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

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[2022/204364]

20 JULI 2022. — Wet inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit (1)

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

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

HOOFDSTUK 1. — *Definities en algemene bepalingen*

Afdeling 1. — Onderwerp en toepassingsgebied

Onderafdeling 1. — Onderwerp

Artikel 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, hierna : de "Cyberbeveiligingsverordening".

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, 7 en 8, alsook de artikelen 21 en 22, zijn ook van toepassing op een verplichte Europese cyberbeveiligingscertificering.

Bij de uitvoering van artikel 21 en 22 in het kader van de in het eerste lid bedoelde certificering zijn artikel 19 en 26 van toepassing.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de hoofdstukken 5 en 6 volledig of gedeeltelijk toepasselijk maken in het kader van de in het eerste lid bedoelde certificering.

§ 3. 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 bedoeld in artikel 6, 2°, 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, in artikel 3, 3°, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en in artikel 2, eerste lid, 1°, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.

Met inachtneming van paragraaf 2 zorgen de in het eerste lid bedoelde overheden en de bevoegde inspectiediensten voor het toezicht op en de sancties met betrekking tot verplichte Europese cyberbeveiligingscertificeringen.

§ 4. Artikel 5, § § 2 tot 4, is 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.

§ 5. Deze wet doet geen afbreuk aan de toepassing van het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling.

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[2022/204364]

20 JUILLET 2022. — Loi 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 (1)

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

La Chambre des représentants a adopté et Nous sanctionnons ce qui suit :

CHAPITRE 1er. — *Définitions et dispositions générales*

Section 1re. — Objet et champ d'application

Sous-section 1re. — Objet

Article 1er. 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, ci-après : le « Règlement sur la cybersécurité ».

Sous-section 2. — Champ d'application

Art. 3. § 1er. 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 1er à 4, 7 et 8, 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 de la certification visée à l'alinéa 1er, 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 de la certification visée à l'alinéa 1er.

§ 3. 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 visées à l'article 6, 2°, 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, de l'article 3, 3°, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et de l'article 2, alinéa 1er, 1°, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

Dans le respect du paragraphe 2, les autorités visées à l'alinéa 1er et les services d'inspection compétents assurent le contrôle et les sanctions des certifications européennes de cybersécurité rendues obligatoires.

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

§ 5. La présente loi ne porte pas préjudice à l'application de l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité.

Afdeling 2. — Definities

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

1° "nationale cyberbeveiligingscertificeringsautoriteit" : de autoriteit bedoeld in artikel 58 van de Cyberbeveiligingsverordening die is aangewezen door de Koning overeenkomstig artikel 5, § 1;

2° "EGC" : de Europese Groep voor cyberbeveiligingscertificering bedoeld in artikel 62 van de Cyberbeveiligingsverordening;

3° "nationale accreditatieautoriteit" : de nationale accreditatie-instelling bedoeld in artikel 2, 16), van de Cyberbeveiligingsverordening die door de Koning is opgericht in uitvoering van artikel VIII.30 van het Wetboek van economisch recht;

4° "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;

5° "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 een besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in de hoofdstukken 5 en 6 van de autoriteit bedoeld in paragraaf 1, volledig of gedeeltelijk toevertrouwen aan een andere overheid, met uitzondering van de opdrachten bedoeld in de artikelen 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 paragraaf 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 de hoofdstukken 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 de hoofdstukken 5 en 6 door de Koning is aangewezen, voeren hun taken uit in overleg met de overheden, met name met de nationale accreditatieautoriteit. Naargelang het specifieke voorwerp van de certificeringsregeling kunnen de autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, ook de private actoren raadplegen die betrokken zijn bij de cyberbeveiligingscertificering.

§ 2. Overeenkomstig artikel 58, lid 7, onder *h),* van de Cyberbeveiligingsverordening wordt informatie uitgewisseld tussen, enerzijds, de autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen en, anderzijds, de sectorale overheden en de inspectiediensten, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of in artikel 7, § § 3 en 5, 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, het Belgisch Instituut voor postdiensten en telecommunicatie en de nationale accreditatieautoriteit. Deze informatie is noodzakelijk voor de toepassing van de Cyberbeveiligingsverordening, deze wet of de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, met name wat betreft de afgifte van certificaten, het toezicht, sancties en klachten. Indien een informatie-uitwisseling persoonsgegevens betreft, gebeurt deze overeenkomstig de bepalingen van hoofdstuk 8. De nadere regels van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.

Section 2. — Définitions

Art. 4. Pour l'application de la présente loi, on entend par:

1° « 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, § 1er;

2° « GECC » : le Groupe européen de certification de cybersécurité visé à l'article 62 du Règlement sur la cybersécurité;

3° « autorité nationale d'accréditation » : l'organisme national d'accréditation unique créé par le Roi en exécution de l'article VIII.30 du Code de droit économique et visé à l'article 2, 16), du Règlement sur la cybersécurité;

4° « 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;

5° « service d'inspection » : le service d'inspection visé à l'article 13, § 1er.

CHAPITRE 2. — *Autorités compétentes et coopération au niveau national*

Section 1re. — Autorités compétentes

Art. 5. § 1er. 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 Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6 de l'autorité visée au paragraphe 1er à une autre autorité publique, à l'exception des missions visées aux 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 concerte au préalable avec l'autorité visée au paragraphe 1er 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. § 1er. L'autorité visée à l'article 5, § 1er, 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, notamment avec l'autorité nationale d'accréditation. En fonction de l'objet précis du schéma de certification, l'autorité visée à l'article 5, § 1er, 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. Conformément à l'article 58, paragraphe 7, *h),* du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, d'une part, les autorités sectorielles et les services d'inspection, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou à l'article 7, § § 3 et 5, 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, l'Institut belge des services postaux et des télécommunications et l'autorité nationale d'accréditation, d'autre part, s'échangent les informations nécessaires à l'application du Règlement sur la cybersécurité, de la présente loi ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, notamment en matière de délivrance de certificats, de contrôle, de sanctions et de réclamations. Lorsqu'un échange d'informations porte sur des données à caractère personnel, cet échange est effectué conformément aux dispositions du chapitre 8. Les modalités d'échange d'informations préservent la confidentialité des informations concernées.

§ 3. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen verstrekken de ontvangers, namelijk een sectorale overheid, een inspectiedienst, de luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, in artikel 7, § § 3 en 5, 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 of in de artikelen 2, eerste lid, 1° en 9°, en 15, § § 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, alle informatie verkregen in het kader van de uitvoering van de Cyberbeveiligingsverordening, deze wet of een Europese cyberbeveiligingscertificeringsregeling, indien deze informatie betrekking heeft op een inbreuk op artikel 13 van de voormelde wet van 1 juli 2011, de artikelen 20, 21, § 1, en 33, van de voormelde wet van 7 april 2019, artikel 11 van het voormelde koninklijk besluit van 2 december 2011 of de afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, en de entiteit waarop de informatie betrekking heeft onder het toezicht staat van voornoemde ontvangers.

§ 4. In het kader van de samenwerking bedoeld in de paragrafen 2 en 3 mogen overheden die uit hoofde van hun staat kennis dragen van geheimen of vertrouwelijke informatie die hun zijn toevertrouwd, deze geheimen of vertrouwelijke informatie bekendmaken aan de autoriteit bedoeld in artikel 5, § 1, of aan de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, indien dit nodig is voor de toepassing van de Cyberbeveiligingsverordening of deze wet.

Enkel de noodzakelijke informatie met betrekking tot toezicht, sancties en klachten mogen bekendgemaakt worden. Indien deze informatie persoonsgegevens betreft, is hoofdstuk 8 van toepassing. De nadere regels 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, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, bijstaan bij de in deze wet bedoelde toezichtsopdrachten.

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 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.

§ 3. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 communiquent aux destinataires, à savoir une autorité sectorielle, un service d'inspection, l'inspection aéroportuaire, l'inspection aéronautique ou la Belgian Supervising Authority for Air Navigation Services visés respectivement aux articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, à l'article 7, § § 3 et 5, 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 aux articles 2, alinéa 1er, 1° et 9°, et 15, §§ 1er à 3, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, toute information obtenue dans le cadre de l'exécution du Règlement sur la cybersécurité, de la présente loi ou d'un schéma européen de certification de cybersécurité lorsque cette information porte sur un manquement à l'article 13 de la loi précitée du 1er juillet 2011, aux articles 20, 21, § 1er, et 33, de la loi précitée du 7 avril 2019, à l'article 11 de l'arrêté royal précité du 2 décembre 2011 ou aux sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, et que l'entité concernée par l'information se trouve sous la surveillance desdits destinataires.

§ 4. Dans le cadre de la coopération prévue aux paragraphes 2 et 3, les autorités publiques dépositaires, par état, des secrets ou informations confidentielles qu'on leur confie sont autorisées à faire connaître ces secrets ou ces informations confidentielles à l'autorité visée à l'article 5, § 1er, ou à l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.

Seules les informations nécessaires en matière de contrôle, de sanctions et de réclamations peuvent être communiquées. Lorsque ces informations portent sur des données à caractère personnel, le chapitre 8 est d'application. 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, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, dans ses missions de contrôle visées par la présente loi.

CHAPITRE 3. — *Autorité nationale de certification de cybersécurité*

Section 1re. — Représentation au Groupe européen de certification de cybersécurité

Art. 8. § 1er. L'autorité visée à l'article 5, § 1er, 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, § 1er, se concerte 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, § 1er, aux travaux et réunions du GECC.

Section 2. — Indépendance

Art. 9. § 1er. L'autorité visée à l'article 5, § 1er, 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, § 1er, chargé de la certification ou du contrôle a, directement ou indirectement, un intérêt financier, économique ou un autre intérêt personnel qui pourrait être 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, § 1er, ne reçoivent ni ne cherchent dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne.

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. Overeenkomstig artikel 56, lid 4, van de Cyberbeveiligingsverordening geven de conformiteitsbeoordelingsinstanties die door de nationale accreditatieautoriteit geaccrediteerd zijn, de Europese cyberbeveiligingscertificaten voor zekerheidsniveau ″basis″ of ″substantieel″ af.

§ 2. Overeenkomstig artikel 56, lid 5, onder *a),* van de Cyberbeveiligingsverordening is de afgifte van de in paragraaf 1 bedoelde certificaten, indien vereist door de Europese cyberbeveiligingscertificeringsregeling, voorbehouden aan de autoriteit bedoeld in artikel 5, § 1.

§ 3. Overeenkomstig artikel 56, lid 5, onder *b),* van de Cyberbeveiligingsverordening kan de autoriteit bedoeld in artikel 5, § 1, naargelang de technische vereisten van de certificeringsregeling en na voorafgaande delegatie, de afgifte van een certificaat bedoeld in paragraaf 2 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. Overeenkomstig artikel 56, lid 6, van de Cyberbeveiligingsverordening geeft de autoriteit bedoeld in artikel 5, § 1, de Europese cyberbeveiligingscertificaten voor zekerheidsniveau ″hoog″ af.

§ 2. Overeenkomstig artikel 56, lid 6, onder *b),* van de Cyberbeveiligingsverordening kan de autoriteit bedoeld in artikel 5, § 1, naargelang de technische vereisten van de certificeringsregeling en na voorafgaande delegatie, 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. Overeenkomstig artikel 63, lid 1, van de Cyberbeveiligingsverordening kan de aanvrager, ingeval de afgifte van een Europees cyberbeveiligingscertificaat geweigerd wordt door de autoriteit bedoeld in artikel 5, § 1, of door een conformiteitsbeoordelingsinstantie in het kader van de delegatie bedoeld in artikel 10, § 3, of in artikel 11, § 2, een klacht indienen bij de autoriteit bedoeld in artikel 5, § 1, volgens de in hoofdstuk 7 bepaalde nadere regels.

HOOFDSTUK 5. — *Toezicht*

Art. 13. § 1. Overeenkomstig artikel 58, leden 7 en 8, van de Cyberbeveiligingsverordening beschikken de autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, elk 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.

De bevoegdheden van deze inspectiedienst doen geen afbreuk aan de toepassing van het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling.

Overeenkomstig artikel 58, lid 4, van de Cyber-beveiligingsverordening handelt de inspectiedienst bij de uitvoering van zijn toezichtstaken onafhankelijk van de andere diensten van de autoriteit bedoeld in artikel 5, § 1, met name van de dienst belast met de afgifte van cyberbeveiligingscertificaten, of van de andere diensten van de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen.

§ 2. Bij het formuleren van een verzoek om informatie of bewijzen vermeldt de inspectiedienst het doeleinde van het verzoek, de wettelijke bepalingen en, in voorkomend geval, het deel of de delen van de Europese cyberbeveiligingscertificeringsregeling, alsook de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt.

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 1re. — Certificats de cybersécurité européens attestant d'un niveau d'assurance « élémentaire » ou « substantiel »

Art. 10. § 1er. Conformément à l'article 56, paragraphe 4, du Règlement sur la cybersécurité, 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. Conformément à l'article 56, paragraphe 5, *a),* du Règlement sur la cybersécurité, lorsque le schéma européen de certification de cybersécurité l'impose, la délivrance des certificats visés au paragraphe 1er est réservée à l'autorité visée à l'article 5, § 1er.

§ 3. Conformément à l'article 56, paragraphe 5, *b),* du Règlement sur la cybersécurité, en fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1er, peut 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. § 1er. Conformément à l'article 56, paragraphe 6, du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, délivre les certificats de cybersécurité européens attestant d'un niveau d'assurance dit « élevé ».

§ 2. Conformément à l'article 56, paragraphe 6, *b),* du Règlement sur la cybersécurité, en fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1er, 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

Art. 12. Conformément à l'article 63, paragraphe 1er, du Règlement sur la cybersécurité, en cas de refus de délivrance d'un certificat de cybersécurité européen par l'autorité visée à l'article 5, § 1er, ou par un organisme d'évaluation de la conformité dans le cadre de la délégation prévue à l'article 10, § 3, ou à l'article 11, § 2, le demandeur peut introduire une réclamation devant l'autorité visée à l'article 5, § 1er, selon les modalités prévues au chapitre 7.

CHAPITRE 5. — *Contrôle*

Art. 13. § 1er. Conformément à l'article 58, paragraphes 7 et 8, du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 disposent chacune 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.

Les compétences de ce service d'inspection sont sans préjudice de l'application de l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité.

Conformément à l'article 58, paragraphe 4, du Règlement sur la cybersécurité, 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, § 1er, notamment du service chargé de la délivrance des certificats de cybersécurité, ou des autres services de l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6.

§ 2. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection mentionne la finalité de la demande, les dispositions légales ainsi que, le cas échéant, la ou les parties du schéma européen de certification de cybersécurité et précise le délai dans lequel les informations ou preuves doivent être fournies.

§ 3. Naargelang de specifieke kenmerken van elke Europese cyberbeveiligingscertificeringsregeling kan de inspectiedienst een beroep doen op experten die onderworpen zijn aan het in paragraaf 4 bedoelde beroepsgeheim.

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

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

Art. 14. Wanneer een conformiteitsbeoordelingsinstantie, een houder van vrijwillige Europese cyberbeveiligingscertificaten of een afgever van EU-conformiteitsverklaringen zich buiten het Belgische grondgebied bevindt, kan de inspectiedienst de bevoegde nationale cyberbeveiligingscertificeringsautoriteiten van de betrokken 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. Ze leggen de eed af bij de leidinggevend ambtenaar van hun dienst.

§ 2. De beëdigde leden van de inspectiedienst of de experten 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 kunnen komen.

§ 3. Om de toezichthoudende werkzaamheden bedoeld in artikel 58 van de Cyberbeveiligingsverordening uit te voeren en 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 toezichtsbevoegdheden bij de uitoefening van hun opdracht :

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

§ 4. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de beëdigde 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 beëdigde 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 te 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.

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.

§ 3. En fonction des caractéristiques propres à chaque schéma européen de certification de cybersécurité, le service d'inspection peut faire appel à des experts qui sont soumis au secret professionnel visé au paragraphe 4.

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

§ 4. 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.

Art. 14. Lorsqu'un organisme d'évaluation de la conformité, un titulaire de certificats de cybersécurité européens volontaires ou un émetteur de déclarations 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 des États concernés.

Art. 15. § 1er. Les membres assermentés du service d'inspection sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi. Ils prêtent serment auprès du fonctionnaire dirigeant de leur service.

§ 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 certificats de cybersécurité européens ou émetteurs de déclarations de conformité de l'Union européenne qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité.

§ 3. Afin de mener à bien les activités de supervision visées à l'article 58 du Règlement sur la cybersécurité et 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 certificats de cybersécurité européens ou l'émetteur de déclarations de conformité de l'Union européenne; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par un 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 certificats de cybersécurité européens ou l'émetteur de déclarations de conformité de l'Union européenne et dont ils estiment l'audition nécessaire pour l'exercice de leur mission. À cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification;

§ 4. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres assermentés 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 assermentés 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 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.

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 het proces-verbaal van 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 informaticasysteem en de erin opgenomen gegevens in beslag nemen.

§ 7. Om de zoekactie in een informaticasysteem of een deel hiervan die op basis van paragraaf 6 werd opgestart, uit te breiden naar een informaticasysteem 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.

§ 9. Indien dit nodig is voor de uitvoering van de toezichtsactiviteiten bedoeld in dit hoofdstuk en de andere middelen niet volstaan, kunnen de beëdigde leden van de inspectiedienst toegang krijgen tot de informatie of geheimen bedoeld in artikel 458 van het Strafwetboek en deze verwerken, wanneer een houder van Europese cyberbeveiligingscertificaten of een afgever van EU-conformiteitsverklaringen er kennis van draagt.

§ 10. Bij de uitvoering van hun toezichtsbevoegdheden bedoeld in dit artikel zorgen de beëdigde leden van de inspectiedienst ervoor dat de door hen gebruikte middelen passend en noodzakelijk zijn voor het toezicht op de bepalingen van de Cyberbeveiligingsverordening of een certificeringsregeling waarvan zij de naleving controleren.

Art. 16. § 1. Na afloop van de inspecties stelt de inspectiedienst een verslag op waarvan een kopie wordt bezorgd aan de geïnspecteerde conformiteitsbeoordelingsinstantie, houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen.

§ 2. De verslagen opgesteld door de inspectiedienst mogen geen persoonsgegevens bevatten van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, noch persoonsgegevens die deze klanten verwerken.

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.

À la fin de l'audition, la personne interrogée a le droit de relire le procès-verbal de son audition 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 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.

§ 9. Lorsque cela est nécessaire à la réalisation des activités de contrôle visées au présent chapitre et que les autres moyens ne suffisent pas, les membres assermentés du service d'inspection peuvent avoir accès aux informations ou secrets visés à l'article 458 du Code pénal et dont un titulaire de certificats de cybersécurité européens ou un émetteur de déclarations de conformité de l'Union européenne est le dépositaire, et les traiter.

§ 10. Lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les membres assermentés du service d'inspection veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour le contrôle des dispositions du Règlement sur la cybersécurité ou d'un schéma de certification dont ils contrôlent le respect.

Art. 16. § 1er. À la fin des inspections, un rapport est dressé par le service d'inspection. Une copie de ce rapport est transmise à l'organisme d'évaluation de la conformité, au titulaire de certificats de cybersécurité européens ou à l'émetteur de déclarations de conformité de l'Union européenne inspecté.

§ 2. Les rapports dressés par le service d'inspection ne peuvent contenir, ni les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne, ni les données à caractère personnel traitées par ces clients.

§ 3. Op hun verzoek en voor zover dit nodig is voor het vervullen van de opdrachten bedoeld in artikel VIII.30, § 2, van het Wetboek van economisch recht, in hoofdstuk II van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, in de artikelen 58, lid 7, onder *c)*, en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of in de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, kan de nationale accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie een kopie krijgen van het in paragraaf 1 bedoelde verslag.

In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het verslag bedoeld in het eerste lid niet worden geformaliseerd aan de hand van een protocol voor zover:

1° de doorgifte noodzakelijk is voor de uitvoering van het eerste lid;

2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van de wet, van de artikelen 58, lid 7, onder *c)*, en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of van de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie;

3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;

4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.

§ 4. Met inachtneming van de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, 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 sectorale overheid en de inspectiedienst, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de voormelde wet van 1 juli 2011 en in artikel 7, § § 3 en 5, van de voormelde wet van 7 april 2019, die bevoegd zijn naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12° tot 14°, van de Cyberbeveiligingsverordening, indien dit verslag betrekking heeft op een controle bij een kritieke infrastructuur, een aanbieder van essentiële diensten of een digitaledienstverlener als bedoeld in de voormelde wet van 1 juli 2011 of de voormelde wet van 7 april 2019.

Met inachtneming van artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer en de afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, 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 luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services, als bedoeld in de artikelen 2, eerste lid, 1° en 9°, en 15, § § 1 tot 3, van het voormelde koninklijk besluit van 2 december 2011, indien dit verslag betrekking heeft op een controle bij een kritieke infrastructuur als bedoeld in dit koninklijk besluit.

In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het in deze paragraaf bedoelde verslag niet worden geformaliseerd aan de hand van een protocol voor zover :

1° de doorgifte noodzakelijk is voor de uitvoering van het tweede lid;

2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van 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 netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer;

3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;

§ 3. À leur demande et pour autant que cela poursuive l'accomplissement des missions prévues à l'article VIII.30, § 2, du Code de droit économique, au chapitre II du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, aux articles 58, paragraphe 7, *c)*, et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou aux articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, l'autorité nationale d'accréditation ou l'Institut belge des services postaux et des télécommunications peut recevoir une copie du rapport visé au paragraphe 1er.

Par dérogation à 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, la transmission de rapport prévue à l'alinéa 1er ne doit pas être formalisée par un protocole pour autant que:

1° le transfert soit nécessaire à l'exécution de l'alinéa 1er;

2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi, des articles 58, paragraphe 7, *c)*, et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques;

3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;

4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.

§ 4. Dans le respect des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et de l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet une copie du rapport prévu au paragraphe 1er à l'autorité sectorielle et au service d'inspection, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi précitée du 1er juillet 2011 et à l'article 7, § § 3 et 5, de la loi précitée du 7 avril 2019, compétents en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12° à 14°, du Règlement sur la cybersécurité, lorsque ce rapport 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 précitée du 1er juillet 2011 ou de la loi précitée du 7 avril 2019.

Afin d'assurer le respect de l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien et des sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet une copie du rapport prévu au paragraphe 1er à l'inspection aéroportuaire, à l'inspection aéronautique ou à la Belgian Supervising Authority for Air Navigation Services, au sens des articles 2, alinéa 1er, 1° et 9°, et 15, § § 1er à 3, de l'arrêté royal précité du 2 décembre 2011, lorsque ce rapport est lié à un contrôle effectué auprès d'une infrastructure critique, au sens de cet arrêté royal.

Par dérogation à 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, la transmission de rapport prévue au présent paragraphe ne doit pas être formalisée par un protocole pour autant que :

1° le transfert soit nécessaire à l'exécution de l'alinéa 2;

2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi du 1er 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 et de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien;

3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;

4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.

Art. 17. § 1. De beëdigde leden van de inspectiedienst stellen de in artikel 20, § 1, bedoelde processen-verbaal op.

§ 2. Op hun verzoek en voor zover dit nodig is voor het vervullen van de opdrachten bedoeld in artikel VIII.30, § 2, van het Wetboek van economisch recht, in hoofdstuk II van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 en in de artikelen 58, lid 7, onder *c)*, en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of in de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, krijgt de nationale accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie een kopie 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.

In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het proces-verbaal bedoeld in het eerste lid niet worden geformaliseerd aan de hand van een protocol voor zover :

1° de doorgifte noodzakelijk is voor de uitvoering van het eerste lid;

2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van de wet, van de artikelen 58, lid 7, onder *c)*, en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of van de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie;

3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;

4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.

§ 3. Met inachtneming van artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de artikelen 20, 21, § 1, en 33 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, bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, de bevoegde sectorale overheid en de bevoegde inspectiedienst, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de voormelde wet van 1 juli 2011 en in artikel 7, § § 3 en 5, van de voormelde wet van 7 april 2019, naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening, 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 digitaledienstverlener als bedoeld in de voormelde wet van 1 juli 2011 of de voormelde wet van 7 april 2019.

Met inachtneming van artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer en de afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, 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 proces-verbaal en van alle bijkomende informatie in verband met een controle bij een kritieke infrastructuur, als bedoeld in artikel 2, 3°, van het voormelde koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, aan de luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services, als bedoeld in de artikelen 2, eerste lid, 1° en 9°, en 15, § § 1 tot 3, van dit koninklijk besluit.

In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het in deze paragraaf bedoelde proces-verbaal niet worden geformaliseerd aan de hand van een protocol voor zover :

1° de doorgifte noodzakelijk is voor de uitvoering van het tweede lid;

4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.

Art. 17. § 1er. Les membres assermentés du service d'inspection rédigent des procès-verbaux visés à l'article 20, § 1er.

§ 2. À leur demande et pour autant que cela poursuive l'accomplissement des missions prévues à l'article VIII.30, § 2, du Code de droit économique, au chapitre II du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil ainsi qu'aux articles 58, paragraphe 7, *c)*, et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou aux articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, l'autorité nationale d'accréditation ou l'Institut belge des services postaux et des télécommunications reçoit une copie d'un procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué par l'autorité visée à l'article 5, § 1er, ou par l'autorité publique désignée par le Roi en vertu de l'article 5, § 2.

Par dérogation à 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, la transmission de procès-verbal prévue à l'alinéa 1er ne doit pas être formalisée par un protocole pour autant que :

1° le transfert soit nécessaire à l'exécution de l'alinéa 1er;

2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi, des articles 58, paragraphe 7, *c)*, et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques;

3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;

4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.

§ 3. Dans le respect de l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et des articles 20, 21, § 1er, et 33 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, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet à l'autorité sectorielle et au service d'inspection compétents, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi précitée du 1er juillet 2011 et à l'article 7, § § 3 et 5, de la loi précitée du 7 avril 2019, en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité, 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 précitée du 1er juillet 2011 ou de la loi précitée du 7 avril 2019.

Dans le respect de l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien et des sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet une copie du procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué auprès d'une infrastructure critique, au sens de l'article 2, 3°, de l'arrêté royal précité du 2 décembre 2011, à l'inspection aéroportuaire, à l'inspection aéronautique ou à la Belgian Supervising Authority for Air Navigation Services, au sens des articles 2, alinéa 1er, 1° et 9°, et 15, § § 1er à 3, de cet arrêté royal.

Par dérogation à 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, la transmission de procès-verbal prévue au présent paragraphe ne doit pas être formalisée par un protocole pour autant que :

1° le transfert soit nécessaire à l'exécution de l'alinéa 2;

2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van 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 netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer;

3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;

4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.

Art. 18. § 1. Overeenkomstig de artikelen 53, lid 3, en 58, lid 8, onder *a),* van de Cyberbeveiligingsverordening verleent de conformiteitsbeoordelingsinstantie, de houder van vrijwillige Europese cyberbeveiligingscertificaten of de afgever van EU-conformiteitsverklaringen volledige medewerking aan de leden van de inspectiedienst of de experten 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 vrijwillige Europese cyberbeveiligingscertificaten of de afgever van EU-conformiteitsverklaringen het nodige materiaal ter beschikking van de leden van de inspectiedienst en de experten 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 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 Cyber-beveiligingsverordening 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. Overeenkomstig artikel 58, lid 8, *e),* van de Cyberbeveiligingsverordening trekt de autoriteit bedoeld in artikel 5, § 1, een cyberbeveiligingscertificaat in als de begunstigde de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft.

2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi du 1er 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 et de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien;

3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;

4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.

Art. 18. § 1er. Conformément aux articles 53, paragraphe 3, et 58, paragraphe 8, *a),* du Règlement sur la cybersécurité, l'organisme d'évaluation de la conformité, le titulaire de certificats de cybersécurité européens volontaires ou l'émetteur de déclarations 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 certificats de cybersécurité européens volontaires ou l'émetteur de déclarations 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, § 1er, 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, des titulaires de certificats de cybersécurité européens volontaires et des émetteurs de déclarations de conformité de l'Union européenne. Le Roi fixe les modalités de calcul et de paiement.

CHAPITRE 6. — *Sanctions*

Section 1re. — Procédure

Art. 19. § 1er. 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. § 1er. 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. Conformément à l'article 58, paragraphe 8, *e),* du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, retire un certificat de cybersécurité lorsque le bénéficiaire ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité.

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

Art. 22. Overeenkomstig artikel 58, lid 7, *e),* van de Cyberbeveiligingsverordening voorziet de autoriteit bedoeld in artikel 5, § 1, in de beperking, opschorting of intrekking van toelatingen alsook 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. Eenieder die niet reageert op een verzoek om informatie van de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, wordt gestraft met een administratieve geldboete van 500 tot 75 000 euro.

§ 2. 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, wordt gestraft met een administratieve geldboete van 500 tot 100 000 euro.

§ 3. De houder van een Europees cyberbeveiligingscertificaat voor zekerheidsniveau ″basis″ die niet voldoet aan de verplichtingen die voortvloeien uit de overeenstemmende Europese cyberbeveiligingscertificeringsregeling, wordt gestraft met een administratieve geldboete van 500 tot 100 000 euro.

§ 4. De houder van een Europees cyberbeveiligingscertificaat voor zekerheidsniveau ″substantieel″ of ″hoog″ die niet voldoet aan de verplichtingen die voortvloeien uit de overeenstemmende Europese cyberbeveiligingscertificeringsregeling, wordt gestraft met een administratieve geldboete van 500 tot 125 000 euro.

§ 5. Onverminderd artikel 15, § 5, eerste lid, 3°, wordt eenieder die niet meewerkt tijdens een inspectie door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken, of die anderszins weigert mee te werken tijdens een inspectie, gestraft met een administratieve geldboete van 500 tot 150 000 euro.

§ 6. 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, wordt gestraft met een administratieve geldboete van 500 tot 200 000 euro.

Art. 24. § 1. De beslissing om een administratieve geldboete op te leggen vermeldt het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§ 2. De autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie zoals bedoeld in de artikelen 21, 22 of 23 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 zijn ontvangen door de overtreder de zesde dag na de verzending ervan door de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen.

§ 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, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, 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 administratieve geldboete binnen een maand wordt bij de beslissing gevoegd.

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

Art. 22. Conformément à l'article 58, paragraphe 7, *e),* du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, limite, suspend ou retire les autorisations ainsi que les délégations qu'elle a 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. § 1er. Est puni d'une amende administrative de 500 à 75 000 euros quiconque ne répond pas à une demande d'information de l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6.

§ 2. Est puni d'une amende administrative 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.

§ 3. Est puni d'une amende administrative 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.

§ 4. Est puni d'une amende administrative 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.

§ 5. Sans préjudice de l'article 15, § 5, alinéa 1er, 3°, est puni d'une amende administrative de 500 à 150 000 euros quiconque ne coopère pas lors d'un contrôle en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle ou ne coopère pas lors d'un contrôle de toute autre manière.

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

Art. 24. § 1er. La décision d'imposer une amende administrative mentionne le montant de l'amende administrative et les infractions visées.

§ 2. L'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, informe au préalable le contrevenant de sa proposition motivée de sanction administrative telle que visée aux articles 21, 22 ou 23 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 sixième jour suivant son envoi par l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6.

§ 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, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, 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 administrative dans un délai d'un mois est jointe à la décision.

Art. 26. De overtreder kan de beslissing die de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, krachtens hoofdstuk 6 heeft genomen, betwisten bij het Marktenhof.

Het Marktenhof spreekt zich uit over de grond van de zaak en beschikt over 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, of van de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, wordt ingediend.

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

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, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door de wettelijke vertegenwoordiger van de autoriteit bedoeld in artikel 5, § 1, of van de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaardersexploot 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. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het wordt aangetekend door middel van een dagvaarding van de autoriteit bedoeld in artikel 5, § 1, of van de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, 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.

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, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, 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 betekeningskosten 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, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, 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. Overeenkomstig artikel 63, lid 1, van de Cyberbeveiligingsverordening ontvangt en behandelt de autoriteit bedoeld in artikel 5, § 1, klachten over een Europees cyberbeveiligingscertificaat dat is afgegeven door de autoriteit bedoeld in artikel 5, § 1, of door een conformiteitsbeoordelingsinstantie in het kader van de delegatie bedoeld in artikel 10, § 3, of 11, § 2, over de weigering om een dergelijk certificaat af te geven of over 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. 26. Le contrevenant peut contester la décision prise en vertu du chapitre 6 par l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, devant la Cour des marchés.

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, § 1er, ou de l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6.

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

Art. 27. § 1er. 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 l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, peut décerner une contrainte.

La contrainte est décernée par le représentant légal de l'autorité visée à l'article 5, § 1er, ou de l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, 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.

§ 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, § 1er, ou à l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, 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.

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, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, 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, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, 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 1re. — Saisine de l'autorité nationale de certification de cybersécurité

Art. 29. Conformément à l'article 63, paragraphe 1er, du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, reçoit et traite les réclamations liées à un certificat de cybersécurité européen délivré par l'autorité visée à l'article 5, § 1er, ou par un organisme d'évaluation de la conformité dans le cadre de la délégation visée à l'article 10, § 3, ou 11, § 2, au refus de délivrance d'un tel certificat ou à 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. De bevoegde autoriteit gaat na of de klacht ontvankelijk is.

§ 2. Een klacht is ontvankelijk wanneer zij:

— 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 indiener van de klacht verzoeken zijn klacht toe te lichten.

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

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

Art. 34. Indien de autoriteit bedoeld in artikel 5, § 1, de klacht ontvankelijk verklaart, kan zij de bevoegdheden uitoefenen die haar overeenkomstig de artikelen 10, 11, 21 en 22 zijn verleend.

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

Afdeling 2. — Beroepen

Art. 35. Overeenkomstig artikel 64, lid 1, van de Cyberbeveiligingsverordening kan de indiener van de klacht de beslissing die de autoriteit bedoeld in artikel 5, § 1, krachtens afdeling 1 heeft genomen, betwisten bij het Marktenhof.

Het Marktenhof spreekt zich uit over de grond van de zaak en beschikt over 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. — *Verwerking van persoonsgegevens*

Afdeling 1. — Beginselen inzake verwerking, wettelijke basis en doeleinden

Art. 36. § 1. De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden :

1° de afgifte van Europese cyberbeveiligingscertificaten en het klachtenbeheer in dit verband door de autoriteit bedoeld in artikel 5, § 1;

2° het toezicht op houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen en conformiteitsbeoordelingsinstanties en, in voorkomend geval, het opleggen van sancties overeenkomstig de hoofdstukken 5 en 6;

3° de deelname aan de EGC van de autoriteit bedoeld in artikel 5, § 1, of van elke andere overheid die hierom verzoekt;

4° de samenwerking met de sectorale overheden en de inspectiediensten, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, in artikel 7, § § 3 en 5, 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, of in de artikelen 2, eerste lid, 1° en 9°, en 15, § § 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, die bevoegd zijn naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening, in het kader van hun bevoegdheden bedoeld in artikel 24, § 1, van de voormelde wet van 1 juli 2011 of in de artikelen 7, § 3, eerste lid, § 5, en 42, § 1, van de voormelde wet van 7 april 2019;

5° de samenwerking met de overheden die belast zijn met specifieke opdrachten inzake cyberbeveiliging, als bedoeld in artikel 2, 1), van de Cyberbeveiligingsverordening, overeenkomstig artikel 58, lid 7, onder *a),* c) en *h),* van dezelfde verordening.

§ 2. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen zijn elk verantwoordelijk voor de verwerkingen die ze uitvoeren voor de verwezenlijking van de doeleinden bedoeld in paragraaf 1.

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

§ 2. Une réclamation est recevable lorsqu'elle:

— 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, § 1er, 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 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.

Art. 34. Si l'autorité visée à l'article 5, § 1er, conclut à la recevabilité de la réclamation, elle peut exercer les pouvoirs qui lui sont conférés conformément aux articles 10, 11, 21 et 22.

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

Section 2. — Recours

Art. 35. Conformément à l'article 64, paragraphe 1er, du Règlement sur la cybersécurité, le réclamant peut contester la décision prise en vertu de la section 1re par l'autorité visée à l'article 5, § 1er, devant la Cour des marchés.

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, § 1er.

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. — *Traitement des données à caractère personnel*

Section 1re. — Principes relatifs au traitement, base légale et finalités

Art. 36. § 1er. Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes :

1° la délivrance des certificats de cybersécurité européen et la gestion des réclamations y relatives par l'autorité visée à l'article 5, § 1er;

2° le contrôle des titulaires de certificats de cybersécurité européens, des émetteurs de déclarations de conformité de l'Union européenne et des organismes d'évaluation de la conformité et, le cas échéant, l'imposition de sanctions conformément aux chapitres 5 et 6;

3° la participation de l'autorité visée à l'article 5, § 1er, ou de toute autre autorité publique qui en fait la demande, au GECC;

4° la coopération avec les autorités sectorielles et les services d'inspection, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, à l'article 7, § § 3 et 5, 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 aux articles 2, alinéa 1er, 1° et 9°, et 15, § § 1er à 3, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, compétents en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité, dans le cadre de leurs pouvoirs visés à l'article 24, § 1er, de la loi précitée du 1er juillet 2011 ou aux articles 7, § 3, alinéa 1er, § 5, et 42, § 1er, de la loi précitée du 7 avril 2019;

5° la coopération avec les autorités publiques disposant de missions spécifiques en matière de cybersécurité, au sens de l'article 2, 1), du Règlement sur la cybersécurité, conformément à l'article 58, paragraphe 7, *a),* c) et *h),* du même règlement.

§ 2. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 sont chacune responsables des traitements qu'elles effectuent pour la réalisation des finalités visées au paragraphe 1er.

§ 3. De verwerkingsverantwoordelijken bedoeld in paragraaf 2 verwerken de volgende categorieën van persoonsgegevens:

1° voor het doeleinde bedoeld in paragraaf 1, 1°: de identificatiegegevens van elke natuurlijke persoon die rechtstreeks betrokken is bij een verzoek om afgifte van een Europees cyberbeveiligingscertificaat of bij een klacht in dit verband door de autoriteit bedoeld in artikel 5, § 1, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres;

2° voor het doeleinde bedoeld in paragraaf 1, 2°: elk persoonsgegeven dat noodzakelijk is voor de uitoefening van de toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6;

3° voor het doeleinde bedoeld in paragraaf 1, 3°: de identificatiegegevens van natuurlijke personen die wensen deel te nemen aan de EGC, namelijk hun naam, hun voornaam, hun adres, hun telefoonnummer en hun e-mailadres;

4° voor het doeleinde bedoeld in paragraaf 1, 4°: de identificatiegegevens, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres, of de elektronische-communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die rechtstreeks verband houden met de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening en verzameld worden door de inspectiedienst in het kader van zijn toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6, waarbij deze gegevens geen betrekking mogen hebben op natuurlijke personen die klant zijn van de betrokken houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen, of op de persoonsgegevens die deze klanten verwerken;

5° voor het doeleinde bedoeld in paragraaf 1, 5°: de identificatiegegevens, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres of de elektronische-communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die rechtstreeks verband houden met de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening en verzameld worden door de inspectiedienst in het kader van zijn toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6, waarbij deze gegevens geen betrekking mogen hebben op natuurlijke personen die klant zijn van de betrokken houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen, of op de persoonsgegevens die deze klanten verwerken.

In het geval bedoeld in het eerste lid, in de bepaling onder 2°, mogen de persoonsgegevens van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, en de persoonsgegevens die deze klanten verwerken, slechts worden verwerkt indien ze noodzakelijk zijn voor de toezichtsopdrachten bedoeld in hoofdstuk 5.

Indien mogelijk worden de gegevens bedoeld in het tweede lid gepseudonimiseerd of geaggregeerd om het risico te verkleinen dat persoonsgegevens worden gebruikt op een wijze die onverenigbaar is met 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) of de wetten en reglementen die deze verordening aanvullen of verduidelijken.

§ 4. Onverminderd paragraaf 3, 2°, mag de informatie-uitwisseling tussen overheden bedoeld in deze wet geen betrekking hebben op persoonsgegevens van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, noch op persoonsgegevens die deze klanten verwerken.

§ 5. De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van verwerkingen :

1° iedere natuurlijke persoon die optreedt voor conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen of voor een overheid;

2° iedere natuurlijke persoon die deelneemt aan een controle of verhoor in het kader van de toezichtsopdrachten bedoeld in hoofdstuk 5;

3° iedere natuurlijke persoon die een klacht indient;

4° iedere natuurlijke persoon die deelneemt aan de EGC;

§ 3. Les catégories de données à caractère personnel traitées par les responsables de traitement visés au paragraphe 2 sont les suivantes:

1° pour la finalité visée au paragraphe 1er, 1°: les données d'identification de toute personne physique intervenant directement dans une demande de délivrance d'un certificat de cybersécurité européen ou dans une réclamation y relative par l'autorité visée à l'article 5, § 1er, c'est-à-dire le nom, le prénom, l'adresse, le numéro de téléphone et l'adresse e-mail;

2° pour la finalité visée au paragraphe 1er, 2°: toute donnée à caractère personnel nécessaire à l'exercice des missions de contrôle et de sanction visées aux chapitres 5 et 6;

3° pour la finalité visée au paragraphe 1er, 3°: les données d'identification des personnes physiques ayant vocation à participer au GECC, c'est-à-dire leur nom, leur prénom, leur adresse, leur numéro de téléphone et leur adresse e-mail;

4° pour la finalité visée au paragraphe 1er, 4°: les données d'identification, c'est-à-dire le nom, le prénom, l' adresse, le numéro de téléphone et l'adresse e-mail, ou les données de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 relative aux communications électroniques directement liées au prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité et collectées par le service d'inspection dans le cadre de ses missions de contrôle et de sanction visées aux chapitres 5 et 6, sans que ces données puissent porter sur les personnes physiques, clientes du titulaire de certificats de cybersécurité européens ou de l'émetteur de déclarations de conformité de l'Union européenne concerné, ou sur les données à caractère personnel traitées par ces clients;

5° pour la finalité visée au paragraphe 1er, 5°: les données d'identification, c'est-à-dire le nom, le prénom, l'adresse, le numéro de téléphone et l'adresse e-mail, ou les données de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 relative aux communications électroniques directement liées au prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité et collectées par le service d'inspection dans le cadre de ses missions de contrôle et de sanction visées aux chapitres 5 et 6, sans que ces données puissent porter sur les personnes physiques, clientes du titulaire de certificats de cybersécurité européens ou de l'émetteur de déclarations de conformité de l'Union européenne concerné, ou sur les données à caractère personnel traitées par ces clients.

Dans le cas mentionné à l'alinéa 1er, 2°, les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne et les données à caractère personnel traitées par ces clients, ne peuvent être traitées que si elles se révèlent nécessaires aux missions de contrôle visées au chapitre 5.

Chaque fois que possible, les données visées à l'alinéa 2 sont pseudonymisées ou agrégées de façon à diminuer le risque d'une utilisation de données personnelles incompatible avec le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ou les lois et règlements qui le complètent ou le précisent.

§ 4. Sans préjudice du paragraphe 3, 2°, les échanges d'informations entre autorités publiques visés par la présente loi ne peuvent porter, ni sur les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne, ni sur les données à caractère personnel traitées par ces clients.

§ 5. Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet de traitements sont les suivantes :

1° toute personne physique intervenant pour les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne ou une autorité publique;

2° toute personne physique participant à un contrôle ou à une audition dans le cadre des missions de contrôle prévues au chapitre 5;

3° toute personne physique introduisant une réclamation;

4° toute personne physique participant au GECC;

5° iedere natuurlijke persoon wiens persoonsgegevens gebruikt worden in ICT-producten, ICT-diensten of ICT-processen als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening.

Art. 37. § 1. Met toepassing van artikel 23, lid 1, onder *c)*, e) en *h)*, van 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) worden bepaalde verplichtingen en rechten van deze verordening beperkt of uitgesloten, overeenkomstig de bepalingen van dit artikel. Deze beperkingen of uitsluitingen doen geen afbreuk aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefde doel.

§ 2. De artikelen 12 tot 16, 18 en 19 van voornoemde verordening zijn niet van toepassing op de verwerking van persoonsgegevens door de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, die optreedt als verwerkingsverantwoordelijke voor het doeleinde bedoeld in artikel 36, § 1, 2°, voor zover de uitoefening van de in deze artikelen vastgelegde rechten nadelig zou zijn voor de controle of de voorbereidende werkzaamheden ervan.

§ 3. De uitzondering geldt, onder voorbehoud van het evenredigheidsbeginsel en in voorkomend geval van het beginsel van minimale gegevensverwerking, voor alle categorieën van persoonsgegevens, voor zover de verwerking van deze gegevens in overeenstemming is met voornoemde doeleinden. Deze uitzondering geldt ook voor voorbereidende werkzaamheden of procedures met het oog op de eventuele toepassing van een administratieve sanctie.

§ 4. De uitzondering geldt slechts voor de periode tijdens dewelke de betrokkene onderworpen is aan een controle of de voorbereidende werkzaamheden ervan, voor zover de uitoefening van de rechten die het voorwerp uitmaken van de in dit artikel bedoelde afwijking nadelig zou zijn voor de controle of de voorbereidende werkzaamheden ervan. In ieder geval geldt ze maximaal één jaar na ontvangst van het verzoek tot uitoefening van het recht dat het voorwerp uitmaakt van de in dit artikel bedoelde afwijking.

De duur van de voorbereidende werkzaamheden bedoeld in het eerste lid, tijdens dewelke de in paragraaf 2 bedoelde artikelen niet van toepassing zijn, is beperkt tot maximaal één jaar vanaf de ontvangst van een verzoek over de toepassing van een van de in deze artikelen vastgelegde rechten.

§ 5. Zodra de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke een verzoek ontvangt in verband met de uitoefening van een van de rechten die zijn vastgelegd in de artikelen bedoeld in paragraaf 2, bevestigt hij de ontvangst ervan.

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke informeert de betrokkene schriftelijk en onverwijld, in ieder geval binnen een maand na ontvangst van het verzoek, over iedere weigering of beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in paragraaf 2, alsook over de redenen voor deze weigering of beperking. De informatie over de weigering of beperking kan achterwege worden gelaten wanneer de verstrekking ervan het doeleinde vermeld in paragraaf 2 zou ondermijnen. Afhankelijk van de complexiteit van de verzoeken en van het aantal ervan kan die termijn indien nodig met twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van deze verlenging en van de redenen voor het uitstel.

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke licht de betrokkene in over de mogelijkheid om klacht in te dienen bij de Gegevensbeschermingsautoriteit en om beroep in rechte in te stellen.

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke vermeldt de feitelijke of juridische redenen waarop zijn beslissing steunt. Deze inlichtingen worden ter beschikking gesteld van de Gegevensbeschermingsautoriteit.

Wanneer de inspectiedienst een beroep heeft gedaan op de uitzondering bedoeld in paragraaf 2, wordt deze onmiddellijk opgeheven na het afsluiten van de controle. De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke stelt de betrokkene daarvan onverwijld in kennis.

5° toute personne physique dont les données à caractère personnel sont présentes au sein des produits TIC, services TIC ou processus TIC, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité.

Art. 37. § 1er. En application de l'article 23, paragraphe 1er, *c)*, e) et *h)*, 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), certaines obligations et droits prévus par ledit règlement sont limités ou exclus, conformément aux dispositions du présent article. Ces limitations ou exclusions ne portent pas préjudice à l'essence des libertés et droits fondamentaux et sont appliquées dans la stricte mesure nécessaire au but poursuivi.

§ 2. Les articles 12 à 16, 18 et 19 dudit règlement ne sont pas applicables aux traitements de données à caractère personnel, effectués par l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, agissant en tant que responsable de traitement des données, pour la finalité visée à l'article 36, § 1er, 2°, dans la mesure où l'exercice des droits consacrés par ces articles nuirait aux besoins du contrôle ou des actes préparatoires à celui-ci.

§ 3. L'exemption vaut, sous réserve du principe de proportionnalité et le cas échéant de minimisation des données, pour toutes les catégories de données à caractère personnel, dans la mesure où le traitement de ces données est conforme aux finalités précitées. Cette exemption vaut également pour les actes préparatoires ou pour les procédures visant à l'application éventuelle d'une sanction administrative.

§ 4. L'exemption ne s'applique que pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle ou d'actes préparatoires à celui-ci, dans la mesure où l'exercice des droits faisant l'objet de la dérogation visée au présent article nuirait aux besoins du contrôle ou des actes préparatoires à celui-ci et, en tous les cas, ne s'applique que jusqu'à un an après réception de la demande d'exercice du droit faisant l'objet de la dérogation prévue au présent article.

La durée des actes préparatoires, visés à l'alinéa 1er, pendant laquelle les articles visés au paragraphe 2 ne sont pas applicables, ne peut excéder un an à partir de la réception d'une demande relative à l'application d'un des droits consacrés par ces articles.

§ 5. Dès réception d'une demande concernant l'exercice d'un des droits consacrés par les articles visés au paragraphe 2, le délégué à la protection des données du responsable du traitement en accuse réception.

Le délégué à la protection des données du responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, de tout refus ou de toute limitation aux droits consacrés par les articles visés au paragraphe 2, ainsi que des motifs du refus ou de la limitation. Ces informations concernant le refus ou la limitation peuvent ne pas être fournies lorsque leur communication risque de compromettre la finalité énoncée au paragraphe 2. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

Le délégué à la protection des données du responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'Autorité de protection des données et de former un recours juridictionnel.

Le délégué à la protection des données du responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition de l'Autorité de protection des données.

Lorsque le service d'inspection a fait usage de l'exemption visée au paragraphe 2, cette dernière est immédiatement levée après la clôture du contrôle. Le délégué à la protection des données du responsable du traitement en informe la personne concernée sans délai.

Afdeling 2. — Bewaartermijn

Art. 38. Onverminderd de bewaring die noodzakelijk is voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, bedoeld in artikel 89 van Verordening (EU) 2016/679, bewaart de verwerkingsverantwoordelijke de persoonsgegevens die verwerkt worden door de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen om de doeleinden bedoeld in artikel 36, § 1, te realiseren, onverminderd eventuele beroepsprocedures, gedurende tien jaar na afloop van de verwerking.

HOOFDSTUK 9. — *Wijzigingsbepalingen*

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

Art. 39. Artikel 14, § 1, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, laatstelijk gewijzigd bij de wet van 17 februari 2022, wordt aangevuld met een bepaling onder 7°, luidende :

"7° het uitoefenen van 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 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit.".

Art. 40. In artikel 14, § 2, 3°, *g),* van dezelfde wet, ingevoegd bij de wet van 10 juli 2012, worden de woorden "met inbegrip van de beveiliging van netwerk- en informatiesystemen," ingevoegd tussen de woorden "openbare veiligheid," en de woorden "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. 41. Artikel 45 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, laatstelijk gewijzigd bij de wet van 23 februari 2022, 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 de hoofdstukken 5 en 6, met uitzondering van artikel 21 en 22, van de wet van 20 juli 2022 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 toezichtsopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens paragraaf 1, 2°, en de bijzondere wetten die het toezicht op de financiële instellingen regelen.".

Art. 42. Artikel 75, § 1, van dezelfde wet, laatstelijk gewijzigd bij de wet van 23 februari 2022, wordt aangevuld met een bepaling onder 27°, luidende :

"27° aan de autoriteit bedoeld in artikel 5, § 1, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit of 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. 43. In artikel 36/14, § 1, van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, ingevoegd bij het koninklijk besluit van 3 maart 2011 en laatstelijk gewijzigd bij de wet van 11 juli 2021, wordt een bepaling onder 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 20 juli 2022 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;".

Section 2. — Durée de conservation

Art. 38. Sans préjudice de la conservation nécessaire pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, visé à l'article 89 du règlement (UE) 2016/679, les données à caractère personnel traitées par l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 en vue de réaliser les finalités visées à l'article 36, § 1er, sont conservées, sans préjudice de recours éventuels, par le responsable du traitement dix ans après la fin du traitement effectué.

CHAPITRE 9. — *Dispositions modificatives*

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

Art. 39. L'article 14, § 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, modifié en dernier lieu par la loi du 17 février 2022, est complété par un 7° rédigé comme suit:

« 7° l'exercice des 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 20 juillet 2022 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. ».

Art. 40. Dans l'article 14, § 2, 3°, *g),* de la même loi, inséré par la loi du 10 juillet 2012, les mots « en ce compris la sécurité des réseaux et des systèmes d'information, » sont insérés entre les mots « sécurité publique, » et les mots « 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. 41. L'article 45 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, modifié en dernier lieu par la loi du 23 février 2022, est complété par un paragraphe 6, rédigé comme suit:

« § 6. À 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 20 juillet 2022 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. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, 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 1er, 2°, et des lois particulières qui régissent le contrôle des établissements financiers. ».

Art. 42. L'article 75, § 1er, de la même loi, modifié en dernier lieu par la loi du 23 février 2022, est complété par un 27°, rédigé comme suit :

« 27° à l'autorité visée à l'article 5, § 1er, de la loi du 20 juillet 2022 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 3. — Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 43. Dans l'article 36/14, § 1er, de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique, inséré par l'arrêté royal du 3 mars 2011 et modifié en dernier lieu par la loi du 11 juillet 2021, 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, § 1er, de la loi du 20 juillet 2022 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; ».

Art. 44. In hoofdstuk IV/4 van dezelfde wet, het organiek statuut van de Nationale Bank van België, ingevoegd bij de wet van 7 april 2019 en gewijzigd bij de wet van 11 juli 2021, 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 de hoofdstukken 5 en 6, met uitzondering van artikel 21 en 22, van de wet van 20 juli 2022 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 toezichtsopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens de artikelen 8 en 12bis en de bijzondere wetten die het toezicht op de financiële instellingen regelen.".

Afdeling 4. — Wijzigingen van het Wetboek van economisch recht

Art. 45. Artikel I.20 van het Wetboek van economisch recht, ingevoegd bij de wet van 17 juli 2013 en laatstelijk gewijzigd bij de wet van 8 mei 2022, wordt aangevuld met een bepaling onder 12º, luidende :

"12 ºCyberbeveiligingsverordening: 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. 46. In boek XV, titel 1, hoofdstuk 2, van hetzelfde Wetboek, ingevoegd bij de wet van 20 november 2013, wordt een afdeling 10 ingevoegd, luidende "Afdeling 10. Certificering van de cyberbeveiliging".

Art. 47. In afdeling 10, ingevoegd bij artikel 46, wordt een onderafdeling 1 ingevoegd, luidende "Onderafdeling 1. Vrijwillige cyberbeveiligingscertificering".

Art. 48. In onderafdeling 1, ingevoegd bij artikel 47, wordt een artikel XV.30/3 ingevoegd, luidende :

"Art. XV. 30/3. Op het gebied van vrijwillige cyberbeveiligingscertificering kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde opdrachten bedoeld in de hoofdstukken 5 en 6, met uitzondering van artikel 21 en 22, van de wet van 20 juli 2022 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. De FOD Economie vervult die toezichtsopdrachten enkel ten aanzien van producten of entiteiten die gereglementeerd 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. 49. In afdeling 10, ingevoegd bij artikel 46, wordt een onderafdeling 2 ingevoegd, luidende "Onderafdeling 2. Verplichte cyberbeveiligingscertificering".

Art. 50. In onderafdeling 2, ingevoegd bij artikel 49, wordt een artikel XV.30/4 ingevoegd, luidende:

"Art. XV.30/4. § 1. Met betrekking tot de Europese cyberbeveiligingscertificering die verplicht is op grond van de Europese of nationale wetgeving, na advies van de nationale cyberbeveiligingscertificeringsautoriteit, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, bepaalde toezichtsopdrachten in verband met de Cyberbeveiligingsverordening of in verband met de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, toevertrouwen aan bepaalde ambtenaren van de FOD Economie, op voorwaarde dat die laatste over de voor deze doeleinden vereiste expertise beschikt.

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

Art. 44. Dans le chapitre IV/4 de la même loi, inséré par la loi du 7 avril 2019 et modifié par la loi du 11 juillet 2021, il est inséré un article 36/48/1 rédigé comme suit: :

« Art. 36/48/1. À 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 20 juillet 2022 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. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, 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 12bis et des lois particulières qui régissent le contrôle des établissements financiers. ».

Section 4. — Modifications du Code de droit économique

Art. 45. L'article I.20 du Code de droit économique, inséré par la loi du 17 juillet 2013 et modifié en dernier lieu par la loi du 8 mai 2022, est complété par un 12º rédigé comme suit: :

« 12º 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. »

Art. 46. Dans le livre XV, titre 1er, chapitre 2, du même Code, inséré par la loi du 20 novembre 2013, il est inséré une section 10 intitulée « Section 10. Certification de cybersécurité ».

Art. 47. Dans la section 10, insérée par l'article 46, il est inséré une sous-section 1re intitulée « Sous-section 1re. Certification de cybersécurité volontaire ».

Art. 48. Dans la sous-section 1re, insérée par l'article 47, il est inséré un article XV.30/3, rédigé comme suit:

« Art. XV.30/3. En matière de certification de cybersécurité volontaire, 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 20 juillet 2022 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 Économie, à condition que le SPF Économie dispose de l'expertise requise à ces fins. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, de la loi précitée. Le SPF Économie 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. 49. Dans la section 10, insérée par l'article 46, il est inséré une sous-section 2 intitulée « Sous-section 2. Certification de cybersécurité obligatoire ».

Art. 50. Dans la sous-section 2, insérée par l'article 49, il est inséré un article XV.30/4, rédigé comme suit:

« Art. XV.30/4. § 1er. En matière de certification européenne de cybersécurité rendue obligatoire en vertu du droit de l'Union ou du droit national, 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 20 juillet 2022 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 Économie, à condition que ce dernier dispose de l'expertise requise à ces fins.

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

Art. 51. 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.125/4/1 en XV.125/4/2 ingevoegd, luidende :

"Art. XV.125/4/1. Wordt in het kader van het toezicht bedoeld in artikel XV.30/4 gestraft met een sanctie van niveau 2 :

1° de houder van een cyberbeveiligingscertificaat dat verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "basis" die niet voldoet aan de verplichtingen die voortvloeien uit de overeenstemmende Europese cyberbeveiligingscertificeringsregeling;

2° eenieder die niet meewerkt tijdens een inspectie door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken of die anderszins weigert mee te werken tijdens een inspectie.

Art. XV.125/4/2. Wordt in het kader van het toezicht bedoeld in artikel XV.30/4 gestraft met een sanctie van niveau 3 :

1° de houder van een cyberbeveiligingscertificaat dat 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 overeenstemmende 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.".

HOOFDSTUK 10. — *Inwerkingtreding*

Art. 52. Deze wet treedt in werking de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

Kondigen deze wet af, bevelen dat zij met 's Lands zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te Brussel, 20 juli 2022.

FILIP

Van Koningswege :
De eerste minister,
A. DE CROO
De minister van Economie,
P.-Y. DERMAGNE
De minister van Financiën,
belast met de coördinatie van de fraudebestrijding,
V. VAN PETEGHEM
De minister van Telecommunicatie en Post,
P. DE SUTTER
Met 's Lands zegel gezegeld :
De minister van Justitie,
V. VAN QUICKENBORNE

Nota

Kamer van volksvertegenwoordigers (www.dekamer.be) :
Stukken : 55 - 2693/6
Integraal verslag: 14 Juli 2022

Art. 51. 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.125/4/1 et XV.125/4/2, rédigés comme suit: :

« Art. XV.125/4/1. Dans le cadre de la surveillance visée 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 en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle ou ne coopère pas lors d'un contrôle de toute autre manière.

Art. XV.125/4/2. Dans le cadre de la surveillance visée 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 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. ».

CHAPITRE 10. — *Entrée en vigueur*

Art. 52. La présente loi entre en vigueur le jour de sa publication au *Moniteur belge*.

Promulguons la présente loi, ordonnons qu'elle soit revêtue du sceau de l'État et publiée par le *Moniteur belge*.

Donné à Bruxelles, le 20 juillet 2022.

PHILIPPE

Par le Roi :
Le Premier Ministre,
A. DE CROO
Le ministre de l'Économie,
P.-Y. DERMAGNE
Le ministre des Finances,
chargé de la Coordination de la lutte contre la fraude,
V. VAN PETEGHEM
La ministre des Télécommunications et de la Poste,
P. DE SUTTER
Scellé du Sceau de l'Etat :
Le Ministre de la Justice,
V. VAN QUICKENBORNE

Note

Chambres des représentants (www.lachambre.be) :
Documents : 55 - 2693/6
Compte rendu intégral : 14 juillet 2022

FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2022/15455]

14 JULI 2022. — Wet tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

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

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

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

Art. 2. In artikel 3 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, laatstelijk gewijzigd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° de Franse tekst van de bepaling onder 4° wordt aangevuld met de woorden "des Forces Armées";

SERVICE PUBLIC FEDERAL JUSTICE

[C − 2022/15455]

14 JUILLET 2022. — Loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

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

La Chambre des représentants a adopté et Nous sanctionnons ce qui suit :

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. À l'article 3 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, modifié en dernier lieu par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° le 4° est complété par les mots "des Forces armées";