. Conformément à l'article 60, § 2, du Règlement sur la cybersécurité, l'autorité nationale de certification de cybersécurité devra obtenir une accréditation auprès de l'organisme national d'accréditation.</p> <p>Le projet énonce ainsi que l'autorité nationale de certification de cybersécurité délivre les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élevé" ou, moyennant une délégation préalable de l'autorité nationale de certification de cybersécurité, un organisme accrédité d'évaluation de la conformité pourrait en tout ou en partie accomplir cette tâche.</p> <p>L'article 56, § 7 du Règlement précise que l'autorité nationale de certification de cybersécurité ou l'organisme d'évaluation de la conformité peuvent obtenir de la personne physique ou morale sollicitant une certification toutes les informations nécessaires pour accorder celle-ci.</p> <p>L'article 52, § 7 du Règlement sur la cybersécurité indique que le niveau d'assurance dit «élevé» offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels un certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser le risque que des cyberattaques de pointe soient menées par des acteurs aux aptitudes solides et aux ressources importantes.</p> <p>L'éventuelle délégation prévue au deuxième paragraphe est, au travers d'un raisonnement similaire à la délégation prévue à l'article 10, légalement admissible dès lors qu'elle n'octroie à l'organisme accrédité d'évaluation de la conformité aucun pouvoir réglementaire. De plus, cette délégation ne porte que sur une mission technique et</p>	<p>Krachtens artikel 56, lid 6, van de Cyberbeveiligingsverordening kan een Europees cyberbeveiligingscertificaat voor zekerheidsniveau "hoog" enkel worden afgegeven door de nationale cyberbeveiligingscertificeringsautoriteit of, eventueel in geval van delegatie, door een conformiteitsbeoordelingsinstantie. Overeenkomstig artikel 60, lid 2, van de Cyberbeveiligingsverordening moet de nationale cyberbeveiligingscertificeringsautoriteit door de nationale accreditatie-instantie worden geaccrediteerd.</p> <p>Zo bepaalt het ontwerp dat de nationale cyberbeveiligingscertificeringsautoriteit de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog" afgeeft, maar dat deze taak, na voorafgaande delegatie door de nationale cyberbeveiligingscertificeringsautoriteit, ook volledig of gedeeltelijk kan worden uitgevoerd door een geaccrediteerde conformiteitsbeoordelingsinstantie.</p> <p>Artikel 56, lid 7, van de Verordening bepaalt dat de nationale cyberbeveiligingscertificeringsautoriteit of de conformiteitsbeoordelingsinstantie alle informatie kan verkrijgen van de natuurlijke of rechtspersoon die een certificering vraagt wanneer die nodig is om deze certificering te verlenen.</p> <p>Volgens artikel 52, lid 7, van de Cyberbeveiligingsverordening biedt het zekerheidsniveau "hoog" de zekerheid dat de ICT-producten, -diensten en -processen waarvoor een certificaat is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om het risico van geavanceerde cyberaanvallen door actoren met aanzienlijke vaardigheden en middelen, tot een minimum te beperken.</p> <p>De eventuele delegatie bedoeld in de tweede paragraaf is, volgens een soortgelijke redenering als de delegatie in artikel 10, wettelijk toegestaan, aangezien ze geen regelgevende bevoegdheid verleent aan de geaccrediteerde conformiteitsbeoordelingsinstantie. Bovendien betreft deze</p>

spécifique, à savoir la délivrance de certificats de cybersécurité de niveau « haut ». Cette mission exige une expertise particulière, l'intérêt de la présente délégation est de permettre à un organisme accrédité d'évaluation de la conformité possédant déjà cette expertise de s'en acquitter.	delegatie slechts een technische en specifieke opdracht, namelijk de afgifte van cyberbeveiligingscertificaten voor niveau "hoog". Deze opdracht vereist een bijzondere expertise. Dankzij deze delegatie kan een geaccrediteerde conformiteitsbeoordelingsinstantie die al over deze expertise beschikt, deze opdracht uitvoeren.
Section 3. - Réclamation en cas de refus de délivrance	Afdeling 3. - Klacht ingeval de afgifte geweigerd wordt
Article 12	Artikel 12
En cas de refus de délivrance du certificat, le demandeur peut introduire une réclamation devant l'autorité nationale de certification de cybersécurité selon les modalités prévues à l'article 29 et suivants.	Ingeval de afgifte van een certificaat geweigerd wordt, kan de aanvrager een klacht indienen bij de nationale cyberbeveiligingscertificeringsautoriteit volgens de modaliteiten bepaald in artikel 29 en volgende.
CHAPITRE 5. - Contrôle	HOOFDSTUK 5. - Toezicht
Ce chapitre énonce les règles relatives aux contrôles du respect par les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens volontaires et les émetteurs de déclarations de conformité de l'Union européenne des règles imposées par le Règlement sur la cybersécurité, la présente loi ou ses arrêtés d'exécution.	Dit hoofdstuk bevat de regels over de controles om na te gaan of de conformiteitsbeoordelingsinstanties, de houders van vrijwillige Europese cyberbeveiligingscertificaten en de afgevers van EU-conformiteitsverklaringen de regels naleven die zijn opgelegd door de Cyberbeveiligingsverordening, deze wet of de uitvoeringsbesluiten ervan.
Article 13	Artikel 13
<p>Cette disposition indique que l'autorité nationale de certification de cybersécurité doit disposer d'un service d'inspection capable de réaliser à tout moment des contrôles du respect des règles relatives au Règlement sur la cybersécurité.</p> <p>L'article 58, § 4 du Règlement exige que les activités de l'autorité nationale de cybersécurité en matière de délivrance de certificats de cybersécurité européens soient strictement distinctes de ses activités de supervision, et à ce que ces deux activités soient exécutées indépendamment l'une de l'autre.</p> <p>Lors de l'accomplissement de ses missions de contrôle, le service d'inspection de l'autorité nationale de cybersécurité sera entièrement autonome des autres départements de cette autorité, notamment du service chargé de la délivrance des certificats.</p> <p>Afin d'assurer cette indépendance fonctionnelle et cette séparation des tâches, le service d'inspection sera doté d'un directeur, de membres du personnel et d'outils propres pour accomplir ses tâches de supervision.</p> <p>Conformément aux articles 58, § 5 et 59, § 2 du Règlement sur la cybersécurité, le service d'inspection doit, afin d'assurer ses missions de contrôle, disposer des moyens humains et budgétaires suffisants.</p> <p>Toutefois, ce service d'inspection pourra faire appel à des experts, lesquels sont soumis également aux règles de</p>	<p>Volgens deze bepaling moet de nationale cyberbeveiligingscertificeringsautoriteit over een inspectiedienst beschikken die op elk ogenblik controles kan uitvoeren om na te gaan of de regels van de Cyberbeveiligingsverordening worden nageleefd.</p> <p>Artikel 58, lid 4, van de Verordening vereist dat de werkzaamheden van de nationale cyberbeveiligingscertificeringsautoriteit met betrekking tot de afgifte van Europese cyberbeveiligingscertificaten strikt gescheiden zijn van haar toezichthoudende werkzaamheden, en dat beide werkzaamheden onafhankelijk van elkaar worden verricht.</p> <p>De inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit vervult zijn toezichtsopdrachten volledig autonoom van de andere departementen van deze autoriteit, met name van de dienst belast met de afgifte van certificaten.</p> <p>Om deze functionele onafhankelijkheid en taakverdeling te garanderen, beschikt de inspectiedienst over een eigen directeur en over eigen personeelsleden en middelen om zijn toezichtstaken te vervullen.</p> <p>Overeenkomstig de artikelen 58, lid 5, en 59, lid 2, van de Cyberbeveiligingsverordening moet de inspectiedienst over voldoende menselijke en budgettaire middelen beschikken om zijn toezichtsopdrachten te vervullen.</p>

<p>l'article 17 de la présente loi, en fonction des caractéristiques propres à chaque schéma européen de certification de cybersécurité.</p> <p>L'autorité nationale pourrait ainsi faire appel à des experts externes, par exemple, des organismes privés, des autorités de surveillance du marché ou des autorités sectorielles. Ces experts disposent également d'une certaine expertise dans le contrôle des produits, services ou processus. Une mise en œuvre combinée des contrôles entre les autorités compétentes en vertu de différentes législations est de nature à renforcer le travail de surveillance du marché, ce qui est aussi explicitement prévu par le Règlement sur la cybersécurité. Ainsi, l'article 58, § 7, a) du Règlement sur la cybersécurité précise bien que les tâches de supervision de l'autorité nationale de certification de cybersécurité doivent être réalisées en coopération avec les autres autorités compétentes de surveillance du marché.</p> <p>Cette disposition permet une collaboration entre l'autorité nationale de certification de cybersécurité et une autre autorité publique lorsque les deux parties y trouvent un intérêt commun. Les experts de l'autorité publique demeureraient attachés à leur service d'origine et se verraient confier, avec l'accord de cette dernière, des tâches ponctuelles d'assistance pour les services de l'autorité nationale de certification de cybersécurité.</p> <p>Les frais d'experts externes requis par le service d'inspection peuvent être mis à charge des organismes d'évaluation de la conformité, les titulaires de certificat de cybersécurité européen ou les émetteurs de déclaration de conformité de l'Union européenne dès lors que, d'une part, ces derniers sollicitent volontairement une autorisation ou une certification, et d'autre part, ces derniers pourraient en tirer un avantage pécuniaire ou commercial.</p>	<p>Deze inspectiedienst kan echter een beroep doen op experten, die ook onderworpen zijn aan de regels van artikel 17 van deze wet, naargelang de specifieke kenmerken van elke Europese cyberbeveiligingscertificeringsregeling.</p> <p>Zo kan de nationale autoriteit een beroep doen op externe experten, bijvoorbeeld van privé-instanties, markttoezichtautoriteiten of sectorale overheden. Deze experten beschikken ook over een bepaalde expertise inzake de controle van producten, diensten of processen. De combinatie van controles door de krachtens verschillende wetgevingen bevoegde autoriteiten kan het markttoezicht versterken, wat ook uitdrukkelijk bepaald is in de Cyberbeveiligingsverordening. Zo verduidelijkt artikel 58, lid 7, a), van de Cyberbeveiligingsverordening dat de nationale cyberbeveiligingscertificeringsautoriteit haar toezichtstaken moet vervullen in samenwerking met de andere betrokken markttoezichtautoriteiten.</p> <p>Deze bepaling biedt de mogelijkheid tot samenwerking tussen de nationale cyberbeveiligingscertificeringsautoriteit en een andere overheid wanneer beide partijen daar belang bij hebben. De experten van de overheid zouden verbonden blijven aan hun dienst van oorsprong en, met het akkoord van deze overheid, belast worden met specifieke bijstandstaken voor de diensten van de nationale cyberbeveiligingscertificeringsautoriteit.</p> <p>De kosten voor externe experten die door de inspectiedienst worden opgeroepen, kunnen ten laste worden gelegd van de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen, aangezien die laatsten enerzijds zelf een toelating of certificering aanvragen en daar anderzijds een financieel of commercieel voordeel uit kunnen halen.</p>
Article 14	Artikel 14
<p>Cet article prévoit la coopération et l'assistance entre le service d'inspection et les autorités nationales de certification de cybersécurité compétentes d'autres États de l'Union européenne lorsqu'un organisme d'évaluation de la conformité, un titulaire de certificat de cybersécurité européen volontaire ou un émetteur de déclaration de conformité est situé en dehors du territoire belge.</p> <p>Ces mesures peuvent, par exemple, porter sur des échanges d'informations et sur des demandes de mesures de contrôle.</p>	<p>Volgens dit artikel is samenwerking en bijstand toegestaan tussen de inspectiedienst en de bevoegde nationale cyberbeveiligingscertificeringsautoriteiten van andere landen van de Europese Unie wanneer een conformiteitsbeoordelingsinstantie, een houder van een vrijwillig Europees cyberbeveiligingscertificaat of een afgever van een EU-conformiteitsverklaring zich buiten het Belgische grondgebied bevindt.</p> <p>Deze maatregelen kunnen bijvoorbeeld betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen.</p>
Article 15	Artikel 15
<p>Les membres du service d'inspection doivent porter une carte de légitimation dont le modèle sera fixé par le Roi.</p> <p>L'article porte également sur les conflits d'intérêts pouvant concerner les inspecteurs et leur prestation de serment.</p>	<p>De leden van de inspectiedienst moeten een legitimatiekaart bij zich hebben waarvan het model door de Koning wordt bepaald.</p>

<p>Le service d'inspection dispose de larges pouvoirs afin d'effectuer des contrôles approfondis du respect du Règlement sur la cybersécurité et de la présente loi.</p> <p>Les membres du service d'inspection peuvent notamment pénétrer sans avertissement préalable dans tous les locaux utilisés par l'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen volontaire ou l'émetteur de déclaration de conformité de l'Union européenne.</p> <p>Les membres du service d'inspection peuvent pénétrer dans les locaux habités moyennant une autorisation préalable d'un juge d'instruction.</p> <p>Il est précisé également les règles à respecter en cas d'audition et sur les données consultables.</p> <p>Le service d'inspection dispose de larges pouvoirs afin d'effectuer des contrôles approfondis du respect du Règlement sur la cybersécurité et de la présente loi.</p> <p>Par ailleurs, lorsque cela s'avère nécessaire pour leurs missions de contrôle, les membres du service d'inspection devront disposer de l'habilitation de sécurité correspondant au niveau de classification, au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, des informations auxquelles ils doivent avoir accès.</p>	<p>Het artikel handelt ook over mogelijke belangenconflicten met betrekking tot inspecteurs en over hun eedaflegging.</p> <p>De inspectiedienst beschikt over ruime bevoegdheden om grondige controles uit te voeren op de naleving van de Cyberbeveiligingsverordening en deze wet.</p> <p>De leden van de inspectiedienst mogen met name zonder voorafgaande verwittiging alle lokalen betreden die gebruikt worden door de conformiteitsbeoordelingsinstantie, de houder van een vrijwillig Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring.</p> <p>De leden van de inspectiedienst mogen de bewoonde lokalen betreden mits voorafgaande machtiging van een onderzoeksrechter.</p> <p>Tevens komen de na te leven regels aan bod in geval van een verhoor en met betrekking tot de gegevens die mogen worden geraadpleegd.</p> <p>De inspectiedienst beschikt over ruime bevoegdheden om grondige controles uit te voeren op de naleving van de Cyberbeveiligingsverordening en deze wet.</p> <p>Bovendien moeten de leden van de inspectiedienst, indien dit nodig is voor hun toezichtopdrachten, over de veiligheidsmachtiging beschikken die overeenstemt met het classificatieniveau, als bedoeld in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, van de informatie waar zij toegang toe moeten hebben.</p>
Article 16	Artikel 16
<p>Le rapport d'inspection est transmis à l'organisme d'évaluation de la conformité, au titulaire de certificat de cybersécurité européen ou à l'émetteur de déclaration de conformité de l'Union européenne inspecté.</p> <p>Ce rapport pourra également être communiqué à d'autres autorités, à leur demande, si cette dernière est effectuée dans le cadre de leurs compétences légales.</p> <p>Les administrations concernées adopteront des protocoles avec l'autorité nationale de certification de cybersécurité afin de faciliter ou d'automatiser ces échanges de documents.</p> <p>A titre dérogatoire, lorsque des contrôles sont effectués auprès d'une infrastructure critique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens 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, le rapport prévu au paragraphe 1^{er}</p>	<p>Het inspectieverslag wordt bezorgd aan de geïnspecteerde conformiteitsbeoordelingsinstantie, houder van een Europees cyberbeveiligingscertificaat of afgever van een EU-conformiteitsverklaring.</p> <p>Op verzoek van andere overheden en voor zover dit gebeurt in het kader van hun wettelijke bevoegdheden, kan dit verslag ook aan deze overheden worden bezorgd.</p> <p>De betrokken administraties sluiten protocollen met de nationale cyberbeveiligingscertificeringsautoriteit om deze uitwisseling van documenten te vergemakkelijken of te automatiseren.</p> <p>Indien controles worden uitgevoerd bij een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of in het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, bij een aanbieder van essentiële diensten of een digitaal dienstverlener als bedoeld in 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, wordt het</p>

est automatiquement transmis à l'autorité sectorielle compétente.	verslag bedoeld in paragraaf 1, bij wijze van afwijking, automatisch aan de bevoegde sectorale overheid bezorgd.
Article 17	Artikel 17
<p>Cet article règle le sort de toute information récoltée par le service d'inspection dans le cadre de ses missions. Il est impératif de limiter l'accès à ces informations par d'autres personnes à ce qui est nécessaire pour l'exécution de leurs missions en rapport avec la présente loi ou d'autres dispositions légales : par exemple, la loi du 9 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (loi NIS), la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, le Règlement (UE) n°910/2014 (e-IDAS), le Règlement (UE) n°2016/679 (RGPD) etc., ainsi que de tenir les membres du personnel du service d'inspection au secret professionnel. En effet, une absence de garanties suffisantes quant au traitement confidentiel des informations fournies au service d'inspection dans le cadre de sa mission de contrôle risquerait de décourager les entreprises qui voudraient avoir recours à des certifications volontaires de cybersécurité.</p> <p>Bien entendu, les membres du personnel des autres services de l'autorité nationale de cybersécurité sont tenus au respect de leurs obligations statutaires ou contractuelles en matière de confidentialité.</p> <p>Le procès-verbal, établi suite à un contrôle, peut, à la demande d'une autorité, pour autant que cette demande soit faite dans le cadre de ses compétences légales, lui être transmis par l'autorité nationale de certification de cybersécurité ou l'autorité à laquelle le Roi aura attribué certaines missions de contrôle conformément à l'article 5, § 2.</p> <p>Les administrations concernées adopteront des protocoles avec l'autorité nationale de certification de cybersécurité afin de faciliter ou d'automatiser ces échanges de documents. La demande de transmission des documents peut être générale en fonction du type d'entité concernée.</p> <p>Il s'agit ici des autorités qui ne sont pas des autorités sectorielles ou des services d'inspection pour les infrastructures critiques, les opérateurs de services essentiels et les fournisseurs de services numériques.</p> <p>L'autorité nationale de certification de cybersécurité transmet automatiquement à l'autorité sectorielle concernée les informations relatives à un contrôle, en ce compris le procès-verbal, effectué auprès d'une infrastructure critique, d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou 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.</p>	<p>Dit artikel bevat de regeling voor alle informatie die de inspectiedienst in het kader van zijn opdrachten verzamelt. Het is absoluut noodzakelijk dat de toegang van andere personen tot deze informatie wordt beperkt tot hetgeen noodzakelijk is voor de uitvoering van hun opdrachten in verband met deze wet of andere wettelijke bepalingen: bijvoorbeeld de wet van 9 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS-wet), de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur, Verordening (EU) nr. 910/2014 (e-IDAS), Verordening (EU) 2016/679 (AVG), enz., en dat de personeelsleden van de inspectiedienst aan het beroepsgeheim gebonden zijn. Het ontbreken van voldoende waarborgen met betrekking tot de vertrouwelijke behandeling van de informatie die aan de inspectiedienst wordt verstrekt in het kader van de toezichtsovereenkomst van die laatste, kan ondernemingen er immers van weerhouden gebruik te maken van vrijwillige cyberbeveiligingscertificeringen.</p> <p>Uiteraard moeten de personeelsleden van de andere diensten van de nationale cyberbeveiligingscertificeringsautoriteit hun statutaire of contractuele verplichtingen inzake vertrouwelijkheid nakomen.</p> <p>Het na een controle opgestelde proces-verbaal kan door de nationale cyberbeveiligingscertificeringsautoriteit of de overheid waaraan de Koning bepaalde toezichtsovereenkomsten heeft toegekend overeenkomstig artikel 5, § 2, worden bezorgd aan een overheid, op verzoek van laatstgenoemde en voor zover dit verzoek kadert in haar wettelijke bevoegdheden.</p> <p>De betrokken administraties sluiten protocollen met de nationale cyberbeveiligingscertificeringsautoriteit om deze uitwisseling van documenten te vergemakkelijken of te automatiseren. Het verzoek om documenten over te maken kan algemeen zijn naargelang het soort betrokken entiteit.</p> <p>Het betreft hier overheden die geen sectorale overheden of inspectiediensten zijn voor kritieke infrastructuur, aanbieders van essentiële diensten en digitaaldienstverleners.</p> <p>De nationale cyberbeveiligingscertificeringsautoriteit bezorgt de betrokken sectorale overheid automatisch de informatie, met inbegrip van het proces-verbaal, over een controle bij een kritieke infrastructuur, aanbieder van essentiële diensten of digitaaldienstverlener als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur of de wet van 7</p>

<p>L'autorité sectorielle compétente pourra transmettre, le cas échéant, les informations aux services de sécurité et de renseignement.</p> <p>A l'instar de l'article 16, § 2, les protocoles conclus entre l'autorité nationale de certification de cybersécurité et les autorités sectorielles préciseront les modalités pratiques de partage de ces procès-verbaux.</p> <p>Le paragraphe 5 énumère, quant à lui, les actions permettant l'accès aux informations relatives à l'exécution des missions du chapitre 5 que les membres du service d'inspection peuvent entreprendre en matière de communications électroniques.</p>	<p>april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.</p> <p>In voorkomend geval kan de bevoegde sectorale overheid de informatie aan de veiligheids- en inlichtingendiensten bezorgen.</p> <p>Naar analogie van artikel 16, § 2, bepalen de protocollen gesloten tussen de nationale cyberbeveiligingscertificeringsautoriteit en de sectorale overheden de praktische modaliteiten voor het delen van deze processen-verbaal.</p> <p>Paragraaf 5 somt de handelingen op die de leden van de inspectiedienst mogen ondernemen inzake elektronische communicatie om toegang te krijgen tot informatie met betrekking tot de uitvoering van de opdrachten in hoofdstuk 5.</p>
Article 18	Artikel 18
<p>Cette disposition porte sur la collaboration entre les personnes visées par une inspection et le service d'inspection ou les experts.</p> <p>Le Roi peut déterminer des rétributions relatives à la délivrance et aux prestations d'inspections. Il s'agit, en effet, de prévoir la possibilité, le cas échéant, de couvrir les frais assumés par le service d'inspection de l'autorité nationale de certification de cybersécurité en raison des certifications européennes volontaires accordées en Belgique (frais d'expert, frais de personnel, frais administratifs, etc.).</p>	<p>Deze bepaling heeft betrekking op de samenwerking tussen de personen die aan een inspectie worden onderworpen en de inspectiedienst of de experts.</p> <p>De Koning kan retributies bepalen voor de afgifte en de inspectieprestaties. Het is immers de bedoeling te voorzien in de mogelijkheid om, in voorkomend geval, de kosten te dekken die de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit maakt in het kader van vrijwillige Europese certificeringen die in België worden toegekend (kosten voor experts, personeelskosten, administratieve kosten, enz.).</p>
CHAPITRE 6. - Sanctions	HOOFDSTUK 6. - Sancties
Section 1^{re}. - Procédure	Afdeling 1. - Procedure
Article 19	Artikel 19
<p>L'article prévoit une mise en demeure préalable en cas de manquement constaté par le service d'inspection.</p> <p>Préalablement à cette mise en demeure, le contrevenant est informé de l'intention du service d'inspection de le mettre en demeure.</p>	<p>Het artikel voorziet in een voorafgaande ingebrekestelling ingeval de inspectiedienst een inbreuk vaststelt.</p> <p>Vóór deze ingebrekestelling deelt de inspectiedienst de overtreder mee dat hij van plan is hem in gebreke te stellen.</p>
Article 20	Artikel 20
<p>Cette disposition porte sur le constat du non-respect des obligations découlant de la loi ou du Règlement sur la cybersécurité. Ainsi, même si le contrevenant se conforme à la mise en demeure adressée par le service d'inspection, cela n'empêche pas la rédaction d'un procès-verbal et l'imposition d'une sanction à son encontre.</p> <p>Les procès-verbaux font foi jusqu'à preuve du contraire.</p>	<p>Deze bepaling heeft betrekking op de vaststelling dat de verplichtingen van de wet of de Cyberbeveiligingsverordening niet zijn nagekomen. Zelfs als de overtreder gevolg geeft aan de ingebrekestelling van de inspectiedienst, kan een proces-verbaal worden opgesteld en een sanctie worden opgelegd.</p> <p>De processen-verbaal hebben bewijskracht tot het tegendeel is bewezen.</p>

Section 2. - Retrait d'un certificat	Afdeling 2. - Intrekking van een certificaat
Article 21	Artikel 21
<p>En cas de non-respect du Règlement sur la cybersécurité ou d'un schéma européen de certification de cybersécurité, l'autorité nationale de certification de cybersécurité peut retirer un certificat de cybersécurité.</p> <p>L'article 58, 8, e) du Règlement sur la cybersécurité précise bien que l'autorité de certification de cybersécurité peut retirer les certificats de cybersécurité européens délivrés lorsque de tels certificats ne respectent pas ledit Règlement ou un schéma européen de certification de cybersécurité.</p>	<p>Ingeval de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet wordt nageleefd, kan de nationale cyberbeveiligingscertificeringsautoriteit een cyberbeveiligingscertificaat intrekken.</p> <p>Volgens artikel 58, 8, e) van de Cyberbeveiligingsverordening kan de cyberbeveiligingscertificeringsautoriteit afgegeven Europese cyberbeveiligingscertificaten intrekken als ze niet voldoen aan deze verordening of aan een Europese cyberbeveiligingscertificeringsregeling.</p>
Section 3. - Limitation, suspension ou retrait d'une autorisation ou d'une délégation	Afdeling 3. - Beperken, opschorten of intrekken van een toelating of een delegatie
Article 22	Artikel 22
<p>Les autorisations accordées aux organismes d'évaluation de la conformité en vertu de l'article 60, § 3, du Règlement sur la cybersécurité ainsi que les délégations effectuées en vertu des articles 10 et 11 peuvent être limitées, suspendues ou retirées par l'autorité nationale de certification de cybersécurité.</p>	<p>De nationale cyberbeveiligingscertificeringsautoriteit kan toelatingen die krachtens artikel 60, § 3, van de Cyberbeveiligingsverordening aan conformiteitsbeoordelingsinstanties zijn verleend en delegaties die krachtens de artikelen 10 en 11 zijn verleend, beperken, opschorten of intrekken.</p>
Section 4. - Amendes administratives	Afdeling 4. - Administratieve geldboetes
<p>Cette section prévoit le principe et le montant des amendes administratives, règle la prise en charge des frais éventuels d'expertise et le recours.</p> <p>L'article 65 du Règlement sur la cybersécurité prévoit que les violations des règles prévues par le Règlement et par les schémas européens de certification de cybersécurité doivent faire l'objet de sanctions. Comme le précise cet article, les sanctions doivent être effectives, proportionnées et dissuasives.</p> <p>Si le retrait de la certification constitue une forme de sanction, il est nécessaire que l'autorité de certification de cybersécurité dispose également d'une gamme plus étendue et plus dissuasive d'instruments de sanction que le seul retrait de la certification.</p> <p>Bien entendu, si les sanctions doivent être dissuasives, elles doivent également être proportionnées. La décision d'imposer une sanction doit être motivée et l'amende en elle-même doit être proportionnelle à la gravité, à la durée, aux moyens utilisés, aux dommages causés et aux circonstances de fait.</p> <p>Chaque Etat membre de l'Union européenne doit, d'ailleurs, informer la Commission du régime de sanction et des mesures ainsi prises, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.</p> <p>Cette section prévoit une compétence de pleine juridiction pour la Cour des marchés, en ce qui concerne les recours des</p>	<p>Deze afdeling vermeldt het principe en het bedrag van de administratieve geldboetes, regelt de tenlasteneming van eventuele expertisecosten en het beroep.</p> <p>Volgens artikel 65 van de Cyberbeveiligingsverordening moeten inbreuken op de regels van de Verordening en van de Europese cyberbeveiligingscertificeringsregelingen aanleiding geven tot sancties. Zoals verduidelijkt in dit artikel moeten de sancties doeltreffend, evenredig en afschrikkend zijn.</p> <p>Als de intrekking van de certificering een vorm van sanctie is, moet de cyberbeveiligingscertificeringsautoriteit ook over een bredere en meer afschrikkende waaier aan sanctie-instrumenten beschikken dan de loutere intrekking van de certificering.</p> <p>Om afschrikkend te zijn, moeten de sancties uiteraard ook evenredig zijn. De beslissing om een sanctie op te leggen moet gemotiveerd worden en de geldboete zelf moet in verhouding staan tot de ernst, duur, gebruikte middelen, veroorzaakte schade en feitelijke omstandigheden.</p> <p>Iedere lidstaat van de Europese Unie moet de Commissie overigens in kennis stellen van de sanctieregeling en de genomen maatregelen alsook van alle eventuele latere wijzigingen aan deze regeling of maatregelen.</p> <p>Deze afdeling voorziet in volle rechtsmacht voor het Marktenhof wat betreft beroepsprocedures tegen</p>

<p>décisions de sanctions de l'autorité nationale de certification de cybersécurité prises en vertu du chapitre 6.</p> <p>Cette Cour a été choisie car elle constitue déjà une juridiction compétente pour des recours similaires prévus par d'autres législations, telles que la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, 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 (loi NIS) ou encore la loi du 3 décembre 2017 portant création de l'Autorité de protection des données. De plus, il s'agit d'une juridiction spécialisée qui sera à même de fournir l'expertise requise.</p>	<p>sanctiebeslissingen die de nationale cyberbeveiligingscertificeringsautoriteit krachtens hoofdstuk 6 heeft genomen.</p> <p>Dit Hof werd als rechtscollege gekozen omdat het al bevoegd is voor soortgelijke beroepsprocedures waarin andere wetgevingen voorzien, zoals de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, 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 (NIS-wet) of nog de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Bovendien is het een gespecialiseerd rechtscollege dat de vereiste expertise kan inbrengen.</p>
CHAPITRE 7. - Réclamations	HOOFDSTUK 7. - Klachten
Section 1^{re}. - Saisine de l'autorité nationale de certification de cybersécurité	Afdeling 1. - Aanhangigmaking bij de nationale cyberbeveiligingscertificeringsautoriteit
<p>Cette section prévoit les modalités de saisine de l'autorité nationale de certification de cybersécurité pour statuer sur les réclamations en rapport avec un certificat de cybersécurité européen, un refus de délivrance d'un certificat ou une déclaration de conformité de l'Union européenne.</p> <p>Conformément à l'article 21, l'autorité nationale de certification de cybersécurité peut notamment retirer un certificat de cybersécurité lorsque le bénéficiaire ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité. L'autorité nationale de certification de cybersécurité peut également limiter, suspendre ou retirer les autorisations et délégations qu'elle a accordées aux organismes d'évaluation de la conformité, comme le prévoit l'article 22.</p>	<p>Deze afdeling bepaalt de nadere regels om klachten over een Europees cyberbeveiligingscertificaat, de weigering om een certificaat af te geven of een EU-conformiteitsverklaring aanhangig te maken bij de nationale cyberbeveiligingscertificeringsautoriteit.</p> <p>Overeenkomstig artikel 21 kan de nationale cyberbeveiligingscertificeringsautoriteit een cyberbeveiligingscertificaat met name intrekken als de begunstigde de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft. Zoals bepaald in artikel 22 kan de nationale cyberbeveiligingscertificeringsautoriteit ook toelatingen en delegaties die ze aan conformiteitsbeoordelingsinstanties heeft verleend, beperken, opschorten of intrekken.</p>
Section 2. Recours	Afdeling 2. Beroepen
Article 35	Artikel 35
<p>Comme le prévoit l'article 64 du Règlement sur la cybersécurité, les personnes physiques ou morales disposent d'un droit de recours juridictionnel effectif en ce qui concerne les décisions prises par l'autorité nationale de certification de cybersécurité ou par l'organisme d'évaluation de la conformité accrédité, en ce qui concerne la délivrance non justifiée, la non-délivrance ou la reconnaissance d'un certificat de cybersécurité européen détenu par ces personnes physiques ou morales, ainsi qu'en l'absence de réaction suite à une réclamation.</p> <p>A cette fin, cet article instaure une compétence de pleine juridiction pour la Cour des marchés.</p> <p>Cette Cour a été choisie car elle constitue déjà une juridiction compétente pour des recours similaires prévus par d'autres législations, telles que la loi du 2 août 2002 relative à la</p>	<p>Volgens artikel 64 van de Cyberbeveiligingsverordening hebben natuurlijke en rechtspersonen recht op een doeltreffende voorziening in rechte met betrekking tot besluiten van de nationale cyberbeveiligingscertificeringsautoriteit of de geaccrediteerde conformiteitsbeoordelingsinstantie betreffende de onjuiste afgifte, het nalaten van afgifte of de erkenning van een Europees cyberbeveiligingscertificaat dat door die natuurlijke of rechtspersonen wordt gehouden, en met betrekking tot het verzuim om gevolg te geven aan een klacht.</p> <p>Daartoe voorziet dit artikel in volle rechtsmacht voor het Marktenhof.</p> <p>Dit Hof werd als rechtscollege gekozen omdat het al bevoegd is voor soortgelijke beroepsprocedures waarin andere</p>

surveillance du secteur financier et aux services financiers, 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 (loi NIS) ou encore la loi du 3 décembre 2017 portant création de l'Autorité de protection des données. De plus, il s'agit d'une juridictions spécialisée qui sera à même de fournir l'expertise requise.	wetgevingen voorzien, zoals de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, 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 (NIS-wet) of nog de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Bovendien is het een gespecialiseerd rechtscollege dat de vereiste expertise kan inbrengen.
CHAPITRE 8. - Dispositions finales	HOOFDSTUK 8. - Slotbepalingen
Section 1^{re}. - Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges	Afdeling 1. - Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector
Article 36	Artikel 36
L'article 36 insère, au sein de l'article 14, § 1, un 7° afin que l'Institut belge des services postaux et des télécommunications puisse exercer les missions de contrôle lui étant éventuellement confiées par le Roi conformément à l'article 5, § 2 de la loi.	Artikel 36 voegt, in artikel 14, § 1, een punt 7° in zodat het Belgisch Instituut voor postdiensten en telecommunicatie de toezichtsoverdrachten kan uitoefenen die hem eventueel zijn toevertrouwd door de Koning overeenkomstig artikel 5, § 2, van de wet.
Article 37	Artikel 37
Cette disposition clarifie le fait que la sécurité des réseaux et des systèmes d'information fait partie de la notion de sécurité publique afin de s'assurer que l'Institut belge des services postaux et des télécommunications puisse communiquer des informations confidentielles à l'autorité nationale de certification de cybersécurité. L'article 14, § 2, 3° de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges énumère les autorités avec lesquelles les membres du Conseil et les membres du personnel de l'Institut belge des services postaux et des télécommunications peuvent communiquer des informations confidentielles dont ils ont eu connaissance dans le cadre de l'exercice de leur fonction. L'institut peut ainsi communiquer de telles informations aux services publics compétents en matière de sécurité publique.	Deze bepaling verduidelijkt dat de beveiliging van netwerk- en informatiesystemen onder het begrip "openbare veiligheid" valt om te garanderen dat het Belgisch Instituut voor postdiensten en telecommunicatie vertrouwelijke informatie kan meedelen aan de nationale cyberbeveiligingscertificeringsautoriteit. Artikel 14, § 2, 3°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector somt de overheden op waarmee de leden van de Raad en de personeelsleden van het Belgisch Instituut voor postdiensten en telecommunicatie vertrouwelijke informatie waarvan ze kennis hebben gekregen in het kader van de uitoefening van hun functie mogen uitwisselen. Zo mag het Instituut deze informatie meedelen aan de openbare diensten die bevoegd zijn voor openbare veiligheid.
Section 2. - Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers	Afdeling 2. - Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten
Article 38	Artikel 38
Cette disposition met en place le régime dérogatoire à l'article 5, §§ 2 à 4 prévu en combinaison de l'article 3, § 5, auquel il est fait référence au commentaire de ce dernier. Cette disposition insère à l'article 45 de la loi organique de la FSMA un paragraphe 6 habilitant le Roi, à la demande de la FSMA et en fonction de l'objet du schéma de certification de	Deze bepaling voert de afwijkende regeling van artikel 5, §§ 2 tot 4, in, die geldt in combinatie met artikel 3, § 5, en waarnaar wordt verwezen in de toelichting bij dit laatste artikel. Deze bepaling voegt in artikel 45 van de organieke wet van de FSMA een paragraaf 6 in, die de Koning machtigt om, op

cybersécurité concerné, à confier à la FSMA les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, en matière de contrôle et de sanctions des certifications européennes volontaires de cybersécurité de l'autorité nationale de certification de cybersécurité, à condition que la FSMA dispose de l'expertise requise. Dans cette hypothèse, le Roi sollicite l'avis et se consulte au préalable avec l'autorité visée à l'article 5, § 1er de la loi précitée et la FSMA. Cette autorité n'exerce ces missions de contrôle qu'envers les entités visées au paragraphe § 1er, 2° de l'article 45 de sa loi organique.	verzoek van de FSMA en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling, de toezichts- en sanctieopdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, die de nationale cyberbeveiligingscertificeringsautoriteit met betrekking tot vrijwillige Europese cyberbeveiligingscertificeringen vervult, toe te vertrouwen aan de FSMA, op voorwaarde dat laatstgenoemde over de vereiste expertise beschikt. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de FSMA. Deze autoriteit vervult die toezichtopdrachten enkel ten aanzien van de entiteiten bedoeld in paragraaf § 1, 2°, van artikel 45 van haar organieke wet.
Article 39	Artikel 39
Cet article vise à insérer une disposition dans la loi organique de la FSMA, afin de lui permettre de communiquer les informations confidentielles dont elle dispose à l'autorité nationale de certification de cybersécurité ou à une autre autorité désignée par le Roi, lorsque cela est nécessaire à l'application de la présente loi.	Dit artikel heeft tot doel een bepaling in te voegen in de organieke wet van de FSMA, waardoor deze de vertrouwelijke informatie waarover zij beschikt kan delen met de nationale cyberbeveiligingscertificeringsautoriteit of een andere door de Koning aangewezen overheid indien dit nodig is voor de toepassing van deze wet.
Section 3. - Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique	Afdeling 3. - Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België
Article 40	Artikel 40
Cette disposition met en place le régime dérogatoire à l'article 5, §§ 2 à 4 prévu en combinaison de l'article 3, § 5 auquel il est fait référence au commentaire de ce dernier. L'article 40 insère un article 36/48/1. Ce qui a été exposé au commentaire de l'article 38 est applicable <i>mutatis mutandis</i> au régime institué par cet article, à la différence que la Banque nationale de Belgique n'exerce les missions de contrôle dont il est question qu'envers les entités sur lesquelles elle exerce le contrôle en vertu des articles 8 et 12bis de sa loi organique et des lois particulières relatives au contrôle des établissements financiers.	Deze bepaling voert de afwijkende regeling van artikel 5, §§ 2 tot 4, in, die geldt in combinatie met artikel 3, § 5, en waarnaar wordt verwezen in de toelichting bij dit laatste artikel. Artikel 40 voegt een artikel 36/48/1 in. De toelichting bij artikel 38 is <i>mutatis mutandis</i> van toepassing op de regeling die door dit artikel wordt ingevoerd, met dit verschil dat de Nationale Bank van België de betrokken toezichtopdrachten enkel vervult ten aanzien van de entiteiten waarop zij toezicht uitoefent krachtens de artikelen 8 en 12bis van haar organieke wet en de bijzondere wetten betreffende het toezicht op de financiële instellingen.
Article 41	Artikel 41
Cet article vise à insérer une disposition dans la loi organique de la Banque nationale de Belgique, afin de lui permettre de communiquer les informations confidentielles dont elle dispose à l'autorité nationale de certification de cybersécurité ou à une autre autorité désignée par le Roi, lorsque cela est nécessaire à l'application de la présente loi.	Dit artikel heeft tot doel een bepaling in te voegen in de organieke wet van de Nationale Bank van België, waardoor deze de vertrouwelijke informatie waarover zij beschikt kan delen met de nationale cyberbeveiligingscertificeringsautoriteit of een andere door de Koning aangewezen overheid indien dit nodig is voor de toepassing van deze wet.
Section 4. Modifications du Code de droit économique	Afdeling 4. - Wijzigingen van het Wetboek van Economisch recht

Article 42	Artikel 42
Cet article vise à insérer une disposition dans le Code de droit économique afin que les termes “règlement sur la cybersécurité” puissent y être régulièrement employés par la suite.	Dit artikel heeft tot doel een bepaling in te voegen in het Wetboek van economisch recht, zodat de term “Cyberbeveiligingsverordening” daarna regelmatig kan worden gebruikt.
Article 43	Artikel 43
Cet article vise à insérer dans le livre XV du Code de droit économique, les dispositions relatives aux compétences du SPF Economie en matière de certification de cybersécurité volontaire et de certification de cybersécurité rendue obligatoire en vertu du droit de l’Union ou du droit national.	Dit artikel heeft tot doel in boek XV van het Wetboek van economisch recht de bepalingen in te voegen betreffende de bevoegdheden van de FOD Economie inzake de vrijwillige cyberbeveiligingscertificering en inzake de cyberbeveiligingscertificering die verplicht is op grond van de Europese of nationale wetgeving.
Article 44	Artikel 44
Cet article vise à insérer dans le livre XV du Code de droit économique, les dispositions relatives aux compétences du SPF Economie en matière de certification de cybersécurité volontaire.	Dit artikel heeft tot doel in boek XV van het Wetboek van economisch recht de bepalingen in te voegen betreffende de bevoegdheden van de FOD Economie inzake de vrijwillige cyberbeveiligingscertificering.
Article 45	Artikel 45
<p>L’article XV.30/3 précise que en matière de certification européenne de cybersécurité volontaire, le Roi peut confier, par arrêté délibéré en Conseil des ministres, certaines missions de contrôle et de sanction en matière de certification de cybersécurité (les missions visées aux chapitres 5 et 6 de la loi), à l’exception des articles 21 et 22, à des agents du SPF Economie moyennant plusieurs conditions cumulatives à savoir : le SPF Economie doit en avoir exprimé la demande, le Roi doit solliciter l’avis de l’autorité nationale de certification de cybersécurité et enfin, le SPF Economie doit disposer de l’expertise requise.</p> <p>Dans la mesure où il est dérogé à l’article 5, §§ 2 à 4, le Roi pourra également déterminer s’il entend confier ces missions aux agents du SPF Economie en procédant par schéma de certification de cybersécurité ou par toute autre forme (par exemple par entités ou produits faisant déjà l’objet d’une surveillance de la part du SPF Economie, etc.).</p> <p>Cette attribution de compétences à des agents du SPF Économie n’est possible que dans la mesure où cette attribution est cohérente avec les compétences déjà détenues par le SPF Économie en vertu du Code de droit économique, de ses arrêtés d’exécution ou des règlements européens.</p>	<p>Artikel XV.30/3 bepaalt dat op het gebied van vrijwillige Europese cyberbeveiligingscertificering, de Koning, bij besluit waarover overleg wordt gepleegd in de Ministerraad, bepaalde controletaken en de sanctionering op het gebied van de certificering van de cyberbeveiliging (de taken bedoeld in de hoofdstukken 5 en 6 van de wet) kan toevertrouwen aan ambtenaren van de FOD Economie, mits aan verschillende cumulatieve voorwaarden wordt voldaan: de FOD Economie moet het verzoek hebben geformuleerd, de Koning moet het advies inwinnen van de nationale certificeringsinstantie voor cyberbeveiliging en, tenslotte, moet de FOD Economie over de vereiste deskundigheid beschikken.</p> <p>Voor zover afgeweken wordt van artikel 5, §§ 2 tot 4, kan de Koning ook bepalen of hij deze taken wil toevertrouwen aan ambtenaren van de FOD Economie door te werk te gaan via een certificeringsregeling inzake cyberbeveiliging of via een andere vorm (bijvoorbeeld door entiteiten of producten die reeds onderworpen zijn aan het toezicht van de FOD Economie, etc.).</p> <p>Deze toewijzing van bevoegdheden aan ambtenaren van de FOD Economie is slechts mogelijk voor zover ze aansluit bij de bevoegdheden waarover de FOD Economie al beschikt krachtens het Wetboek van economisch recht, de uitvoeringsbesluiten ervan of Europese verordeningen.</p>
Article 46	Artikel 46
Cet article vise à insérer dans le livre XV du Code de droit économique, les dispositions relatives aux compétences du	Dit artikel heeft tot doel in boek XV van het Wetboek van economisch recht de bepalingen in te voegen betreffende de

SPF Economie en matière de certification de cybersécurité obligatoire.	bevoegdheden van de FOD Economie inzake de verplichte cyberbeveiligingscertificering.
Article 47	Artikel 47
<p>Il s'agit de déroger au champ d'application de la loi (article 3, § 2) en ce qui concerne les certifications européennes rendues obligatoires en vertu du droit de l'Union ou du droit national. L'article 47 détermine ainsi les pouvoirs d'enquête, procédures et sanctions applicables dans ce cas, à savoir ceux prévus dans le Code de droit économique. En ce qui concerne les sanctions, un article XV.125/7 est introduit à cet effet dans ce Code par l'article 48.</p> <p>L'article XV.30/5 précise que le Roi peut confier, par arrêté délibéré en Conseil des ministres, certaines missions de contrôle et de sanctions (à l'exception des articles 21 et 22 de la loi) en matière de certification européennes de cybersécurité à des agents du SPF Economie moyennant plusieurs conditions cumulatives à savoir : le SPF Economie doit en avoir exprimé la demande, le Roi doit solliciter l'avis de l'autorité nationale de certification de cybersécurité et enfin, que le SPF Economie dispose de l'expertise requise.</p> <p>Les missions qui sont ainsi confiées au SPF Economie portent uniquement sur les tâches de contrôle et de sanctions mais ne portent pas atteinte aux autres chapitres de la loi. Les chapitres 1 à 4 et 7 de la loi restent d'application pour les certifications européennes rendues obligatoires.</p>	<p>Dit is een afwijking aan de toepassingsgebied van de wet (van artikel 3, § 2) met betrekking tot de Europese certificeringen die verplicht zijn op grond van de Europese of nationale wetgeving. Artikel 47 bepaalt aldus de onderzoeksbevoegdheden, procedures en sancties die in dat geval van toepassing zijn, namelijk deze voorzien in het Wetboek van economisch recht. Wat de sancties betreft, wordt daarvoor door artikel 48 een artikel XV.125/7 ingevoegd in dat Wetboek.</p> <p>Artikel XV.30/5 bepaalt dat de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde toezichts- en sanctieopdrachten (met uitzondering van artikel 21 en 22 van de wet) op het gebied van Europese cyberbeveiligingscertificering kan toevertrouwen aan ambtenaren van de FOD Economie, onder verschillende cumulatieve voorwaarden, namelijk: de FOD Economie moet hiertoe een verzoek hebben geformuleerd, de Koning moet het advies inwinnen van de nationale cyberbeveiligingscertificeringsautoriteit en de FOD Economie moet, tot slot, over de vereiste expertise beschikken.</p> <p>De opdrachten die aldus aan de FOD Economie worden toevertrouwd, hebben enkel betrekking op de controle- en sanctietaken, maar doen geen afbreuk aan de andere hoofdstukken van de wet. De hoofdstukken 1 tot 4 en 7 van de wet blijven van toepassing op Europese certificeringen die worden opgelegd.</p>
Article 48	Artikel 48
<p>Cet article vise à déterminer les sanctions applicables en matière de certification obligatoire et fait la distinction entre les infractions qui seront punies d'amendes pénales de niveau 2 au sens de l'article XV.70 du Code de droit économique et celles, plus graves, qui seront punies d'amendes pénales de niveau 3 au sens de l'article XV.70 du même Code.</p>	<p>Dit artikel heeft tot doel de sancties vast te stellen die van toepassing zijn op de verplichte certificering en maakt een onderscheid tussen inbreuken die met strafrechtelijke geldboetes van niveau 2 worden bestraft als bedoeld in artikel XV.70 van het Wetboek van economisch recht en zwaardere inbreuken die met strafrechtelijke geldboetes van niveau 3 worden bestraft als bedoeld in artikel XV.70 van hetzelfde Wetboek.</p>
Section 5. - Entrée en vigueur et dispositions transitoires	Afdeling 5. - Inwerkingtreding en overgangsbepalingen
Article 49	Artikel 49
Cette disposition précise la date d'entrée en vigueur de la loi.	Deze bepaling vermeldt de datum van inwerkingtreding van de wet.