JUSTEL - Geconsolideerde wetgeving

http://www.ejustice.just.fgov.be/eli/wet/2022/07/20/2022204364/justel

Dossiernummer : 2022-07-20/11

Titel

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

Bron : KANSELARIJ VAN DE EERSTE MINISTER

Publicatie : Belgisch Staatsblad van 05-08-2022 bladzijde : 60924

Inwerkingtreding : 05-08-2022

Inhoudstafel

Tekst

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.

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.

§ 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.
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 Cyber-beveiligingsverordening 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 Cyber-beveiligingsverordening 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 Cyber-beveiligingsverordening 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.

§ 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.

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.
§ 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;

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;

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 Cyber-beveiligingsverordening trekt de autoriteit bedoeld in artikel 5, § 1, een cyberbeveiligingscertificaat in als de begunstigde de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft.

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

Art. 22. Overeenkomstig artikel 58, lid 7, e), van de Cyber-beveiligingsverordening 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.

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 Cyber-beveiligingsverordening 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. 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 Cyber-beveiligingsverordening 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.
§ 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;

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.

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;".

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 12°, luidende :
"12 °Cyberbeveiligingsverordening: Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr.

526/2013."

Art. 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. 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.