EUROPESE
COMMISSIE

Brussel, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020

(Voor de EER relevante tekst)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

Hardware- en softwareproducten worden steeds vaker getroffen door geslaagde cyberaanvallen, waardoor de jaarlijkse kosten van cybercriminaliteit wereldwijd tegen 2021 naar schatting 5,5 biljoen EUR bedragen. Dergelijke producten hebben te kampen met twee grote problemen die voor de gebruikers en de samenleving extra kosten met zich meebrengen: 1) een laag niveau van cyberbeveiliging, wat tot uiting komt in wijdverbreide kwetsbaarheden en de ontoereikende en inconsistente verstrekking van beveiligingsupdates om deze aan te pakken, en 2) onvoldoende inzicht in en toegang tot informatie door gebruikers, waardoor zij niet in staat zijn producten met passende cyberbeveiligingskenmerken te kiezen of deze op een veilige manier te gebruiken. In een verbonden omgeving kan een cyberbeveiligingsincident in één product gevolgen hebben voor een hele organisatie of een hele toeleveringsketen en zich vaak binnen enkele minuten over de grenzen van de interne markt verspreiden. Dit kan leiden tot een ernstige verstoring van de economische en sociale activiteiten of zelfs levensbedreigend worden.

De cyberbeveiliging van producten met digitale elementen heeft een sterke grensoverschrijdende dimensie, aangezien producten die in één land worden vervaardigd, vaak op de gehele interne markt worden gebruikt. Daarnaast verspreiden incidenten die aanvankelijk één entiteit of één lidstaat betroffen, zich vaak binnen enkele minuten over de interne markt.

Hoewel de bestaande internemarktwetgeving van toepassing is op bepaalde producten met digitale elementen, vallen de meeste hardware- en softwareproducten momenteel niet onder EU-wetgeving inzake cyberbeveiliging. Het huidige rechtskader van de EU heeft met name geen betrekking op de cyberbeveiliging van niet-ingebedde software, ook al zijn cyberaanvallen steeds vaker gericht op kwetsbaarheden in deze producten, wat aanzienlijke maatschappelijke en economische kosten met zich meebrengt. Er zijn talrijke voorbeelden van opzienbarende cyberaanvallen als gevolg van suboptimale productbeveiliging, zoals de ransomware-worm WannaCry, die gebruikmaakte van een zwakke plek in Windows en in 2017 200 000 computers in 150 landen trof en een schade van miljarden USD veroorzaakte; de aanval op de toeleveringsketen van Kaseya VSA, waarbij de software voor netwerkbeheer van Kaseya werd gebruikt voor een aanval op meer dan 1 000 bedrijven en een supermarktketen werd gedwongen om al haar 500 winkels in Zweden te sluiten; of de vele incidenten waarbij toepassingen voor thuisbankieren worden gehackt om geld van nietsvermoedende consumenten te stelen.

Er werden twee hoofddoelstellingen vastgesteld om de goede werking van de interne markt te waarborgen: 1) de voorwaarden scheppen voor de ontwikkeling van veilige producten met digitale elementen door ervoor te zorgen dat hardware- en softwareproducten met minder kwetsbaarheden in de handel worden gebracht en dat fabrikanten de beveiliging gedurende de hele levenscyclus van een product serieus nemen; en 2) de voorwaarden scheppen die gebruikers in staat stellen rekening te houden met cyberbeveiliging bij het selecteren en gebruiken van producten met digitale elementen. Er werden vier specifieke doelstellingen geformuleerd: i) ervoor zorgen dat fabrikanten de beveiliging van producten met digitale elementen verbeteren vanaf de ontwerp- en ontwikkelingsfase en gedurende de gehele levenscyclus; ii) zorgen voor een samenhangend cyberbeveiligingskader, waardoor naleving voor hardware- en softwarefabrikanten gemakkelijker wordt; iii) de beveiligingskenmerken

van producten met digitale elementen transparanter maken, en iv) bedrijven en consumenten in staat stellen producten met digitale elementen veilig te gebruiken.

De sterke grensoverschrijdende aard van cyberbeveiliging en de toenemende incidenten, met spillover-effecten over grenzen, sectoren en producten heen, maken dat de doelstellingen niet doeltreffend door de lidstaten afzonderlijk kunnen worden verwezenlijkt. Gezien het mondiale karakter van markten voor producten met digitale elementen lopen de lidstaten dezelfde risico's voor hetzelfde product met digitale elementen op hun grondgebied. Een opkomend versnipperd kader van potentieel uiteenlopende nationale voorschriften dreigt een open en concurrerende eengemaakte markt voor producten met digitale elementen in de weg te staan. Een gezamenlijk optreden op EU-niveau is dan ook noodzakelijk om een hoog niveau van vertrouwen onder de gebruikers tot stand te brengen en de aantrekkelijkheid van EU-producten met digitale elementen te vergroten. Het zou ook de interne markt ten goede komen door rechtszekerheid te bieden en een gelijk speelveld tot stand te brengen voor verkopers van producten met digitale elementen, zoals ook wordt benadrukt in het eindverslag van de Conferentie over de toekomst van Europa, waarin burgers pleiten voor een sterkere rol voor de EU bij de bestrijding van cyberdreigingen.

- **Wisselwerking met bestaande bepalingen op het beleidsterrein**

Het EU-kader omvat verschillende horizontale wetgevingsteksten met betrekking tot bepaalde aspecten die verband houden met cyberbeveiliging vanuit verschillende hoeken (producten, diensten, crisisbeheersing en criminaliteit). In 2013 is de richtlijn over aanvallen op informatiesystemen[1] in werking getreden, waarbij de strafbaarstelling en de straffen voor een aantal strafbare feiten tegen informatiesystemen werden geharmoniseerd. In augustus 2016 is Richtlijn (EU) 2016/1148 betreffende de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn)[2] in werking getreden als eerste EU-wetgevingstekst inzake cyberbeveiliging. De herziening ervan, die resulteerde in Richtlijn [Richtlijn XXX/XXXX (NIS2)], verhoogt het gemeenschappelijke ambitieniveau van de EU. In 2019 trad de cyberbeveiligingsverordening[3] van de EU in werking, die tot doel heeft de beveiliging van ICT-producten, -diensten en -processen te verbeteren door een vrijwillig Europees kader voor cyberbeveiligingscertificering in te voeren[4].

De cyberbeveiliging van de gehele toeleveringsketen wordt alleen gewaarborgd als alle onderdelen ervan cyberbeveiligd zijn. De bovengenoemde EU-wetgeving vertoont in dit opzicht echter aanzienlijke lacunes, aangezien zij geen betrekking heeft op verplichte eisen voor de beveiliging van producten met digitale elementen.

---

1 Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PB L 218 van 14.8.2013, blz. 8).

2 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

3 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 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

4 De cyberbeveiligingsverordening maakt de ontwikkeling van specifieke certificeringsregelingen mogelijk. Elke regeling bevat verwijzingen naar relevante normen, technische specificaties of andere cyberbeveiligingsvoorschriften die in de regeling zijn omschreven. Het besluit om een cyberbeveiligingscertificering te ontwikkelen is risicogebaseerd.

Terwijl de voorgestelde verordening cyberweerbaarheid betrekking heeft op producten met digitale elementen die in de handel worden gebracht, is Richtlijn [Richtlijn XXX/XXX (NIS2)] gericht op het waarborgen van een hoog niveau van cyberbeveiliging van diensten die door essentiële en belangrijke entiteiten worden verleend. Richtlijn [Richtlijn XXX/XXXX (NIS2)] verplicht de lidstaten ervoor te zorgen dat essentiële en belangrijke entiteiten die binnen het toepassingsgebied vallen, zoals overheidsinstanties en aanbieders van gezondheidszorg of clouddiensten, passende en evenredige technische, operationele en organisatorische cyberbeveiligingsmaatregelen nemen. Dit omvat onder meer de verplichting om de beveiliging bij de verwerving, de ontwikkeling en het onderhoud van netwerk- en informatiesystemen te waarborgen, met inbegrip van de respons op en de bekendmaking van kwetsbaarheden. Richtlijn [Richtlijn XXX/XXXX (NIS2)] verplicht de Commissie binnen 21 maanden na de datum van inwerkingtreding van deze richtlijn voor bepaalde soorten entiteiten, zoals aanbieders van cloudcomputerdiensten, uitvoeringshandelingen vast te stellen waarin de technische en methodologische eisen van die maatregelen worden vastgelegd. Voor alle andere entiteiten kan de Commissie een uitvoeringshandeling aannemen om de technische en methodologische eisen alsmede de sectorale eisen vast te stellen. Dit kader zal ervoor zorgen dat technische specificaties en maatregelen die vergelijkbaar zijn met de essentiële cyberbeveiligingsvereisten van de verordening cyberweerbaarheid, ook worden ingevoerd voor het ontwerp, de ontwikkeling en de respons op kwetsbaarheden van software die als dienst wordt geleverd (Software-as-a-Service). Dit kan bijvoorbeeld een middel zijn om een hoog niveau van cyberbeveiliging te waarborgen bij systemen voor elektronische patiëntendossiers (EPD-systemen), ook wanneer deze worden geleverd als Software-as-a-Service (SaaS) of worden ontwikkeld binnen zorginstellingen (intern), overeenkomstig de voorgestelde [verordening betreffende de Europese ruimte voor gezondheidsgegevens].

- **Wisselwerking met andere beleidsterreinen van de Unie**

Zoals uiteengezet in de mededeling "De digitale toekomst van Europa vormgeven"[5] is het van cruciaal belang dat de EU alle vruchten van het digitale tijdperk plukt en haar industrie en innovatiecapaciteit versterkt, binnen veilige en ethische grenzen. De Europese datastrategie bevat vier pijlers — gegevensbescherming, grondrechten, veiligheid en cyberbeveiliging — als essentiële voorwaarden voor een samenleving die zich verder ontwikkelt door gegevens te gebruiken.

Het huidige EU-kader[6] dat van toepassing is op producten die mogelijk ook digitale elementen bevatten, omvat verschillende wetgevingsteksten, waaronder EU-wetgeving inzake specifieke producten met betrekking tot veiligheidsgerelateerde aspecten en algemene wetgeving inzake productaansprakelijkheid. Het voorstel is in overeenstemming met het huidige productgerelateerde regelgevingskader van de EU en met recente wetgevingsvoorstellen, zoals het voorstel van de Commissie voor Verordening [de verordening artificiële intelligentie (AI)][7].

De voorgestelde verordening zou van toepassing zijn op alle radioapparatuur die binnen het toepassingsgebied van Gedelegeerde Verordening (EU) 2022/30 van de Commissie valt.

---

5 Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's — De digitale toekomst van Europa vormgeven (COM(2020) 67 final van 19.2.2020).

6 Voornamelijk wetgeving van het nieuwe wetgevingskader (NWK).

7 Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie (COM(2021) 206 final van 21.4.2021).

Bovendien omvatten de bij deze verordening vastgestelde eisen alle elementen van de essentiële eisen als bedoeld in artikel 3, lid 3, punten d), e) en f), van Richtlijn 2014/53/EU, met inbegrip van de belangrijkste elementen die zijn uiteengezet in [Uitvoeringsbesluit XXX/2022 van de Commissie betreffende een normalisatieverzoek aan de Europese normalisatieorganisaties], dat op basis van die gedelegeerde verordening is uitgevaardigd. Om overlappingen in de regelgeving te voorkomen, is het de bedoeling dat de Commissie de gedelegeerde verordening intrekt of wijzigt met betrekking tot de radioapparatuur die onder de voorgestelde verordening valt, zodat deze laatste hierop van toepassing zou zijn zodra zij in werking treedt.

Om dubbel werk te voorkomen, is het bovendien de bedoeling dat de Commissie en de Europese normalisatieorganisaties bij de voorbereiding en ontwikkeling van geharmoniseerde normen rekening houden met de normalisatiewerkzaamheden die zijn verricht in het kader van Uitvoeringsbesluit C(2022) 5637 van de Commissie betreffende een normalisatieverzoek voor Gedelegeerde Verordening (EU) 2022/30 tot aanvulling van de richtlijn radioapparatuur om de uitvoering van de verordening te vergemakkelijken.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

De rechtsgrondslag van dit voorstel is artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU), dat voorziet in de vaststelling van maatregelen om de oprichting en werking van de interne markt te waarborgen. Doel van het voorstel is de cyberbeveiligingsvereisten voor producten met digitale elementen in alle lidstaten te harmoniseren en belemmeringen voor het vrije verkeer van goederen weg te nemen.

Artikel 114 VWEU kan als rechtsgrondslag worden gebruikt om te voorkomen dat deze belemmeringen zich voordoen als gevolg van uiteenlopende nationale wetgevingen en benaderingen voor het aanpakken van de rechtsonzekerheid en lacunes in de bestaande rechtskaders[8]. Voorts heeft het Hof van Justitie van de Europese Unie erkend dat de toepassing van heterogene technische voorschriften een geldige reden kan zijn om artikel 114 VWEU in werking te doen treden[9].

Het huidige wetgevingskader van de EU dat van toepassing is op producten met digitale elementen, is gebaseerd op artikel 114 VWEU en omvat verschillende wetgevingsteksten, onder meer inzake specifieke producten en veiligheidsgerelateerde aspecten en algemene wetgeving inzake productaansprakelijkheid. Het bestrijkt echter slechts bepaalde aspecten die verband houden met de cyberbeveiliging van materiële digitale producten en, in voorkomend geval, software die in deze producten is ingebed. Op nationaal niveau beginnen de lidstaten nationale maatregelen te nemen om verkopers van digitale producten te verplichten hun cyberbeveiliging te verbeteren[10]. Tegelijkertijd heeft de cyberbeveiliging van digitale producten een sterke grensoverschrijdende dimensie, aangezien producten die in één land worden vervaardigd vaak door organisaties en consumenten op de gehele interne markt

8 Arrest van het Hof (Grote kamer) van 3 december 2019, Tsjechische Republiek/Parlement en Raad, C-482/17, punt 35.

9 Arrest van het Hof (Grote kamer) van 2 mei 2006, Verenigd Koninkrijk/Parlement en Raad, C-217/04, punten 62-63.

10 Zo heeft Finland in 2019 een etiketteringsregeling voor IoT-apparaten ingevoerd, zoals smart tv's, smartphones en speelgoed op basis van de ETSI-normen. Duitsland heeft onlangs een etiket voor de veiligheid van de consument ingevoerd voor breedbandrouters, smart tv's, camera's, luidsprekers, speelgoed en schoonmaak- en tuinrobots.

worden gebruikt. Incidenten die aanvankelijk één entiteit of lidstaat betreffen, verspreiden zich vaak binnen enkele minuten over organisaties, sectoren en verschillende lidstaten.

Met de verschillende rechtshandelingen en initiatieven die tot dusver op EU- en nationaal niveau zijn genomen, worden de vastgestelde problemen slechts gedeeltelijk aangepakt en bestaat het risico dat er binnen de interne markt een lappendeken van wetgeving ontstaat, waardoor de rechtsonzekerheid voor zowel verkopers als gebruikers van deze producten toeneemt en bedrijven onnodig worden belast om aan een groot aantal vereisten voor soortgelijke producten te voldoen.

De voorgestelde verordening zou het regelgevingslandschap van de EU harmoniseren en stroomlijnen door cyberbeveiligingsvereisten in te voeren voor producten met digitale elementen, en zou overlappende voorschriften uit verschillende wetgevingsteksten vermijden. Dit zou leiden tot meer rechtszekerheid voor marktdeelnemers en gebruikers in de hele Unie en tot een betere harmonisatie van de Europese eengemaakte markt, waardoor de voorwaarden voor exploitanten die de EU-markt willen betreden, worden verbeterd.

- **Subsidiariteit (bij niet-exclusieve bevoegdheid)**

De sterke grensoverschrijdende aard van cyberbeveiliging in het algemeen en het toenemende aantal risico's en incidenten, die spillover-effecten over grenzen, sectoren en producten heen hebben, maken dat de doelstellingen van de huidige interventie niet doeltreffend door de lidstaten afzonderlijk kunnen worden verwezenlijkt. Een aanpak van de problemen op nationaal niveau, en met name een aanpak waarbij verplichte vereisten worden ingevoerd, zal leiden tot verdere rechtsonzekerheid en juridische belemmeringen. Ondernemingen kunnen daarbij worden belet zich vlot uit te breiden naar andere lidstaten, waardoor gebruikers de voordelen van hun producten mislopen.

Een gezamenlijk optreden op EU-niveau is dan ook noodzakelijk om een hoog niveau van vertrouwen onder de gebruikers tot stand te brengen en de aantrekkelijkheid van EU-producten met digitale elementen te vergroten. Het zou ook de digitale eengemaakte markt en de interne markt in het algemeen ten goede komen door rechtszekerheid te bieden en een gelijk speelveld tot stand te brengen voor fabrikanten van producten met digitale elementen.

Uiteindelijk wordt de Commissie in de conclusies van de Raad van 23 mei 2022 over de invoering van een cyberstrategie van de Europese Unie verzocht om uiterlijk eind 2022 gemeenschappelijke cyberbeveiligingsvereisten voor verbonden apparaten voor te stellen.

- **Evenredigheid**

Wat de evenredigheid van de voorgestelde verordening betreft, zouden de maatregelen in de onderzochte beleidsopties niet verder gaan dan wat nodig is om de algemene en specifieke doelstellingen te verwezenlijken en zouden zij geen onevenredige kosten met zich meebrengen. Meer in het bijzonder zou de betrokken interventie ervoor zorgen dat producten met digitale elementen beveiligd zijn gedurende hun gehele levenscyclus en in verhouding tot de risico's die zij lopen, door middel van doelgerichte en technologieneutrale vereisten die redelijk zijn en in het algemeen overeenstemmen met het belang van de betrokken entiteiten.

De essentiële cyberbeveiligingsvereisten in het voorstel bouwen voort op wijdverbreid gebruikte normen en het normalisatieproces dat zal volgen, zou rekening houden met de technische specifieke kenmerken van de producten. Dit betekent dat beveiligingscontroles zouden worden aangepast wanneer dat nodig is voor een bepaald risiconiveau. Bovendien zouden de beoogde horizontale regels alleen voor kritieke producten voorzien in beoordelingen door derden. Dit zou slechts een klein deel van de markt voor producten met

digitale elementen betreffen. De gevolgen voor kmo's zouden afhangen van hun aanwezigheid op de markt van deze specifieke categorieën producten.

Wat de evenredigheid van de kosten voor de conformiteitsbeoordeling betreft, houden aangemelde instanties die beoordelingen door derden uitvoeren, bij de vaststelling van hun vergoedingen rekening met de omvang van de onderneming. Er zou ook worden voorzien in een redelijke overgangsperiode van 24 maanden voor de voorbereiding van de uitvoering, waardoor de betrokken markten de tijd hebben om zich voor te bereiden en tegelijkertijd een duidelijke koers wordt aangegeven voor O&O-investeringen. De nalevingskosten voor bedrijven zouden worden gecompenseerd door de voordelen van een hogere mate van beveiliging van producten met digitale elementen en een daaruit voortvloeiende toename van het vertrouwen in deze producten bij de gebruikers.

- **Keuze van het instrument**

Een regelgevingsinterventie zou de vaststelling inhouden van een verordening en niet van een richtlijn. De reden hiervoor is dat een verordening voor dit specifieke type productwetgeving de vastgestelde problemen doeltreffender zou aanpakken en de geformuleerde doelstellingen beter zou verwezenlijken, aangezien het een interventie betreft die voorwaarden stelt aan het in de handel brengen van een zeer brede categorie producten op de interne markt. Het omzettingsproces in het geval van een richtlijn voor een dergelijke interventie zou op nationaal niveau te veel speelruimte kunnen laten, wat kan leiden tot een gebrek aan uniformiteit van bepaalde essentiële cyberbeveiligingsvereisten, rechtsonzekerheid, verdere versnippering of zelfs discriminatie over de grenzen heen, des te meer vanwege het feit dat de betrokken producten voor meerdere doeleinden of toepassingen kunnen dienen en dat fabrikanten meerdere categorieën van dergelijke producten kunnen produceren.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- **Raadpleging van belanghebbenden**

De Commissie heeft een breed scala aan belanghebbenden geraadpleegd. De lidstaten en belanghebbenden werden uitgenodigd om deel te nemen aan de openbare raadpleging en aan de enquêtes en workshops die werden georganiseerd in het kader van een studie ter ondersteuning van de voorbereidende werkzaamheden van de Commissie voor de effectbeoordeling, die door een consortium werd uitgevoerd: Wavestone, het Centrum voor Europese Beleidsstudies (CEPS) en ICF. Tot de geraadpleegde belanghebbenden behoorden nationale markttoezichtautoriteiten, organen van de Unie die zich bezighouden met cyberbeveiliging, fabrikanten en importeurs van hardware en software, bedrijfsverenigingen, consumentenorganisaties en gebruikers van producten met digitale elementen en burgers, onderzoekers en academici, aangemelde instanties, accreditatie-instanties en professionals uit de cyberbeveiligingssector.

De raadplegingsactiviteiten omvatten:

- Een eerste studie uitgevoerd door een consortium bestaande uit ICF, Wavestone, Carsa en CEPS, gepubliceerd in december 2021[11]. In de studie

[11] *Study on the need of Cybersecurity requirements for ICT products — No. 2020-0715, Final Study Report*, beschikbaar op https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products

werden verschillende tekortkomingen van de markt vastgesteld en werden mogelijke regelgevingsmaatregelen beoordeeld.

- Een openbare raadpleging van burgers, belanghebbenden en deskundigen op het gebied van cyberbeveiliging. Er werden 176 antwoorden ingediend. Daarbij werden uiteenlopende meningen en ervaringen van alle groepen belanghebbenden verzameld.
- De workshops die werden georganiseerd in het kader van de studie ter ondersteuning van de voorbereidende werkzaamheden van de Commissie voor de verordening cyberweerbaarheid, werden bijgewoond door ongeveer 100 vertegenwoordigers uit alle 27 lidstaten, die verschillende belanghebbenden vertegenwoordigden.
- Er werden gesprekken met deskundigen gevoerd om meer inzicht te krijgen in de huidige problemen op het gebied van cyberbeveiliging in verband met producten met digitale elementen, en om beleidsopties voor een mogelijke regelgevingsinterventie te bespreken.
- Er vonden bilaterale besprekingen plaats met nationale cyberbeveiligingsautoriteiten, de particuliere sector en consumentenorganisaties.
- De belangrijkste belanghebbende kmo's werden gericht aangezocht.

- **Bijeenbrengen en gebruik van expertise**

De raadplegingsactiviteiten waren bedoeld om input te verkrijgen voor de vijf belangrijkste evaluatiecriteria van de richtsnoeren voor betere regelgeving van de EU (doeltreffendheid, efficiëntie, relevantie, samenhang, toegevoegde waarde voor de EU) en over de potentiële gevolgen van mogelijke opties voor de toekomst. De contractant heeft niet alleen contact opgenomen met de belanghebbenden waarvoor de voorgestelde verordening rechtstreeks gevolgen zou hebben, maar heeft ook overleg gepleegd met een breed scala aan deskundigen op het gebied van cyberbeveiliging.

- **Effectbeoordeling**

De Commissie heeft voor dit voorstel een effectbeoordeling uitgevoerd, die door de Raad voor regelgevingstoetsing van de Commissie is onderzocht. Op 6 juli 2022 heeft een vergadering met de Raad voor regelgevingstoetsing plaatsgevonden, waaruit een positief advies is voortgevloeid. De effectbeoordeling werd aangepast om gevolg te geven aan de aanbevelingen en opmerkingen van de Raad voor regelgevingstoetsing.

De Commissie heeft verschillende beleidsopties onderzocht om de algemene doelstelling van het voorstel te verwezenlijken:

- Zachte wetgeving en vrijwillige maatregelen (optie 1): deze optie zou geen verplichte regelgevingsinterventie omvatten. In plaats daarvan zou de Commissie mededelingen, richtsnoeren, aanbevelingen en eventueel gedragscodes publiceren om vrijwillige maatregelen aan te moedigen. Nationale regelingen, al dan niet verplicht, zouden verder worden ontwikkeld om het gebrek aan horizontale EU-regels te compenseren.
- Ad-hocregelgeving voor cyberbeveiliging van materiële producten met digitale elementen en bijbehorende ingebedde software (optie 2): deze optie zou een productspecifieke ad-hoc-regelgevingsinterventie omvatten die beperkt zou

blijven tot het toevoegen en/of wijzigen van de cyberbeveiligingsvereisten in de reeds bestaande wetgeving of tot het invoeren van nieuwe wetgeving naarmate er nieuwe risico's ontstaan, eventueel ook met betrekking tot niet-ingebedde software.

De opties 3 en 4 omvatten een horizontale regelgevingsinterventie die qua reikwijdte varieert, grotendeels in overeenstemming met het nieuwe wetgevingskader (NWK). Dit kader bevat essentiële eisen als voorwaarde voor het in de handel brengen van bepaalde producten op de interne markt. Het NWK voorziet doorgaans ook in conformiteitsbeoordeling, de procedure die door de fabrikant wordt gevolgd om aan te tonen dat aan de specifieke productvereisten is voldaan.

- Een gemengde aanpak met horizontale verplichte regels voor cyberbeveiliging van materiële producten met digitale elementen en bijbehorende ingebedde software en een gespreide aanpak voor niet-ingebedde software (optie 3): deze optie zou een verordening omvatten waarbij horizontale cyberbeveiligingsvereisten worden ingevoerd voor alle materiële producten met digitale elementen en de daarin ingebedde software, als voorwaarde voor het in de handel brengen ervan, en zou twee subopties omvatten met en zonder een verplichte beoordeling door derden (3i en 3ii). Niet-ingebedde software zou niet worden gereguleerd.
- Een horizontale regelgevingsinterventie waarbij cyberbeveiligingsvereisten worden ingevoerd voor een breed scala aan materiële en immateriële producten met digitale elementen, met inbegrip van niet-ingebedde software (optie 4): deze optie lijkt, met uitzondering van het toepassingsgebied, op optie 3. Bij optie 4 zou niet-ingebedde software (met twee subopties die respectievelijk alleen kritieke (4a) of alle software (4b) omvatten) binnen het toepassingsgebied vallen van een potentiële verordening. Voor elke suboptie zouden dezelfde subopties met betrekking tot conformiteitsbeoordelingen als die voor optie 3 worden overwogen.

Optie 4 (met subopties die alle software dekken en met verplichte beoordeling door derden voor kritieke producten) bleek de voorkeursoptie te zijn op basis van de beoordeling van de doeltreffendheid ten aanzien van de specifieke doelstellingen en de efficiëntie met betrekking tot kosten en baten. Deze optie zou de vaststelling van specifieke horizontale cyberbeveiligingsvereisten waarborgen voor alle producten met digitale elementen die op de interne markt in de handel worden gebracht of worden aangeboden, en is de enige optie die de hele digitale toeleveringsketen bestrijkt. Niet-ingebedde software, die vaak kwetsbaarheden bevat, zou ook onder een dergelijke regelgevingsinterventie vallen, waardoor een coherente aanpak van alle producten met digitale elementen wordt gewaarborgd, en waarbij de verschillende marktdeelnemers een duidelijk aandeel in de verantwoordelijkheden hebben.

Deze beleidsoptie heeft ook een toegevoegde waarde doordat rekening wordt gehouden met zorgplicht en aspecten van de hele levenscyclus na het in de handel brengen van de producten met digitale elementen, om onder meer te zorgen voor passende informatie over beveiligingsondersteuning en de verstrekking van beveiligingsupdates. Deze beleidsoptie zou bovendien de meest doeltreffende manier zijn om de recente herziening van het NIS-kader aan te vullen door de voorwaarden voor een betere beveiliging van de toeleveringsketen te waarborgen.

De voorkeursoptie zou aanzienlijke voordelen opleveren voor de verschillende belanghebbenden. Voor bedrijven zouden uiteenlopende beveiligingsregels voor producten met digitale elementen worden voorkomen en zouden de nalevingskosten op het gebied van

de betrokken cyberbeveiligingswetgeving dalen. Het aantal cyberincidenten, de kosten voor incidentenbehandeling en de reputatieschade zouden worden beperkt. Voor de hele EU kan het initiatief de geraamde kosten als gevolg van incidenten in bedrijven doen dalen met grofweg 180 tot 290 miljard EUR per jaar. Dit zou leiden tot een hogere omzet als gevolg van de vraag naar producten met digitale elementen. Het zou de wereldwijde reputatie van bedrijven verbeteren, waardoor ook de vraag van buiten de EU zou stijgen. Voor gebruikers zou de voorkeursoptie de transparantie van de beveiligingseigenschappen vergroten en het gebruik van producten met digitale elementen vergemakkelijken. Consumenten en burgers zouden ook een betere bescherming genieten van hun grondrechten, zoals privacy en gegevensbescherming.

Met betrekking tot de vraag om de doeltreffendheid van de beleidsmaatregelen te beoordelen, waren de respondenten van de openbare raadpleging het erover eens dat optie 4 de meest doeltreffende maatregel zou zijn (4,08 op een schaal van 1 tot 5). Hiertoe behoorden consumentenorganisaties (5,00), respondenten die zichzelf als gebruikers identificeren (4,22), aangemelde instanties (4,17), markttoezichtautoriteiten (5,00) en fabrikanten van producten met digitale elementen (3,85), waaronder kleine en middelgrote ondernemingen (4,05).

- **Resultaatgerichtheid en vereenvoudiging**

Bij dit voorstel worden eisen vastgelegd die van toepassing zullen zijn op fabrikanten van software en hardware. Er moet voor rechtszekerheid worden gezorgd en verdere marktversnippering van productgerelateerde eisen op het gebied van cyberbeveiliging op de interne markt moet worden voorkomen, hetgeen is aangetoond door de brede ondersteuning van de verschillende belanghebbenden voor een horizontale interventie. Het voorstel zal de regeldruk voor fabrikanten vanwege verschillende wetten inzake productveiligheid tot een minimum beperken. De afstemming op het NWK betekent een betere werking van de interventie en de handhaving ervan. Het voorstel stroomlijnt de vrijwaringsprocedures door fabrikanten en lidstaten te betrekken voordat de Commissie in kennis wordt gesteld. Een groot deel van de fabrikanten die binnen het toepassingsgebied van het voorstel vallen, is reeds vertrouwd met de werking van het NWK, wat zal bijdragen tot het begrip en de uitvoering ervan. Voor consumenten en bedrijven zal het voorstel het vertrouwen in producten met digitale elementen bevorderen.

- **Grondrechten**

Alle beleidsopties zullen naar verwachting tot op zekere hoogte zorgen voor een betere bescherming van grondrechten en fundamentele vrijheden als privacy, bescherming van persoonsgegevens, vrijheid van ondernemerschap en bescherming van eigendom of persoonlijke waardigheid en integriteit. Met name voorkeursoptie 4, die bestaat uit horizontale regelgevingsinterventies en een breed beleidsperspectief heeft, zou in dit opzicht het meest doeltreffend zijn, aangezien deze optie de meeste mogelijkheden biedt om het aantal en de ernst van incidenten, met inbegrip van inbreuken in verband met persoonsgegevens, te verminderen. Deze optie zou ook de rechtszekerheid vergroten en een gelijk speelveld voor marktdeelnemers tot stand brengen, het vertrouwen onder de gebruikers verhogen, evenals de aantrekkelijkheid van EU-producten met digitale elementen als geheel, waardoor de eigendom wordt beschermd en de voorwaarden voor marktdeelnemers om zaken te doen worden verbeterd.

De horizontale cyberbeveiligingsvereisten zouden bijdragen tot de beveiliging van persoonsgegevens door de vertrouwelijkheid, integriteit en beschikbaarheid van informatie in producten met digitale elementen te beschermen. Naleving van die vereisten zal het makkelijker maken om de vereiste beveiliging van de verwerking van persoonsgegevens in

het kader van Verordening (EU) 2016/679 (AVG) na te leven[12]. Het voorstel zou de transparantie en informatievoorziening voor gebruikers verbeteren, met inbegrip van gebruikers met minder kennis over cyberbeveiliging. Gebruikers zouden ook beter worden geïnformeerd over de risico's, capaciteiten en beperkingen van de producten met digitale elementen, waardoor zij beter in staat zouden zijn de nodige preventieve en risicobeperkende maatregelen te nemen om de resterende risico's te verminderen.

4. GEVOLGEN VOOR DE BEGROTING

Om de taken te vervullen die in het kader van deze verordening aan het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) worden toegewezen, zal Enisa ongeveer 4,5 vte moeten herschikken. De Commissie zou 7 vte moeten toewijzen om haar verantwoordelijkheden op het gebied van handhaving uit hoofde van deze verordening na te komen.

Een gedetailleerd overzicht van de betrokken kosten is te vinden in het financieel memorandum bij dit voorstel.

5. OVERIGE ELEMENTEN

• Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage

De Commissie zal toezicht houden op de uitvoering, de toepassing en de naleving van deze nieuwe bepalingen om de doeltreffendheid ervan te beoordelen. In de verordening wordt de Commissie verzocht uiterlijk 36 maanden na de datum van toepassing en vervolgens om de vier jaar een evaluatie en toetsing te verrichten en een openbaar verslag in te dienen bij het Europees Parlement en de Raad.

• Artikelsgewijze toelichting

Algemene bepalingen (hoofdstuk I)

Dit voorstel van verordening voorziet in a) voorschriften voor het in de handel brengen van producten met digitale elementen om de cyberbeveiliging van dergelijke producten te waarborgen; b) essentiële eisen voor het ontwerp, de ontwikkeling en de productie van producten met digitale elementen, en verplichtingen voor marktdeelnemers in verband met deze producten op het gebied van cyberbeveiliging; c) essentiële eisen voor de procedures inzake de respons op kwetsbaarheden, die fabrikanten hebben ingevoerd om de cyberbeveiliging van producten met digitale elementen gedurende de gehele levenscyclus te waarborgen, en verplichtingen voor marktdeelnemers met betrekking tot deze procedures; d) voorschriften inzake markttoezicht en handhaving van bovengenoemde voorschriften en eisen.

De voorgestelde verordening zal van toepassing zijn op alle producten met digitale elementen waarvan het beoogde en redelijkerwijs voorzienbaar gebruik een directe of indirecte logische of fysieke dataverbinding met een apparaat of netwerk omvat.

[12] 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) (PB L 119 van 4.5.2016, blz. 1).

De voorgestelde verordening zal niet van toepassing zijn op producten met digitale elementen die binnen het toepassingsgebied van Verordening (EU) 2017/745 [medische hulpmiddelen voor menselijk gebruik en toebehoren van dergelijke hulpmiddelen] en Verordening (EU) 2017/746 [medische hulpmiddelen voor in-vitrodiagnostiek voor menselijk gebruik en toebehoren van dergelijke hulpmiddelen] vallen, aangezien beide verordeningen voorschriften voor hulpmiddelen bevatten, onder meer inzake software en algemene verplichtingen voor fabrikanten, die de gehele levenscyclus van producten bestrijken, alsook conformiteitsbeoordelingsprocedures. Deze verordening is niet van toepassing op producten met digitale elementen die zijn gecertificeerd overeenkomstig Verordening 2018/1139 [hoog uniform niveau van veiligheid van de burgerluchtvaart], noch op producten waarop Verordening (EU) 2019/2144 van toepassing is [betreffende de voorschriften voor de typegoedkeuring van motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd].

Kritieke producten met digitale elementen worden onderworpen aan specifieke conformiteitsbeoordelingsprocedures en worden ingedeeld in klasse I en klasse II, zoals vastgesteld in bijlage III, afhankelijk van hun cyberbeveiligingsrisico, waarbij klasse II een groter risico inhoudt. Een product met digitale elementen wordt als kritiek beschouwd en daarom opgenomen in bijlage III, met het oog op de gevolgen van potentiële kwetsbaarheden op het gebied van cyberbeveiliging in het product met digitale elementen. Bij de bepaling van het cyberbeveiligingsrisico wordt onder meer rekening gehouden met de aan cyberbeveiliging gerelateerde functionaliteit van het product met digitale elementen en het beoogde gebruik ervan in gevoelige omgevingen, zoals een industriële omgeving.

De Commissie is ook bevoegd om gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen door categorieën zeer kritieke producten met digitale elementen te specificeren waarvoor de fabrikanten in het kader van een Europese cyberbeveiligingscertificeringsregeling een Europees cyberbeveiligingscertificaat moeten verkrijgen om de conformiteit met de essentiële eisen van bijlage I of delen daarvan aan te tonen. Bij het bepalen van dergelijke categorieën zeer kritieke producten met digitale elementen houdt de Commissie rekening met het niveau van cyberbeveiligingsrisico van de categorie producten met digitale elementen, aan de hand van een of meer van de criteria die gehanteerd worden voor de opneming van kritieke producten met digitale elementen in bijlage III, alsook aan de hand van de beoordeling of die categorie producten wordt gebruikt of toegepast door de essentiële entiteiten van het type als bedoeld in bijlage [bijlage I] bij Richtlijn [Richtlijn XXX/XXXX (NIS2)] of in de toekomst mogelijk van belang zal zijn voor de activiteiten van deze entiteiten, of relevant is voor de veerkracht van de gehele toeleveringsketen van producten met digitale elementen tegen verstorende gebeurtenissen.

Verplichtingen van marktdeelnemers (hoofdstuk II)

Het voorstel bevat verplichtingen voor fabrikanten, importeurs en distributeurs op basis van de referentiebepalingen van Besluit 768/2008/EG. Op grond van de essentiële cyberbeveiligingsvereisten en -verplichtingen mogen producten met digitale elementen alleen op de markt worden aangeboden indien zij, wanneer zij naar behoren worden geleverd, correct worden geïnstalleerd, worden onderhouden en gebruikt voor het beoogde doel of in redelijkerwijs voorzienbare omstandigheden, aan de essentiële cyberbeveiligingsvereisten van deze verordening voldoen.

De essentiële eisen en verplichtingen zouden fabrikanten ertoe verplichten om bij het ontwerp, de ontwikkeling en de productie van producten met digitale elementen rekening te houden met cyberbeveiliging, passende zorgvuldigheid te betrachten met betrekking tot beveiligingsaspecten bij het ontwerpen en ontwikkelen van hun producten, transparant te zijn

over cyberbeveiligingsaspecten die aan klanten bekend moeten worden gemaakt, op evenredige wijze te zorgen voor beveiligingsondersteuning (updates) en te voldoen aan de vereisten inzake de respons op kwetsbaarheden.

Er zouden verplichtingen worden vastgesteld voor marktdeelnemers, van fabrikanten tot distributeurs en importeurs, met betrekking tot het in de handel brengen van producten met digitale elementen, die passen bij hun rol en verantwoordelijkheden in de toeleveringsketen.

Conformiteit van het product met digitale elementen (hoofdstuk III)

Het product met digitale elementen dat in overeenstemming is met geharmoniseerde normen of delen daarvan, waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, wordt geacht in overeenstemming te zijn met de essentiële eisen van deze voorgestelde verordening. Wanneer er geen geharmoniseerde normen bestaan of die normen ontoereikend zijn of wanneer de normalisatieprocedure te veel vertraging oploopt of wanneer het verzoek van de Commissie niet door de Europese normalisatieorganisaties is aanvaard, kan de Commissie door middel van uitvoeringshandelingen gemeenschappelijke specificaties vaststellen.

Daarnaast worden producten met digitale elementen die zijn gecertificeerd of waarvoor een EU-conformiteitsverklaring of -certificaat is afgegeven in het kader van een Europese cyberbeveiligingscertificeringsregeling krachtens Verordening (EU) 2019/881, en waarvoor de Commissie bij uitvoeringshandeling heeft gespecificeerd dat zij kan voorzien in een vermoeden van conformiteit voor deze verordening, geacht in overeenstemming te zijn met de essentiële eisen van deze verordening, of delen daarvan, voor zover de EU-conformiteitsverklaring of het cyberbeveiligingscertificaat, of delen daarvan, die eisen dekken.

Voorts moet de Commissie, om onnodige administratieve lasten voor fabrikanten te vermijden, in voorkomend geval specificeren of een cyberbeveiligingscertificaat dat in het kader van een dergelijke Europese cyberbeveiligingscertificeringsregeling is afgegeven, de verplichting voor fabrikanten om een conformiteitsbeoordeling door derden te laten verrichten, zoals bepaald in deze verordening voor de overeenkomstige eisen, overbodig maakt.

De fabrikant voert een conformiteitsbeoordeling uit van het product met digitale elementen en de procedures voor de respons op kwetsbaarheden die hij heeft ingevoerd, om de conformiteit met de essentiële eisen van bijlage I aan te tonen door een van de procedures van bijlage VI te volgen. Fabrikanten van kritieke producten van klasse I en II gebruiken de respectieve modules die nodig zijn voor de naleving. Fabrikanten van kritieke producten van klasse II moeten een derde partij bij hun conformiteitsbeoordeling betrekken.

Aanmelding van conformiteitsbeoordelingsinstanties (hoofdstuk IV)

Een goede werking van aangemelde instanties is van cruciaal belang voor een hoog niveau van cyberbeveiliging en voor het vertrouwen van alle belanghebbende partijen in het "nieuwe aanpak"-systeem. Daarom bevat het voorstel, in overeenstemming met Besluit 768/2008/EG, voorschriften voor de nationale autoriteiten die verantwoordelijk zijn voor conformiteitsbeoordelingsinstanties (aangemelde instanties). Het laat de uiteindelijke verantwoordelijkheid voor de aanwijzing van en het toezicht op aangemelde instanties aan de lidstaten. De lidstaten wijzen een aanmeldende autoriteit aan die verantwoordelijk is voor het opzetten en uitvoeren van de nodige procedures voor de beoordeling en aanmelding van conformiteitsbeoordelingsinstanties en voor het toezicht erop.

Markttoezicht en handhaving (hoofdstuk V)

Overeenkomstig Verordening (EU) 2019/1020 voeren de nationale markttoezichtautoriteiten markttoezicht uit op het grondgebied van die lidstaat. De lidstaten kunnen ervoor kiezen een bestaande of nieuwe autoriteit aan te wijzen als markttoezichtautoriteit, met inbegrip van nationale bevoegde autoriteiten als bedoeld in artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)] of aangewezen nationale cyberbeveiligingscertificeringsautoriteiten als bedoeld in artikel 58 van Verordening (EU) 2019/881. Aan marktdeelnemers wordt gevraagd volledig samen te werken met markttoezichtautoriteiten en andere bevoegde autoriteiten.

Bevoegdheidsdelegatie en comitéprocedure (hoofdstuk VI)

Om ervoor te zorgen dat het regelgevingskader waar nodig kan worden aangepast, wordt aan de Commissie de bevoegdheid toegekend om overeenkomstig artikel 290 VWEU handelingen vast te stellen om de lijst van kritieke producten van de klassen I en II te actualiseren en de definities van deze producten te specificeren; te specificeren of een beperking of uitsluiting noodzakelijk is voor producten met digitale elementen die worden gedekt door andere regels van de Unie waarin eisen zijn vastgesteld die hetzelfde beschermingsniveau bieden als deze verordening; de certificering van bepaalde zeer kritieke producten met digitale elementen verplicht te stellen op basis van de in deze verordening vastgestelde criteria; de minimuminhoud van de EU-conformiteitsverklaring te specificeren en de elementen die in de technische documentatie moeten worden opgenomen, aan te vullen.

De Commissie is ook bevoegd om uitvoeringshandelingen vast te stellen om: de vorm of de elementen van de meldingsplicht en de softwarestuklijst te specificeren; de Europese cyberbeveiligingscertificeringsregelingen te specificeren die kunnen worden gebruikt om de conformiteit met de essentiële eisen of delen daarvan aan te tonen, zoals vastgesteld in deze verordening; gemeenschappelijke specificaties vast te stellen; technische specificaties voor het aanbrengen van de CE-markering vast te stellen; in uitzonderlijke omstandigheden op Unieniveau corrigerende of beperkende maatregelen vast te stellen die een onmiddellijk optreden rechtvaardigen om de goede werking van de interne markt te beschermen.

Vertrouwelijkheid en sancties (hoofdstuk VII)

Alle partijen die deze verordening toepassen, moeten de vertrouwelijkheid eerbiedigen van de informatie en gegevens die zij bij de uitvoering van hun taken en activiteiten hebben verkregen.

Om de doeltreffende handhaving van de verplichtingen van deze verordening te waarborgen, moet elke markttoezichtautoriteit de bevoegdheid hebben om administratieve geldboeten op te leggen of om oplegging hiervan te vragen. In dezelfde geest worden bij deze verordening maximumniveaus vastgesteld voor administratieve geldboeten waarin het interne recht moet voorzien in geval van niet-naleving van de verplichtingen van deze verordening.

Overgangs- en slotbepalingen (hoofdstuk VIII)

Om fabrikanten, aangemelde instanties en lidstaten de tijd te geven zich aan de nieuwe voorschriften aan te passen, zal de voorgestelde verordening [24 maanden] na de inwerkingtreding ervan van toepassing worden, met uitzondering van de meldingsplicht voor fabrikanten, die van toepassing zou zijn vanaf [12 maanden] na de datum van inwerkingtreding.

2022/0272 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité[1],

Gezien het advies van het Comité van de Regio's[2],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) De werking van de interne markt moet worden verbeterd door een uniform rechtskader vast te stellen voor essentiële cyberbeveiligingsvereisten om producten met digitale elementen in de Unie in de handel te brengen. Twee grote problemen die kosten voor gebruikers en de samenleving met zich meebrengen, moeten worden aangepakt: een laag niveau van cyberbeveiliging van producten met digitale elementen, dat tot uiting komt in wijdverbreide kwetsbaarheden en de ontoereikende en inconsistente verstrekking van beveiligingsupdates om deze aan te pakken, en onvoldoende inzicht in en toegang tot informatie door gebruikers, waardoor zij niet in staat zijn producten met passende cyberbeveiligingskenmerken te kiezen of deze op een veilige manier te gebruiken.

(2) Deze verordening is erop gericht de randvoorwaarden te scheppen voor de ontwikkeling van veilige producten met digitale elementen door ervoor te zorgen dat hardware- en softwareproducten met minder kwetsbaarheden in de handel worden gebracht en dat fabrikanten de veiligheid gedurende de hele levenscyclus van een product serieus nemen. Zij is er ook op gericht de voorwaarden te scheppen die gebruikers in staat stellen rekening te houden met cyberbeveiliging bij het selecteren en gebruiken van producten met digitale elementen.

(3) De desbetreffende wetgeving van de Unie die momenteel van kracht is, omvat verschillende reeksen horizontale regels die betrekking hebben op bepaalde aspecten van cyberbeveiliging vanuit verschillende invalshoeken, waaronder maatregelen om de beveiliging van de digitale toeleveringsketen te verbeteren. De bestaande wetgeving

[1] PB C […] van […], blz. […].
[2] PB C […] van […], blz. […].

van de Unie met betrekking tot cyberbeveiliging, met inbegrip van [Richtlijn XXX/XXXX (NIS2)] en Verordening (EU) 2019/881 van het Europees Parlement en de Raad[3], heeft echter niet rechtstreeks betrekking op verplichte eisen voor de beveiliging van producten met digitale elementen.

(4) Hoewel de bestaande wetgeving van de Unie van toepassing is op bepaalde producten met digitale elementen, bestaat er geen horizontaal regelgevingskader van de Unie met uitgebreide cyberbeveiligingsvereisten voor alle producten met digitale elementen. Met de verschillende handelingen en initiatieven die tot dusver op Unie- en nationaal niveau zijn genomen, worden de vastgestelde problemen en risico's op het gebied van cyberbeveiliging slechts gedeeltelijk aangepakt, wat leidt tot het ontstaan van een lappendeken van wetgeving binnen de interne markt, waardoor de rechtsonzekerheid voor zowel fabrikanten als gebruikers van deze producten toeneemt en bedrijven onnodig worden belast om aan een groot aantal vereisten voor soortgelijke producten te voldoen. De cyberbeveiliging van deze producten heeft een sterke grensoverschrijdende dimensie, aangezien producten die in één land worden vervaardigd, vaak door organisaties en consumenten op de gehele interne markt worden gebruikt. Dit maakt het noodzakelijk om dit gebied op het niveau van de Unie te reguleren. Het regelgevingslandschap van de Unie moet worden geharmoniseerd door cyberbeveiligingsvereisten in te voeren voor producten met digitale elementen. Daarnaast zou er moeten worden gezorgd voor rechtszekerheid voor marktdeelnemers en gebruikers in de hele Unie en voor een betere harmonisatie van de eengemaakte markt, waardoor de voorwaarden voor marktdeelnemers die de EU-markt willen betreden, worden verbeterd.

(5) Op het niveau van de Unie wordt in diverse programmatische en politieke documenten, zoals de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[4], de conclusies van de Raad van 2 december 2020 en 23 mei 2022 of de resolutie van het Europees Parlement van 10 juni 2021[5], aangedrongen op specifieke cyberbeveiligingsvereisten van de Unie voor digitale of verbonden producten, in een context waarin verschillende landen over de hele wereld maatregelen nemen om dit probleem op eigen initiatief aan te pakken. In het eindverslag van de Conferentie over de toekomst van Europa[6] werd door de burgers gepleit voor "een sterkere rol voor de EU bij de bestrijding van cyberdreigingen".

(6) Om het algemene cyberbeveiligingsniveau van alle producten met digitale elementen die op de interne markt worden gebracht, te verhogen, moeten voor deze producten doelgerichte en technologieneutrale essentiële cyberbeveiligingsvereisten worden ingevoerd die horizontaal van toepassing zijn.

(7) Onder bepaalde omstandigheden kunnen alle producten met digitale elementen die zijn geïntegreerd in of verbonden met een groter elektronisch informatiesysteem, als

---

3 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 (cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=JOIN:2020:18:FIN

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_NL.html

6 *Conference on the Future of Europe — Report on the Final Outcome*, mei 2022, voorstel 28(2). De conferentie vond plaats tussen april 2021 en mei 2022. Het was een unieke, door burgers geleide vorm van overlegdemocratie op pan-Europees niveau, waarbij duizenden Europese burgers en politieke actoren, sociale partners, vertegenwoordigers van het maatschappelijk middenveld en belangrijke belanghebbenden betrokken waren.

aanvalsvector dienen voor kwaadwillige actoren. Als gevolg daarvan kunnen zelfs hardware en software die als minder kritiek worden beschouwd, een eerste aantasting van een apparaat of netwerk vergemakkelijken, waardoor kwaadwillige actoren geprivilegieerde toegang tot een systeem kunnen krijgen of zich zijwaarts tussen systemen kunnen bewegen. Fabrikanten moeten er daarom voor zorgen dat alle producten met digitale elementen waarmee verbinding mogelijk is, worden ontworpen en ontwikkeld overeenkomstig de essentiële eisen van deze verordening. Hieronder vallen zowel producten die fysiek kunnen worden verbonden via hardware-interfaces als producten die logisch worden verbonden, zoals netwerkaansluitingen, leidingen, bestanden, applicatieprogramma-interfaces of andere soorten software-interfaces. Aangezien cyberdreigingen zich kunnen verspreiden via verschillende producten met digitale elementen voordat zij een bepaald doel treffen, bijvoorbeeld door het koppelen van meerdere exploits, moeten fabrikanten ook zorgen voor de cyberbeveiliging van producten die slechts indirect verbonden zijn met andere apparaten of netwerken.

(8) Door cyberbeveiligingsvereisten vast te stellen voor het in de handel brengen van producten met digitale elementen, zal de cyberbeveiliging van deze producten voor zowel consumenten als bedrijven worden verbeterd. Hieronder vallen ook eisen voor het in de handel brengen van consumentenproducten met digitale elementen die bestemd zijn voor kwetsbare consumenten, zoals speelgoed en babymonitors.

(9) Deze verordening waarborgt een hoog niveau van cyberbeveiliging van producten met digitale elementen. Zij heeft geen betrekking op diensten, zoals Software-as-a-Service (SaaS), met uitzondering van oplossingen voor gegevensverwerking op afstand die zijn gekoppeld aan een product met digitale elementen bedoeld voor normale gegevensverwerking op afstand, waarvoor de software is ontworpen en ontwikkeld door of onder de verantwoordelijkheid van de fabrikant van het betrokken product, bij gebreke waarvan een dergelijk product met digitale elementen een van zijn functies niet zou kunnen vervullen. [Richtlijn XXX/XXXX (NIS2)] stelt eisen vast voor cyberbeveiliging en het melden van incidenten voor essentiële en belangrijke entiteiten, zoals kritieke infrastructuur, om de veerkracht van de door hen verleende diensten te vergroten. [Richtlijn XXX/XXXX (NIS2)] is van toepassing op cloudcomputerdiensten en cloudmodellen, zoals SaaS. Alle entiteiten die cloudcomputerdiensten aanbieden in de Unie die de drempel voor middelgrote ondernemingen halen of overschrijden, vallen binnen het toepassingsgebied van die richtlijn.

(10) Om innovatie of onderzoek niet in de weg te staan, mag vrije en opensourcesoftware die buiten het kader van een handelsactiviteit wordt ontwikkeld of geleverd, niet onder deze verordening vallen. Dit geldt met name voor software, met inbegrip van de broncode en gewijzigde versies ervan, die openlijk gedeeld en vrij toegankelijk, bruikbaar, veranderbaar en herdistribueerbaar is. In de context van software omvat een handelsactiviteit mogelijk niet alleen het in rekening brengen van een prijs voor een product, maar ook het in rekening brengen van een prijs voor technische ondersteuningsdiensten, het aanbieden van een softwareplatform waarmee de fabrikant andere diensten te gelde maakt, of het gebruik van persoonsgegevens voor andere redenen dan uitsluitend de verbetering van de beveiliging, compatibiliteit of interoperabiliteit van de software.

(11) Een veilig internet is onontbeerlijk voor de werking van kritieke infrastructuur en voor de samenleving als geheel. [Richtlijn XXX/XXXX (NIS2)] heeft tot doel een hoog niveau van cyberbeveiliging te waarborgen van diensten die worden verleend door essentiële en belangrijke entiteiten, waaronder aanbieders van digitale infrastructuur

die de kernfuncties van het open internet ondersteunen en internettoegang en internetdiensten waarborgen. Het is daarom belangrijk dat de producten met digitale elementen die aanbieders van digitale infrastructuur nodig hebben om de werking van het internet te waarborgen, op een veilige manier worden ontwikkeld en voldoen aan gevestigde normen voor internetbeveiliging. Deze verordening, die van toepassing is op alle hardware- en softwareproducten die verbonden kunnen worden, heeft ook tot doel de naleving door aanbieders van digitale infrastructuur van de vereisten voor de toeleveringsketen uit hoofde van [Richtlijn XXX/XXXX (NIS2)] te vergemakkelijken, door ervoor te zorgen dat de producten met digitale elementen die zij voor de verlening van hun diensten gebruiken, op veilige wijze worden ontwikkeld en dat zij toegang hebben tot tijdige beveiligingsupdates voor dergelijke producten.

(12) Verordening (EU) 2017/745 van het Europees Parlement en de Raad[7] bevat voorschriften voor medische hulpmiddelen en Verordening (EU) 2017/746 van het Europees Parlement en de Raad[8] bevat voorschriften voor medische hulpmiddelen voor in-vitrodiagnostiek. Beide verordeningen pakken cyberbeveiligingsrisico's aan en volgen specifieke benaderingen die ook in deze verordening aan bod komen. Meer in het bijzonder bevatten de Verordeningen (EU) 2017/745 en (EU) 2017/746 essentiële eisen voor medische hulpmiddelen die via een elektronisch systeem functioneren of die zelf software zijn. Bepaalde niet-ingebedde software en de levenscyclusbenadering vallen ook onder die verordeningen. Deze eisen verplichten fabrikanten om hun producten te ontwikkelen en te bouwen door de beginselen van risicobeheer toe te passen en door eisen vast te stellen met betrekking tot IT-beveiligingsmaatregelen en bijbehorende conformiteitsbeoordelingsprocedures. Bovendien bestaan er sinds december 2019 specifieke richtsnoeren inzake cyberbeveiliging voor medische hulpmiddelen, die fabrikanten van medische hulpmiddelen, met inbegrip van hulpmiddelen voor in-vitrodiagnostiek, ondersteuning bieden om aan alle relevante essentiële eisen van bijlage I bij die verordeningen met betrekking tot cyberbeveiliging te voldoen[9]. Producten met digitale elementen waarop een van die verordeningen van toepassing is, mogen daarom niet onder deze verordening vallen.

(13) Bij Verordening (EU) 2019/2144 van het Europees Parlement en de Raad[10] zijn voorschriften vastgesteld voor de typegoedkeuring van voertuigen en van de systemen

---

7 Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad (PB L 117 van 5.5.2017, blz. 1).

8 Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek en tot intrekking van Richtlijn 98/79/EG en Besluit 2010/227/EU van de Commissie (PB L 117 van 5.5.2017, blz. 176).

9 MDCG 2019-16, bekrachtigd door de bij artikel 103 van Verordening (EU) 2017/745 opgerichte coördinatiegroep voor medische hulpmiddelen (Medical Device Coordination Group — MDCG).

10 Verordening (EU) 2019/2144 van het Europees Parlement en de Raad van 27 november 2019 betreffende de voorschriften voor de typegoedkeuring van motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd wat de algemene veiligheid ervan en de bescherming van de inzittenden van voertuigen en kwetsbare weggebruikers betreft, tot wijziging van Verordening (EU) 2018/858 van het Europees Parlement en de Raad en tot intrekking van de Verordeningen (EG) nr. 78/2009, (EG) nr. 79/2009 en (EG) nr. 661/2009 van het Europees Parlement en de Raad en de Verordeningen (EG) nr. 631/2009, (EU) nr. 406/2010, (EU) nr. 672/2010, (EU) nr. 1003/2010, (EU) nr. 1005/2010, (EU) nr. 1008/2010, (EU) nr. 1009/2010, (EU) nr. 19/2011, (EU) nr. 109/2011, (EU) nr. 458/2011, (EU) nr. 65/2012, (EU) nr. 130/2012, (EU) nr. 347/2012, (EU) nr. 351/2012, (EU) nr. 1230/2012 en (EU) 2015/166 van de Commissie (PB L 325 van 16.12.2019, blz. 1).

en onderdelen daarvan, waarbij bepaalde cyberbeveiligingsvereisten worden ingevoerd, onder meer inzake het gebruik van een gecertificeerd beheersysteem voor cyberbeveiliging en inzake software-updates, die betrekking hebben op het beleid en de processen van organisaties voor cyberrisico's in verband met de gehele levenscyclus van voertuigen, apparatuur en diensten in overeenstemming met de toepasselijke voorschriften van de Verenigde Naties inzake technische specificaties en cyberbeveiliging[11], en waarin wordt voorzien in specifieke conformiteitsbeoordelingsprocedures. Wat de luchtvaart betreft, is de belangrijkste doelstelling van Verordening (EU) 2018/1139 van het Europees Parlement en de Raad[12] de totstandbrenging en instandhouding van een hoog, uniform veiligheidsniveau in de burgerluchtvaart in de Unie. Hiermee komt een kader tot stand voor essentiële eisen inzake luchtwaardigheid voor luchtvaartproducten en hun onderdelen en apparatuur, met inbegrip van software, die rekening houden met de verplichtingen om te beschermen tegen bedreigingen van de informatiebeveiliging. Producten met digitale elementen waarop Verordening (EU) 2019/2144 van toepassing is en producten die zijn gecertificeerd overeenkomstig Verordening (EU) 2018/1139, zijn derhalve niet onderworpen aan de in deze verordening vastgestelde essentiële eisen en conformiteitsbeoordelingsprocedures. Het certificeringsproces uit hoofde van Verordening (EU) 2018/1139 waarborgt het door deze verordening beoogde zekerheidsniveau.

(14) Bij deze verordening worden horizontale cyberbeveiligingsregels vastgesteld die niet specifiek zijn voor sectoren of bepaalde producten met digitale elementen. Niettemin zouden er sectorale of productspecifieke voorschriften van de Unie kunnen worden ingevoerd met eisen die betrekking hebben op alle of een deel van de risico's die onder de essentiële eisen van deze verordening vallen. In dergelijke gevallen kan de toepassing van deze verordening op producten met digitale elementen die vallen onder andere voorschriften van de Unie waarin eisen worden vastgesteld met betrekking tot alle of een deel van de risico's die worden gedekt door de essentiële eisen van bijlage I bij deze verordening, worden beperkt of uitgesloten indien een dergelijke beperking of uitsluiting in overeenstemming is met het algemene regelgevingskader dat op die producten van toepassing is, en de sectorale voorschriften hetzelfde beschermingsniveau bieden als deze verordening. De Commissie is bevoegd gedelegeerde handelingen vast te stellen om deze verordening te wijzigen door dergelijke producten en voorschriften aan te wijzen. Deze verordening bevat specifieke bepalingen voor bestaande Uniewetgeving waarvoor dergelijke beperkingen of uitsluitingen moeten gelden, om de relatie met die Uniewetgeving te verduidelijken.

(15) Bij Gedelegeerde Verordening (EU) 2022/30 is gespecificeerd dat de essentiële eisen van artikel 3, lid 3, punt d) (netwerkschade en misbruik van netwerkmiddelen), punt e) (persoonsgegevens en privacy) en punt f) (fraude) van Richtlijn 2014/53/EU van toepassing zijn op bepaalde radioapparatuur. [Uitvoeringsbesluit XXX/2022 van de

---

11 VN-Reglement nr. 155 — Uniforme bepalingen voor de goedkeuring van voertuigen met betrekking tot cyberbeveiliging en het beheersysteem voor cyberbeveiliging [2021/387].

12 Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot wijziging van de Verordeningen (EG) nr. 2111/2005, (EG) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 en de Richtlijnen 2014/30/EU en 2014/53/EU van het Europees Parlement en de Raad, en tot intrekking van de Verordeningen (EG) nr. 552/2004 en (EG) nr. 216/2008 van het Europees Parlement en de Raad en Verordening (EEG) nr. 3922/91 van de Raad (PB L 212 van 22.8.2018, blz. 1).

Commissie betreffende een normalisatieverzoek aan de Europese normalisatieorganisaties] bevat voorschriften voor de ontwikkeling van specifieke normen waarin nader wordt gespecificeerd hoe deze drie essentiële eisen moeten worden aangepakt. De bij deze verordening vastgestelde essentiële eisen omvatten alle elementen van de essentiële eisen als bedoeld in artikel 3, lid 3, punten d), e) en f), van Richtlijn 2014/53/EU. Daarnaast zijn de in deze verordening vastgestelde essentiële eisen afgestemd op de doelstellingen van de eisen voor specifieke normen die in dat normalisatieverzoek zijn opgenomen. Indien de Commissie Gedelegeerde Verordening (EU) 2022/30 intrekt of wijzigt met als gevolg dat die niet langer van toepassing is op bepaalde producten die onder deze verordening vallen, moeten de Commissie en de Europese normalisatieorganisaties bij de voorbereiding en ontwikkeling van geharmoniseerde normen derhalve rekening houden met de normalisatiewerkzaamheden die in het kader van Uitvoeringsbesluit C(2022) 5637 van de Commissie betreffende een normalisatieverzoek voor Gedelegeerde Verordening (EU) 2022/30 tot aanvulling van de richtlijn radioapparatuur zijn verricht om de uitvoering van deze verordening te vergemakkelijken.

(16) Richtlijn 85/374/EEG[13] vormt een aanvulling op deze verordening. Die richtlijn bevat aansprakelijkheidsregels voor producten met gebreken, zodat gelaedeerden schadevergoeding kunnen vorderen wanneer schade is veroorzaakt door producten met gebreken. Zij stelt het beginsel vast dat de fabrikant van een product aansprakelijk is voor schade die wordt veroorzaakt door een gebrek aan veiligheid in zijn product, ongeacht of er sprake is van schuld ("risicoaansprakelijkheid"). Wanneer een dergelijk gebrek aan veiligheid voortkomt uit een gebrek aan beveiligingsupdates nadat het product in de handel is gebracht, en hierdoor schade wordt veroorzaakt, kan de fabrikant aansprakelijk worden gesteld. In deze verordening moeten verplichtingen voor fabrikanten worden vastgesteld die betrekking hebben op het verstrekken van dergelijke beveiligingsupdates.

(17) Deze verordening mag geen afbreuk doen aan Verordening (EU) 2016/679 van het Europees Parlement en de Raad[14], met inbegrip van bepalingen betreffende de vaststelling van certificeringsmechanismen voor gegevensbescherming en van gegevensbeschermingszegels en -merktekens, om de naleving van die verordening bij verwerkingen door verwerkingsverantwoordelijken en verwerkers aan te tonen. Dergelijke handelingen zouden kunnen worden ingebed in een product met digitale elementen. Gegevensbescherming door ontwerp en door standaardinstellingen, en cyberbeveiliging in het algemeen, zijn essentiële elementen van Verordening (EU) 2016/679. Door consumenten en organisaties te beschermen tegen cyberbeveiligingsrisico's, moeten de essentiële cyberbeveiligingsvereisten van deze verordening ook bijdragen tot een betere bescherming van persoonsgegevens en privacy van personen. Synergieën op het gebied van zowel normalisatie als certificering op het gebied van cyberbeveiliging moeten in aanmerking worden genomen in het kader van de samenwerking tussen de Commissie, de Europese normalisatieorganisaties, het Agentschap van de Europese Unie voor

[13] Richtlijn 85/374/EEG van de Raad van 25 juli 1985 betreffende de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen der lidstaten inzake de aansprakelijkheid voor producten met gebreken (PB L 210 van 7.8.85).

[14] 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) (PB L 119 van 4.5.2016, blz. 1).

cyberbeveiliging (Enisa), het Europees Comité voor gegevensbescherming (EDPB), opgericht bij Verordening (EU) 2016/679, en de nationale toezichthoudende autoriteiten voor gegevensbescherming. Ook op het gebied van markttoezicht en handhaving moeten synergieën tussen deze verordening en de gegevensbeschermingswetgeving van de Unie worden gecreëerd. Daartoe moeten de krachtens deze verordening aangewezen nationale markttoezichtautoriteiten samenwerken met autoriteiten die toezicht houden op de gegevensbeschermingswetgeving van de Unie. Ook moeten deze laatsten toegang hebben tot informatie die relevant is voor de uitvoering van hun taken.

(18) Voor zover hun producten binnen het toepassingsgebied van deze verordening vallen, moeten afgevers van Europese portemonnees voor digitale identiteit als bedoeld in artikel [artikel 6 bis, lid 2, van Verordening (EU) nr. 910/2014, zoals gewijzigd bij het voorstel voor een verordening tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit] zowel voldoen aan de horizontale essentiële eisen van deze verordening als aan de specifieke beveiligingsvereisten die zijn vastgesteld bij artikel [artikel 6 bis van Verordening (EU) nr. 910/2014, zoals gewijzigd bij het voorstel voor een verordening tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit]. Om de naleving te vergemakkelijken, moeten afgevers van Europese portemonnees voor digitale identiteit kunnen aantonen dat die portemonnees voldoen aan de vereisten die respectievelijk zijn vastgesteld in beide rechtshandelingen, door hun producten te certificeren in het kader van een Europese cyberbeveiligingscertificeringsregeling, die is vastgesteld op grond van Verordening (EU) 2019/881 en waarvoor de Commissie bij uitvoeringshandeling heeft voorzien in een vermoeden van conformiteit met betrekking tot deze verordening, voor zover het certificaat, of delen daarvan, die vereisten dekt.

(19) Bepaalde taken waarin deze verordening voorziet, moeten door Enisa worden uitgevoerd overeenkomstig artikel 3, lid 2, van Verordening (EU) 2019/881. Enisa moet met name meldingen van fabrikanten ontvangen van actief uitgebuite kwetsbaarheden in producten met digitale elementen, alsook van incidenten die gevolgen hebben voor de veiligheid van die producten. Enisa moet deze meldingen ook doorsturen naar de betrokken computer security incident response teams (CSIRT's) of, respectievelijk, naar de betrokken centrale contactpunten van de lidstaten die zijn aangewezen overeenkomstig artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)], en de relevante markttoezichtautoriteiten in kennis stellen van de gemelde kwetsbaarheid. Op basis van de informatie die het verzamelt, moet Enisa om de twee jaar een technisch verslag opstellen over opkomende trends met betrekking tot cyberbeveiligingsrisico's in producten met digitale elementen en dit voorleggen aan de samenwerkingsgroep als bedoeld in Richtlijn [Richtlijn XXX/XXXX (NIS2)]. Voorts moet Enisa, gezien zijn deskundigheid en zijn mandaat, het proces voor de uitvoering van deze verordening kunnen ondersteunen. Het moet met name gezamenlijke activiteiten kunnen voorstellen die door markttoezichtautoriteiten moeten worden uitgevoerd op basis van aanwijzingen of informatie over mogelijke niet-conformiteit met deze verordening van producten met digitale elementen in verschillende lidstaten, of categorieën producten kunnen identificeren waarvoor gelijktijdige gecoördineerde controleacties moeten worden georganiseerd. In uitzonderlijke omstandigheden moet Enisa, op verzoek van de Commissie, evaluaties kunnen uitvoeren met betrekking tot specifieke producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden, wanneer

onmiddellijk ingrijpen nodig is om de goede werking van de interne markt te beschermen.

(20) Op producten met digitale elementen moet de CE-markering worden aangebracht om aan te geven dat zij in overeenstemming zijn met deze verordening, zodat zij vrij kunnen bewegen op de interne markt. De lidstaten mogen het in de handel brengen van producten met digitale elementen die aan de eisen van deze verordening voldoen en waarop de CE-markering is aangebracht, niet op ongerechtvaardigde wijze belemmeren.

(21) Om ervoor te zorgen dat fabrikanten software voor testdoeleinden kunnen uitgeven alvorens hun producten aan een conformiteitsbeoordeling te onderwerpen, mogen de lidstaten het beschikbaar stellen van niet-afgewerkte software, zoals alfa- en bètaversies of release candidates, niet verhinderen, mits de versie slechts beschikbaar wordt gesteld voor de tijd die nodig is om deze te testen en feedback te verzamelen. Fabrikanten moeten ervoor zorgen dat software die onder deze voorwaarden beschikbaar wordt gesteld, pas na een risicobeoordeling wordt uitgegeven en voor zover mogelijk voldoet aan de bij deze verordening opgelegde beveiligingseisen met betrekking tot de kenmerken van producten met digitale elementen. Fabrikanten moeten ook de vereisten inzake de respons op kwetsbaarheden zoveel mogelijk toepassen. Fabrikanten mogen gebruikers niet dwingen om te upgraden naar versies die alleen voor testdoeleinden worden uitgegeven.

(22) Om ervoor te zorgen dat producten met digitale elementen, wanneer zij in de handel worden gebracht, geen cyberbeveiligingsrisico's voor personen en organisaties inhouden, moeten voor dergelijke producten essentiële eisen worden vastgesteld. Wanneer de producten vervolgens met fysieke of digitale middelen worden gewijzigd op een wijze die niet door de fabrikant is voorzien en die ertoe kan leiden dat zij niet langer aan de relevante essentiële eisen voldoen, moet de wijziging als ingrijpend worden beschouwd. Software-updates of -reparaties kunnen bijvoorbeeld worden gelijkgesteld met onderhoudswerkzaamheden, mits zij een reeds in de handel gebracht product niet zodanig wijzigen dat de naleving van de toepasselijke eisen in het gedrang komt of dat het beoogde gebruik waarvoor het product is beoordeeld, wordt gewijzigd. Net als bij fysieke reparaties of wijzigingen moet een product met digitale elementen worden beschouwd als ingrijpend gewijzigd door een softwarewijziging wanneer de software-update de oorspronkelijke beoogde functies, het type of de prestaties van het product wijzigt en deze wijzigingen niet in de initiële risicobeoordeling waren voorzien, de aard van het gevaar is gewijzigd of het risiconiveau is toegenomen als gevolg van de software-update.

(23) In lijn met het algemeen erkende begrip van ingrijpende wijziging van producten die vallen onder de harmonisatiewetgeving van de Unie, is het passend dat voor een product met digitale elementen een nieuwe conformiteitsbeoordeling wordt uitgevoerd wanneer er sprake is van een ingrijpende wijziging die gevolgen kan hebben voor de conformiteit van een product met deze verordening, of wanneer het beoogde doel van dat product verandert. Indien de fabrikant een conformiteitsbeoordeling uitvoert waarbij een derde partij betrokken is, moeten wijzigingen die mogelijk ingrijpend zijn, in voorkomend geval ter kennis van de derde partij worden gebracht.

(24) Het opknappen, onderhouden en repareren van een product met digitale elementen, als gedefinieerd in Verordening [verordening inzake ecologisch ontwerp], leidt niet noodzakelijkerwijs tot een ingrijpende wijziging van het product, bijvoorbeeld als het beoogde gebruik en de functies niet worden gewijzigd en het risiconiveau ongewijzigd

blijft. De verbetering van een product door de fabrikant kan echter leiden tot veranderingen in het ontwerp en de ontwikkeling van het product en kan derhalve van invloed zijn op het beoogde gebruik en de conformiteit van het product met de eisen van deze verordening.

(25) Producten met digitale elementen moeten als kritiek worden beschouwd wanneer de negatieve gevolgen van het uitbuiten van potentiële kwetsbaarheden in de cyberbeveiliging van het product ernstig kunnen zijn als gevolg van, onder meer, de aan cyberbeveiliging verbonden functionaliteit of het beoogde gebruik. Met name kunnen kwetsbaarheden in producten met digitale elementen met een aan cyberbeveiliging verbonden functionaliteit, zoals beveiligde elementen, leiden tot de verspreiding van veiligheidsproblemen in de hele toeleveringsketen. De ernst van de gevolgen van een cyberbeveiligingsincident kan ook toenemen wanneer rekening wordt gehouden met het beoogde gebruik van het product, bijvoorbeeld in een industriële omgeving of in de context van een essentiële entiteit van het type als bedoeld in bijlage [bijlage I] bij Richtlijn [Richtlijn XXX/XXXX (NIS2)], of voor de uitvoering van kritieke of gevoelige functies, zoals de verwerking van persoonsgegevens.

(26) Kritieke producten met digitale elementen moeten aan strengere conformiteitsbeoordelingsprocedures worden onderworpen volgens een evenredige aanpak. Daartoe moeten kritieke producten met digitale elementen in twee klassen worden ingedeeld, naargelang van het niveau van het cyberbeveiligingsrisico in verband met deze productcategorieën. Een potentieel cyberincident waarbij producten van klasse II betrokken zijn, kan grotere negatieve gevolgen hebben dan een incident met producten van klasse I, bijvoorbeeld vanwege de aard van hun aan cyberbeveiliging verbonden functie of het beoogde gebruik ervan in gevoelige omgevingen, en moet daarom aan een strengere conformiteitsbeoordelingsprocedure worden onderworpen.

(27) De in bijlage III bij deze verordening bedoelde categorieën kritieke producten met digitale elementen moeten worden opgevat als de producten die de kernfunctionaliteit hebben van het type dat is opgenomen in bijlage III bij deze verordening. Bijlage III bij deze verordening omvat bijvoorbeeld een lijst van producten die door hun kernfunctionaliteit worden gedefinieerd als microprocessoren voor algemeen gebruik van klasse II. Als gevolg daarvan zijn microprocessoren voor algemene doeleinden onderworpen aan een verplichte conformiteitsbeoordeling door derden. Dit is niet het geval voor andere producten die niet uitdrukkelijk in bijlage III bij deze verordening worden genoemd, waarin een microprocessor voor algemeen gebruik kan zijn geïntegreerd. De Commissie moet [uiterlijk 12 maanden na de inwerkingtreding van deze verordening] gedelegeerde handelingen vaststellen om de productcategorieën die vallen onder de klassen I en II van bijlage III nader te specificeren.

(28) Deze verordening pakt cyberbeveiligingsrisico's op gerichte wijze aan. Producten met digitale elementen kunnen echter andere veiligheidsrisico's met zich meebrengen die geen verband houden met cyberbeveiliging. Die risico's moeten verder worden gereguleerd door andere desbetreffende productwetgeving van de Unie. Indien er geen andere harmonisatiewetgeving van de Unie van toepassing is, moeten zij onder Verordening [verordening inzake algemene productveiligheid] vallen. Daarom moeten in het licht van het gerichte karakter van deze verordening, in afwijking van artikel 2, lid 1, derde alinea, punt b), van Verordening [verordening inzake algemene productveiligheid], hoofdstuk III, deel 1, de hoofdstukken V en VII, en de hoofdstukken IX, X en XI van Verordening [verordening inzake algemene

productveiligheid] van toepassing zijn op producten met digitale elementen met betrekking tot veiligheidsrisico's die niet onder deze verordening vallen, indien die producten niet onderworpen zijn aan specifieke eisen die worden opgelegd bij andere harmonisatiewetgeving van de Unie in de zin van [artikel 3, punt 25, van de verordening inzake algemene productveiligheid].

(29) Producten met digitale elementen die overeenkomstig artikel 6 van Verordening[15] [de AI-verordening] als AI-systemen met een hoog risico worden aangemerkt en die binnen het toepassingsgebied van deze verordening vallen, moeten voldoen aan de essentiële eisen van deze verordening. Wanneer die AI-systemen met een hoog risico aan de essentiële eisen van deze verordening voldoen, moeten zij worden geacht in overeenstemming te zijn met de cyberbeveiligingsvereisten van artikel [artikel 15] van Verordening [de AI-verordening], voor zover die vereisten worden gedekt door de EU-conformiteitsverklaring of delen daarvan, die uit hoofde van deze verordening is afgegeven. Wat betreft de conformiteitsbeoordelingsprocedures met betrekking tot de essentiële cyberbeveiligingsvereisten van producten met digitale elementen die onder deze verordening vallen en als een AI-systeem met een hoog risico worden aangemerkt, moeten in de regel de desbetreffende bepalingen van artikel 43 van Verordening [de AI-verordening] worden toegepast in plaats van de respectieve bepalingen van deze verordening. Deze regel mag echter niet leiden tot een verlaging van het vereiste betrouwbaarheidsniveau voor kritieke producten met digitale elementen die onder deze verordening vallen. Daarom moeten, in afwijking van deze regel, AI-systemen met een hoog risico die binnen het toepassingsgebied van Verordening [de AI-verordening] vallen en ook worden aangemerkt als kritieke producten met digitale elementen overeenkomstig deze verordening en waarop de conformiteitsbeoordelingsprocedure op basis van interne controle als bedoeld in bijlage VI bij Verordening [de AI-verordening] van toepassing is, onderworpen zijn aan de bepalingen inzake conformiteitsbeoordeling van deze verordening wat de essentiële eisen van deze verordening betreft. In dat geval moeten voor alle andere aspecten die onder Verordening [de AI-verordening] vallen, de respectieve bepalingen inzake conformiteitsbeoordeling op basis van interne controle van bijlage VI bij Verordening [de AI-verordening] van toepassing zijn.

(30) Machineproducten die binnen het toepassingsgebied van Verordening [voorstel voor een machineverordening] vallen en die producten met digitale elementen zijn in de zin van deze verordening en waarvoor op grond van deze verordening een conformiteitsverklaring is afgegeven, moeten worden geacht in overeenstemming te zijn met de essentiële veiligheids- en gezondheidseisen van [punten 1.1.9 en 1.2.1 van bijlage III] bij Verordening [voorstel voor een machineverordening], wat betreft de bescherming tegen corruptie en de veiligheid en betrouwbaarheid van besturingssystemen, voor zover de overeenstemming met die eisen wordt aangetoond door de krachtens deze verordening afgegeven EU-conformiteitsverklaring.

(31) Verordening [voorstel voor een verordening betreffende de Europese ruimte voor gezondheidsgegevens] vormt een aanvulling op de essentiële eisen van deze verordening. De systemen voor elektronische patiëntendossiers ("EPD-systemen") die onder het toepassingsgebied van Verordening [voorstel voor een verordening betreffende de Europese ruimte voor gezondheidsgegevens] vallen en producten met digitale elementen in de zin van deze verordening zijn, moeten daarom ook voldoen

[15] Verordening [de AI-verordening].

aan de essentiële eisen van deze verordening. De fabrikanten ervan moeten de conformiteit aantonen, zoals vereist bij Verordening [voorstel voor een verordening betreffende de Europese ruimte voor gezondheidsgegevens]. Om de naleving te vergemakkelijken, kunnen fabrikanten één enkele technische documentatie opstellen die de door beide rechtshandelingen vereiste elementen bevat. Aangezien deze verordening niet van toepassing is op SaaS als zodanig, vallen EPD-systemen die via het SaaS-licentie- en leveringsmodel worden aangeboden, niet binnen het toepassingsgebied van deze verordening. Evenzo vallen EPD-systemen die intern worden ontwikkeld en gebruikt, niet binnen het toepassingsgebied van deze verordening, aangezien zij niet in de handel worden gebracht.

(32) Om ervoor te zorgen dat producten met digitale elementen zowel bij het in de handel brengen als gedurende hun hele levenscyclus beveiligd zijn, moeten essentiële eisen inzake de respons op kwetsbaarheden en essentiële cyberbeveiligingsvereisten met betrekking tot de kenmerken van producten met digitale elementen worden vastgesteld. Hoewel fabrikanten moeten voldoen aan alle essentiële eisen in verband met de respons op kwetsbaarheden en ervoor moeten zorgen dat al hun producten worden geleverd zonder bekende kwetsbaarheden die kunnen worden uitgebuit, moeten zij bepalen welke andere essentiële eisen met betrekking tot de productkenmerken relevant zijn voor het betrokken producttype. Daartoe moeten fabrikanten de cyberbeveiligingsrisico's beoordelen die verbonden zijn aan een product met digitale elementen, om betrokken risico's en relevante essentiële eisen vast te stellen en passende geharmoniseerde normen of gemeenschappelijke specificaties toe te passen.

(33) Om de beveiliging van producten met digitale elementen die op de interne markt worden gebracht, te verbeteren, is het noodzakelijk essentiële eisen vast te stellen. Deze essentiële eisen mogen geen afbreuk doen aan de gecoördineerde risicobeoordelingen van kritieke toeleveringsketens van de EU die zijn vastgesteld bij [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)][16], waarbij rekening wordt gehouden met zowel technische als, in voorkomend geval, niet-technische risicofactoren, zoals ongepaste beïnvloeding van leveranciers door een derde land. Voorts mogen ze geen afbreuk doen aan de prerogatieven van de lidstaten om aanvullende eisen vast te stellen die rekening houden met niet-technische factoren om een hoog niveau van veerkracht te waarborgen, waaronder die welke zijn gedefinieerd in Aanbeveling (EU) 2019/534, in de gecoördineerde risicobeoordeling van de beveiliging van 5G-netwerken in de hele EU en in het EU-instrumentarium voor 5G-cyberbeveiliging dat is overeengekomen door de NIS-samenwerkingsgroep als bedoeld in [Richtlijn XXX/XXXX (NIS2)].

(34) Om ervoor te zorgen dat de nationale CSIRT's en het overeenkomstig artikel [artikel X] van Richtlijn [Richtlijn XX/XXXX (NIS2)] aangewezen centrale contactpunt de informatie krijgen die zij nodig hebben om hun taken te vervullen en het algemene niveau van cyberbeveiliging van essentiële en belangrijke entiteiten te verhogen, en om de doeltreffende werking van markttoezichtautoriteiten te waarborgen, moeten fabrikanten van producten met digitale elementen Enisa in kennis stellen van actief uitgebuite kwetsbaarheden. Aangezien de meeste producten met digitale elementen op de hele interne markt in de handel worden gebracht, moet elke

[16] Richtlijn XXX van het Europees Parlement en de Raad van [datum] [betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148 (PB L XX, van XX.XX.XXXX, blz. X)].

uitgebuite kwetsbaarheid in een product met digitale elementen worden beschouwd als een bedreiging voor de werking van de interne markt. Fabrikanten moeten ook overwegen gerepareerde kwetsbaarheden openbaar te maken in de Europese kwetsbaarheidsdatabase die is opgezet krachtens Richtlijn [Richtlijn XX/XXXX (NIS2)] en wordt beheerd door Enisa of in een andere openbaar toegankelijke kwetsbaarheidsdatabase.

(35) Fabrikanten moeten eveneens elk incident dat gevolgen heeft voor de veiligheid van het product met digitale elementen, aan Enisa melden. Niettegenstaande de verplichtingen inzake incidentenmelding in Richtlijn [Richtlijn XXX/XXXX (NIS2)] voor essentiële en belangrijke entiteiten, is het van cruciaal belang dat Enisa, de door de lidstaten overeenkomstig artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)] aangewezen centrale contactpunten en de markttoezichtautoriteiten informatie ontvangen van de fabrikanten van producten met digitale elementen, aan de hand waarvan zij de veiligheid van deze producten kunnen beoordelen. Om ervoor te zorgen dat gebruikers snel kunnen reageren op incidenten die gevolgen hebben voor de beveiliging van hun producten met digitale elementen, moeten fabrikanten ook hun gebruikers informeren over dergelijke incidenten en, in voorkomend geval, over eventuele corrigerende maatregelen die de gebruikers kunnen nemen om de gevolgen van het incident te beperken, bijvoorbeeld door relevante informatie op hun websites te publiceren of, indien de fabrikant in staat is contact op te nemen met de gebruikers en indien de risico's dit rechtvaardigen, door rechtstreeks contact met de gebruikers op te nemen.

(36) Fabrikanten van producten met digitale elementen moeten een gecoördineerd beleid inzake openbaarmaking van kwetsbaarheden invoeren om de melding van kwetsbaarheden door personen of entiteiten te vergemakkelijken. In een beleid voor gecoördineerde openbaarmaking van kwetsbaarheden moet een gestructureerd proces worden gespecificeerd aan de hand waarvan kwetsbaarheden op dusdanige wijze aan een fabrikant worden gemeld dat deze in staat is een diagnose te stellen en de kwetsbaarheden te verhelpen voordat gedetailleerde informatie over de kwetsbaarheden aan derden of het publiek wordt vrijgegeven. Aangezien informatie over kwetsbaarheden die kunnen worden uitgebuit in veelgebruikte producten met digitale elementen tegen hoge prijzen op de zwarte markt kan worden verkocht, moeten fabrikanten van dergelijke producten als onderdeel van hun beleid voor gecoördineerde openbaarmaking van kwetsbaarheden programma's kunnen gebruiken om de melding van kwetsbaarheden te stimuleren, door ervoor te zorgen dat personen of entiteiten erkenning en compensatie krijgen voor hun inspanningen (zogenaamde "bug bounty"-programma's).

(37) Om kwetsbaarheidsanalyses te vergemakkelijken, moeten fabrikanten componenten in de producten met digitale elementen identificeren en documenteren, onder meer door een softwarestuklijst op te stellen. Een softwarestuklijst kan degenen die software vervaardigen, kopen en exploiteren, informatie verschaffen die hun inzicht in de toeleveringsketen vergroot, wat tal van voordelen heeft, en met name fabrikanten en gebruikers helpt nieuwe kwetsbaarheden en risico's op te sporen. Het is bijzonder belangrijk dat fabrikanten ervoor zorgen dat hun producten geen kwetsbare componenten bevatten die door derden zijn ontwikkeld.

(38) Om de beoordeling van de conformiteit met de eisen van deze verordening te vergemakkelijken, moet er een vermoeden van conformiteit bestaan voor producten met digitale elementen die in overeenstemming zijn met geharmoniseerde normen die de essentiële eisen van deze verordening omzetten in gedetailleerde technische

specificaties, en die zijn vastgesteld overeenkomstig Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad[17]. Verordening (EU) nr. 1025/2012 voorziet in een procedure voor bezwaren tegen geharmoniseerde normen die niet volledig aan de eisen van deze verordening voldoen.

(39) Bij Verordening (EU) 2019/881 is een vrijwillig Europees kader voor cyberbeveiligingscertificering voor ICT-producten, -processen en -diensten vastgesteld. Europese cyberbeveiligingscertificeringsregelingen kunnen betrekking hebben op producten met digitale elementen die onder deze verordening vallen. Deze verordening moet synergieën tot stand brengen met Verordening (EU) 2019/881. Om de beoordeling van de conformiteit met de eisen van deze verordening te vergemakkelijken, worden producten met digitale elementen die zijn gecertificeerd of waarvoor een conformiteitsverklaring is afgegeven in het kader van een cyberbeveiligingsregeling krachtens Verordening (EU) 2019/881 en die door de Commissie in een uitvoeringshandeling is geïdentificeerd, geacht in overeenstemming te zijn met de essentiële eisen van deze verordening, voor zover het cyberbeveiligingscertificaat of de conformiteitsverklaring of delen daarvan die eisen dekken. De behoefte aan nieuwe Europese cyberbeveiligingscertificeringsregelingen voor producten met digitale elementen moet in het licht van deze verordening worden beoordeeld. Dergelijke toekomstige Europese cyberbeveiligingscertificeringsregelingen voor producten met digitale elementen moeten rekening houden met de essentiële eisen van deze verordening en de naleving ervan vergemakkelijken. De Commissie moet de bevoegdheid krijgen om door middel van uitvoeringshandelingen de Europese cyberbeveiligingscertificeringsregelingen te specificeren die kunnen worden gebruikt om de conformiteit met de essentiële eisen van deze verordening aan te tonen. Voorts moet de Commissie, om onnodige administratieve lasten voor fabrikanten te vermijden, in voorkomend geval specificeren of een cyberbeveiligingscertificaat dat in het kader van een dergelijke Europese cyberbeveiligingscertificeringsregeling is afgegeven, de verplichting voor fabrikanten om een conformiteitsbeoordeling door derden te laten verrichten, zoals bepaald in deze verordening voor de overeenkomstige eisen, overbodig maakt.

(40) Bij de inwerkingtreding van de uitvoeringshandeling tot vaststelling van [Uitvoeringsverordening (EU) …/… van de Commissie van XXX betreffende de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling] (EUCC) die betrekking heeft op onder deze verordening vallende hardwareproducten, zoals hardwarebeveiligingsmodules en microprocessoren, kan de Commissie door middel van een uitvoeringshandeling bepalen hoe de EUCC een vermoeden van conformiteit met de essentiële eisen als bedoeld in bijlage I bij deze verordening of delen daarvan vestigt. Voorts kan in een dergelijke uitvoeringshandeling worden gespecificeerd hoe een in het kader van de EUCC afgegeven certificaat de verplichting voor fabrikanten wegneemt om een beoordeling te laten uitvoeren door derden, zoals vereist krachtens deze verordening voor de overeenkomstige eisen.

---

[17] Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12).

(41) Indien er geen geharmoniseerde normen worden vastgesteld of wanneer de geharmoniseerde normen onvoldoende betrekking hebben op de essentiële eisen van deze verordening, moet de Commissie door middel van uitvoeringshandelingen gemeenschappelijke specificaties kunnen vaststellen. Redenen om dergelijke gemeenschappelijke specificaties te ontwikkelen, in plaats van te vertrouwen op geharmoniseerde normen, kunnen onder meer bestaan in een afwijzing van het normalisatieverzoek door een van de Europese normalisatieorganisaties, onnodige vertragingen bij de vaststelling van passende geharmoniseerde normen, of een gebrek aan overeenstemming van ontwikkelde normen met de eisen van deze verordening of met een verzoek van de Commissie. Om de beoordeling van de conformiteit met de essentiële eisen van deze verordening te vergemakkelijken, moet er een vermoeden van conformiteit bestaan voor producten met digitale elementen die in overeenstemming zijn met de gemeenschappelijke specificaties, die de Commissie overeenkomstig deze verordening heeft vastgesteld om gedetailleerde technische specificaties van die eisen aan te geven.

(42) Fabrikanten moeten een EU-conformiteitsverklaring opstellen om de krachtens deze verordening vereiste informatie te verstrekken over de conformiteit van producten met digitale elementen met de essentiële eisen van deze verordening en, indien van toepassing, van de andere relevante harmonisatiewetgeving van de Unie waaronder het product valt. Fabrikanten kunnen ook op grond van andere wetgeving van de Unie worden verplicht een EU-conformiteitsverklaring op te stellen. Om effectieve toegang tot informatie voor markttoezichtdoeleinden te waarborgen, moet één EU-conformiteitsverklaring worden opgesteld met betrekking tot de naleving van alle betrokken rechtshandelingen van de Unie. Om de administratieve lasten voor marktdeelnemers te verminderen, moet het mogelijk zijn dat die EU-conformiteitsverklaring een dossier is dat bestaat uit afzonderlijke conformiteitsverklaringen.

(43) De CE-markering, die de conformiteit van een product aangeeft, is het zichtbare resultaat van een volledig proces waaronder de conformiteitsbeoordeling in ruime zin valt. De algemene beginselen voor de CE-markering zijn vastgesteld in Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad[18]. In deze verordening moeten voorschriften worden vastgesteld voor het aanbrengen van de CE-markering op producten met digitale elementen. De CE-markering moet de enige markering zijn die garandeert dat producten met digitale elementen voldoen aan de eisen van deze verordening.

(44) Om marktdeelnemers in staat te stellen de conformiteit met de essentiële eisen van deze verordening aan te tonen en om markttoezichtautoriteiten in staat te stellen te waarborgen dat producten met digitale elementen die op de markt worden aangeboden, aan deze eisen voldoen, moet worden voorzien in conformiteitsbeoordelingsprocedures. Bij Besluit nr. 768/2008/EG van het Europees Parlement en de Raad[19] zijn modules voor conformiteitsbeoordelingsprocedures vastgesteld die in verhouding staan tot het betrokken risiconiveau en het vereiste

[18] 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 (PB L 218 van 13.8.2008, blz. 30).

[19] Besluit nr. 768/2008/EG van het Europees Parlement en de Raad van 9 juli 2008 betreffende een gemeenschappelijk kader voor het verhandelen van producten en tot intrekking van Besluit 93/465/EEG van de Raad (PB L 218 van 13.8.2008, blz. 82).

beveiligingsniveau. Om voor coherentie tussen de sectoren te zorgen en ad-hocvarianten te voorkomen, zijn de conformiteitsbeoordelingsprocedures die geschikt zijn om de conformiteit van producten met digitale elementen met de essentiële eisen van deze verordening te controleren, op die modules gebaseerd. De conformiteitsbeoordelingsprocedures moeten zowel product- als procesgerelateerde eisen voor de gehele levenscyclus van producten met digitale elementen onderzoeken en verifiëren, met inbegrip van planning, ontwerp, ontwikkeling of productie, testen en onderhoud van het product.

(45) De conformiteitsbeoordeling van producten met digitale elementen moet in de regel door de fabrikant onder eigen verantwoordelijkheid worden uitgevoerd volgens de procedure op basis van module A bij Besluit 768/2008/EG. De fabrikant moet over de flexibiliteit blijven beschikken om te kiezen voor een strengere conformiteitsbeoordelingsprocedure waarbij een derde partij betrokken is. Indien het product wordt aangemerkt als een kritiek product van klasse I, is aanvullende zekerheid vereist om aan te tonen dat het product aan de essentiële eisen van deze verordening voldoet. De fabrikant moet in het kader van Verordening (EU) 2019/881 geharmoniseerde normen, gemeenschappelijke specificaties of cyberbeveiligingscertificeringsregelingen toepassen die door de Commissie in een uitvoeringshandeling zijn vastgesteld, indien hij de conformiteitsbeoordeling onder zijn eigen verantwoordelijkheid wil uitvoeren (module A). Als de fabrikant dergelijke geharmoniseerde normen, gemeenschappelijke specificaties of cyberbeveiligingscertificeringsregelingen niet toepast, moet hij een conformiteitsbeoordeling ondergaan waarbij een derde partij betrokken is. Rekening houdend met de administratieve lasten voor fabrikanten en het feit dat cyberbeveiliging een belangrijke rol speelt in de ontwerp- en ontwikkelingsfase van materiële en immateriële producten met digitale elementen, zijn conformiteitsbeoordelingsprocedures op basis van respectievelijk de modules B+C of module H van Besluit 768/2008/EG gekozen als de meest geschikte voor een evenredige en doeltreffende beoordeling van de conformiteit van kritieke producten met digitale elementen. De fabrikant die de conformiteitsbeoordeling door derden laat verrichten, kan de procedure kiezen die het best past bij zijn ontwerp- en productieproces. Gezien het nog grotere cyberbeveiligingsrisico in verband met het gebruik van als kritieke producten van klasse II aangemerkte producten, moet bij de conformiteitsbeoordeling in dat geval altijd een derde partij betrokken zijn.

(46) Hoewel de vervaardiging van materiële producten met digitale elementen doorgaans vereist dat fabrikanten aanzienlijke inspanningen leveren tijdens de ontwerp-, ontwikkelings- en productiefase, is de vervaardiging van producten met digitale elementen in de vorm van software bijna uitsluitend gericht op ontwerp en ontwikkeling, terwijl de productiefase een kleine rol speelt. Toch moeten softwareproducten in veel gevallen nog worden samengesteld, gebouwd, verpakt, beschikbaar gesteld voor download of op fysieke dragers worden gekopieerd voordat zij in de handel worden gebracht. Deze activiteiten moeten worden beschouwd als productieactiviteiten wanneer met de desbetreffende conformiteitsbeoordelingsmodules wordt nagegaan of het product in de ontwerp-, ontwikkelings- en productiefasen aan de essentiële eisen van deze verordening voldoet.

(47) Met het oog op de uitvoering van een conformiteitsbeoordeling door derden voor producten met digitale elementen, moeten de conformiteitsbeoordelingsinstanties door de nationale aanmeldende autoriteiten bij de Commissie en de andere lidstaten worden

aangemeld, op voorwaarde dat zij voldoen aan een reeks vereisten, met name inzake onafhankelijkheid, competenties en afwezigheid van belangenconflicten.

(48) Om een consistent kwaliteitsniveau bij de uitvoering van de conformiteitsbeoordeling van producten met digitale elementen te waarborgen, moeten ook eisen worden vastgesteld voor aanmeldende autoriteiten en andere instanties die betrokken zijn bij de beoordeling, aanmelding en monitoring van aangemelde instanties. Het in deze verordening beschreven systeem moet worden aangevuld met het accreditatiesysteem van Verordening (EG) nr. 765/2008. Aangezien accreditatie een essentieel middel is om de bekwaamheid van conformiteitsbeoordelingsinstanties te verifiëren, moet zij ook worden gebruikt voor doeleinden van aanmelding.

(49) Transparante accreditatie zoals bepaald in Verordening (EG) nr. 765/2008, die het nodige vertrouwen in conformiteitscertificaten waarborgt, moet door de nationale overheidsinstanties in de hele Unie worden beschouwd als het middel bij uitstek om de technische bekwaamheid van conformiteitsbeoordelingsinstanties aan te tonen. Nationale autoriteiten kunnen echter van mening zijn dat zij over passende middelen beschikken om die beoordeling zelf uit te voeren. In dergelijke gevallen moeten zij, om het juiste niveau van geloofwaardigheid van door andere nationale autoriteiten verrichte evaluaties te waarborgen, aan de Commissie en de andere lidstaten de nodige documenten overleggen om te staven dat de geëvalueerde conformiteitsbeoordelingsinstanties voldoen aan de toepasselijke regelgevingsvereisten.

(50) Conformiteitsbeoordelingsinstanties besteden vaak een deel van hun activiteiten in verband met conformiteitsbeoordelingen uit of doen een beroep op een dochteronderneming. Om het beschermingsniveau te waarborgen dat is vereist voor het product met digitale elementen dat in de handel wordt gebracht, is het van essentieel belang dat de betrokken onderaannemers en dochterondernemingen voor de uitvoering van conformiteitsbeoordelingstaken aan dezelfde eisen voldoen als de aangemelde instanties.

(51) De aanmeldende autoriteit moet de aanmelding van een conformiteitsbeoordelingsinstantie via het Nando-informatiesysteem (New Approach Notified and Designated Organisations) aan de Commissie en de andere lidstaten toezenden. Nando is het door de Commissie ontwikkelde en beheerde elektronische aanmeldingsinstrument dat een lijst van alle aangemelde instanties bevat.

(52) Omdat aangemelde instanties hun diensten in de gehele Unie kunnen aanbieden, moeten de andere lidstaten en de Commissie in staat worden gesteld bezwaren in te brengen tegen een aangemelde instantie. Daarom is het belangrijk te voorzien in een periode waarin eventuele twijfels of bedenkingen omtrent de bekwaamheid van conformiteitsbeoordelingsinstanties kunnen worden weggenomen voordat zij als aangemelde instantie gaan functioneren.

(53) In het belang van het concurrentievermogen is het cruciaal dat aangemelde instanties de conformiteitsbeoordelingsprocedures toepassen op een wijze die geen onnodige lasten voor de marktdeelnemers met zich meebrengt. Om dezelfde reden, en om een gelijke behandeling van de marktdeelnemers te waarborgen, moet bij de technische uitvoering van de conformiteitsbeoordelingsprocedures worden gezorgd voor consistentie. Dit kan het best worden bereikt door passende coördinatie en samenwerking tussen aangemelde instanties.

(54) Markttoezicht is een essentieel instrument om de correcte en uniforme toepassing van de Uniewetgeving te waarborgen. Daarom moet een rechtskader tot stand worden gebracht waarbinnen passend markttoezicht kan worden uitgeoefend. De in Verordening (EU) 2019/1020 van het Europees Parlement en de Raad[20] vastgestelde voorschriften inzake markttoezicht in de Unie en controle van producten die de markt van de Unie binnenkomen, zijn van toepassing op onder deze verordening vallende producten met digitale elementen.

(55) Overeenkomstig Verordening (EU) 2019/1020 voeren de markttoezichtautoriteiten markttoezicht uit op het grondgebied van die lidstaat. Deze verordening mag de lidstaten niet beletten te kiezen welke autoriteiten voor de uitvoering van die taken bevoegd zijn. Elke lidstaat moet een of meer markttoezichtautoriteiten op zijn grondgebied aanwijzen. De lidstaten kunnen ervoor kiezen een bestaande of nieuwe autoriteit aan te wijzen als markttoezichtautoriteit, met inbegrip van nationale bevoegde autoriteiten als bedoeld in artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)] of aangewezen nationale cyberbeveiligingscertificeringsautoriteiten als bedoeld in artikel 58 van Verordening (EU) 2019/881. Marktdeelnemers moeten volledig samenwerken met markttoezichtautoriteiten en andere bevoegde autoriteiten. Elke lidstaat moet de Commissie en de andere lidstaten in kennis stellen van zijn markttoezichtautoriteiten en de bevoegdheidsgebieden van elk van die autoriteiten en moet zorgen voor de nodige middelen en vaardigheden voor de uitvoering van de toezichttaken in verband met deze verordening. Overeenkomstig artikel 10, leden 2 en 3, van Verordening (EU) 2019/1020 moet elke lidstaat één verbindingsbureau aanwijzen dat onder meer tot taak moet hebben het gecoördineerde standpunt van de markttoezichtautoriteiten te vertegenwoordigen en ondersteuning te bieden bij de samenwerking tussen de markttoezichtautoriteiten in verschillende lidstaten.

(56) Voor de uniforme toepassing van deze verordening moet krachtens artikel 30, lid 2, van Verordening (EU) 2019/1020 een speciale administratievesamenwerkingsgroep (administrative cooperation group — ADCO) worden opgericht. Deze ADCO moet bestaan uit vertegenwoordigers van de aangewezen markttoezichtautoriteiten en, indien relevant, vertegenwoordigers van de verbindingsbureaus. De Commissie moet ondersteunen en aanmoedigen dat markttoezichtautoriteiten samenwerken via het op grond van artikel 29 van Verordening (EU) 2019/1020 opgerichte Unienetwerk voor productconformiteit, bestaande uit vertegenwoordigers van elke lidstaat, waaronder een vertegenwoordiger van elk verbindingsbureau als bedoeld in artikel 10 van Verordening (EU) 2019/1020 en eventueel een nationale deskundige, de voorzitters van de ADCO's en vertegenwoordigers van de Commissie. De Commissie moet deelnemen aan de vergaderingen van het netwerk, zijn subgroepen en de betrokken ADCO. Zij moet deze ADCO ook bijstaan door middel van een uitvoerend secretariaat dat technische en logistieke ondersteuning biedt.

(57) Om te zorgen voor tijdige, evenredige en doeltreffende maatregelen met betrekking tot producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden, moet worden voorzien in een vrijwaringsprocedure van de Unie in het kader waarvan belanghebbende partijen worden geïnformeerd over voorgenomen maatregelen ten aanzien van dergelijke producten. Dit moet de markttoezichtautoriteiten ook in staat

[20] Verordening (EU) 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van producten en tot wijziging van Richtlijn 2004/42/EG en de Verordeningen (EG) nr. 765/2008 en (EU) nr. 305/2011 (PB L 169 van 25.6.2019, blz. 1).

stellen om, in samenwerking met de betrokken marktdeelnemers, indien nodig in een vroeger stadium op te treden. Indien de lidstaten en de Commissie het eens zijn dat een maatregel van een lidstaat gerechtvaardigd is, is er geen verdere betrokkenheid van de Commissie vereist, behalve wanneer de niet-conformiteit kan worden toegeschreven aan tekortkomingen van een geharmoniseerde norm.

(58) In bepaalde gevallen kan een product met digitale elementen dat aan deze verordening voldoet, niettemin een significant cyberbeveiligingsrisico vormen of een risico vormen voor de gezondheid of veiligheid van personen, voor de naleving van verplichtingen uit hoofde van het Unierecht of het interne recht ter bescherming van de grondrechten, voor de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van diensten die via een elektronisch informatiesysteem worden aangeboden door essentiële entiteiten als bedoeld in [bijlage I bij Richtlijn XXX/XXXX (NIS2)], of voor andere aspecten van de bescherming van het algemeen belang. Daarom moeten regels worden vastgesteld die ervoor zorgen dat die risico's worden beperkt. Bijgevolg moeten de markttoezichtautoriteiten maatregelen nemen om de marktdeelnemer te verplichten ervoor te zorgen dat het product dat risico niet langer met zich meebrengt, of om het, afhankelijk van het risico, terug te roepen of uit de handel te nemen. Zodra een markttoezichtautoriteit het vrije verkeer van een product op die manier beperkt of verbiedt, moet de lidstaat de Commissie en de andere lidstaten onverwijld in kennis stellen van de voorlopige maatregelen, met opgave van de redenen en motivering van het besluit. Wanneer een markttoezichtautoriteit dergelijke maatregelen neemt tegen producten die een risico vormen, moet de Commissie onverwijld in overleg treden met de lidstaten en de betrokken marktdeelnemer en de nationale maatregel beoordelen. Aan de hand van deze beoordeling moet de Commissie besluiten of de maatregel al dan niet gerechtvaardigd is. De Commissie moet haar besluit aan alle lidstaten richten en dit onverwijld aan hen en aan de betrokken marktdeelnemers kenbaar maken. Indien de maatregel gerechtvaardigd wordt geacht, kan de Commissie ook overwegen voorstellen tot herziening van de desbetreffende Uniewetgeving vast te stellen.

(59) Voor producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden en waarvoor er redenen zijn om aan te nemen dat zij niet aan deze verordening voldoen, of voor producten die in overeenstemming zijn met deze verordening maar andere belangrijke risico's inhouden, bijvoorbeeld voor de gezondheid of veiligheid van personen, de grondrechten of de verlening van diensten door essentiële entiteiten als bedoeld in [bijlage I bij Richtlijn XXX/XXXX (NIS2)], kan de Commissie Enisa verzoeken een evaluatie te verrichten. Op basis van die evaluatie kan de Commissie door middel van uitvoeringshandelingen corrigerende of beperkende maatregelen op Unieniveau vaststellen, onder meer door te gelasten de respectieve producten binnen een redelijke termijn in verhouding tot de aard van het risico uit de handel te nemen of terug te roepen. De Commissie mag een dergelijke maatregel alleen toepassen in uitzonderlijke omstandigheden die een onmiddellijk optreden rechtvaardigen om de goede werking van de interne markt te beschermen, en alleen wanneer de toezichthoudende autoriteiten geen doeltreffende maatregelen hebben genomen om de situatie te verhelpen. Dergelijke uitzonderlijke omstandigheden kunnen noodsituaties zijn waarin bijvoorbeeld een niet-conform product door de fabrikant in verschillende lidstaten op grote schaal beschikbaar wordt gesteld, ook in belangrijke sectoren wordt gebruikt door entiteiten die binnen het toepassingsgebied van [Richtlijn XXX/XXXX (NIS2)] vallen, en bekende kwetsbaarheden bevat die door kwaadwillige actoren worden uitgebuit en waarvoor de fabrikant geen patches verstrekt. De Commissie kan in dergelijke noodsituaties alleen optreden voor de duur van de uitzonderlijke omstandigheden en indien de niet-

conformiteit met deze verordening of de belangrijke risico's die zich voordoen, blijven bestaan.

(60) Wanneer er aanwijzingen zijn van niet-conformiteit met deze verordening in verschillende lidstaten, moeten de markttoezichtautoriteiten gezamenlijke activiteiten met andere autoriteiten kunnen uitvoeren om de conformiteit te verifiëren en de cyberbeveiligingsrisico's van producten met digitale elementen vast te stellen.

(61) Gelijktijdig gecoördineerde controleacties ("bezemacties") zijn specifieke handhavingsmaatregelen van markttoezichtautoriteiten die de productveiligheid verder kunnen verbeteren. Bezemacties moeten met name worden uitgevoerd wanneer markttrends, consumentenklachten of andere aanwijzingen erop duiden dat bepaalde productcategorieën vaak cyberbeveiligingsrisico's blijken te vormen. Enisa moet bij de markttoezichtautoriteiten voorstellen indienen voor categorieën producten waarvoor bezemacties kunnen worden georganiseerd, onder meer op basis van de meldingen van kwetsbaarheden van producten en incidenten die het ontvangt.

(62) Om ervoor te zorgen dat het regelgevingskader waar nodig kan worden aangepast, moet aan de Commissie de bevoegdheid worden gedelegeerd om overeenkomstig artikel 290 VWEU handelingen vast te stellen voor het actualiseren van de lijst van kritieke producten van bijlage III en het specificeren van de definities van deze categorieën producten. Aan de Commissie moet de bevoegdheid worden gedelegeerd om overeenkomstig dat artikel handelingen vast te stellen om producten met digitale elementen aan te wijzen die onder andere voorschriften van de Unie vallen die hetzelfde beschermingsniveau bieden als deze verordening, waarbij zij moet aangeven of een beperking of uitsluiting van het toepassingsgebied van deze verordening noodzakelijk zou zijn en, in voorkomend geval, het toepassingsgebied van die beperking moet bepalen. Ook moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig dat artikel handelingen vast te stellen met betrekking tot de mogelijke verplichting tot certificering van bepaalde zeer kritieke producten met digitale elementen op basis van in deze verordening vastgestelde kriticiteitscriteria, alsook voor het specificeren van de minimuminhoud van de EU-conformiteitsverklaring en voor het aanvullen van de elementen die in de technische documentatie moeten worden opgenomen. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen plaatsvinden in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven[21]. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen, ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(63) Om eenvormige voorwaarden voor de uitvoering van deze verordening te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend om: de vorm en de elementen van de softwarestuklijst te specificeren, het soort informatie, de vorm en de procedure van de door de fabrikanten bij Enisa ingediende meldingen van actief uitgebuite kwetsbaarheden en incidenten nader te specificeren, de krachtens Verordening (EU) 2019/881 vastgestelde Europese

[21] PB L 123 van 12.5.2016, blz. 1.

cyberbeveiligingscertificeringsregelingen te specificeren die kunnen worden gebruikt om de conformiteit met de essentiële eisen of onderdelen ervan aan te tonen, zoals uiteengezet in bijlage I bij deze verordening, gemeenschappelijke specificaties vast te stellen met betrekking tot de essentiële eisen van bijlage I, technische specificaties voor pictogrammen of andere merktekens in verband met de beveiliging van producten met digitale elementen vast te stellen, evenals mechanismen om het gebruik ervan te bevorderen, besluiten te nemen over corrigerende of beperkende maatregelen op het niveau van de Unie in uitzonderlijke omstandigheden die een onmiddellijk optreden rechtvaardigen om de goede werking van de interne markt te beschermen. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad[22].

(64) Om een betrouwbare en constructieve samenwerking van markttoezichtautoriteiten op Unie- en nationaal niveau te waarborgen, moeten alle bij de toepassing van deze verordening betrokken partijen de vertrouwelijkheid eerbiedigen van informatie en data die zij bij de uitvoering van hun taken verkrijgen.

(65) Om de doeltreffende handhaving van de verplichtingen van deze verordening te waarborgen, moet elke markttoezichtautoriteit de bevoegdheid hebben om administratieve geldboeten op te leggen of om oplegging hiervan te vragen. Daarom moeten maximumniveaus worden vastgesteld voor administratieve geldboeten waarin het interne recht moet voorzien voor niet-naleving van de verplichtingen van deze verordening. Bij de vaststelling van het bedrag van de administratieve geldboete per geval moet rekening worden gehouden met alle relevante omstandigheden van de specifieke situatie en ten minste met die welke uitdrukkelijk in deze verordening zijn vastgesteld, met inbegrip van de vraag of andere markttoezichtautoriteiten reeds administratieve geldboeten hebben opgelegd aan dezelfde marktdeelnemer voor soortgelijke inbreuken. Dergelijke omstandigheden kunnen ofwel verzwarend zijn indien de inbreuk door dezelfde marktdeelnemer voortduurt op het grondgebied van andere lidstaten dan die waar reeds een administratieve boete is opgelegd, ofwel verzachtend, door ervoor te zorgen dat er bij elke andere administratieve geldboete die door een andere markttoezichtautoriteit voor dezelfde marktdeelnemer of hetzelfde type inbreuk wordt vastgesteld, rekening wordt gehouden met andere relevante specifieke omstandigheden, waaronder de in andere lidstaten opgelegde geldboeten en de hoogte daarvan. In al die gevallen moet bij de cumulatieve administratieve geldboete die markttoezichtautoriteiten van verschillende lidstaten aan dezelfde marktdeelnemer voor dezelfde soort inbreuk kunnen opleggen, het evenredigheidsbeginsel in acht worden genomen.

(66) Wanneer administratieve geldboeten worden opgelegd aan personen die geen onderneming zijn, moet de bevoegde autoriteit bij het bepalen van het passende bedrag van de geldboete rekening houden met het algemene inkomensniveau in de lidstaat en met de economische situatie van de persoon. Het moet aan de lidstaten worden overgelaten om te bepalen of en in welke mate overheidsinstanties aan administratieve boeten moeten worden onderworpen.

---

22 Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).

(67) In haar betrekkingen met derde landen streeft de EU ernaar de internationale handel in gereguleerde producten te bevorderen. Er kan een breed scala aan maatregelen worden toegepast om de handel te vergemakkelijken, waaronder verschillende rechtsinstrumenten, zoals bilaterale (intergouvernementele) overeenkomsten inzake wederzijdse erkenning (Mutual Recognition Agreements, MRA's) voor conformiteitsbeoordeling en markering van gereguleerde producten. Overeenkomsten inzake wederzijdse erkenning komen tot stand tussen de Unie en derde landen die een vergelijkbaar niveau van technische ontwikkeling hebben en een verenigbare aanpak op het gebied van conformiteitsbeoordeling hanteren. Deze overeenkomsten zijn gebaseerd op de wederzijdse aanvaarding van certificaten, conformiteitsmarkering en testverslagen die door de conformiteitsbeoordelingsinstanties van een van beide partijen worden afgegeven in overeenstemming met de wetgeving van de andere partij. Er bestaan momenteel overeenkomsten inzake wederzijdse erkenning voor verschillende landen. De overeenkomsten worden gesloten in een aantal specifieke sectoren, die van land tot land kunnen verschillen. Om de handel verder te vergemakkelijken, en in het besef dat toeleveringsketens van producten met digitale elementen mondiaal zijn, kan de Unie overeenkomstig artikel 218 VWEU overeenkomsten inzake wederzijdse erkenning met betrekking tot conformiteitsbeoordeling sluiten voor producten die onder deze verordening vallen. Samenwerking met partnerlanden is ook belangrijk om de cyberweerbaarheid wereldwijd te versterken, aangezien dit op lange termijn zal bijdragen tot een versterkt cyberbeveiligingskader, zowel binnen als buiten de EU.

(68) De Commissie moet deze verordening in overleg met alle belanghebbende partijen op gezette tijden evalueren, met name om na te gaan of zij in het licht van de veranderende maatschappelijke, politieke, technologische of marktomstandigheden moet worden gewijzigd.

(69) De marktdeelnemers moeten voldoende tijd krijgen om zich aan de voorschriften van deze verordening aan te passen. Deze verordening moet [24 maanden] vanaf de inwerkingtreding ervan van toepassing zijn, met uitzondering van de meldingsplicht met betrekking tot actief uitgebuite kwetsbaarheden en incidenten, die [12 maanden] vanaf de inwerkingtreding van deze verordening van toepassing moet zijn.

(70) Aangezien de doelstelling van deze verordening niet voldoende door de lidstaten kan worden verwezenlijkt, maar vanwege de gevolgen van het optreden beter op het niveau van de Unie kan worden bereikt, kan de Unie maatregelen nemen overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om deze doelstelling te verwezenlijken.

(71) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad[23] en heeft op […] advies uitgebracht,

---

[23] Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Voorwerp

Bij deze verordening worden vastgesteld:

(a) regels voor het in de handel brengen van producten met digitale elementen om de cyberbeveiliging van dergelijke producten te waarborgen;

(b) essentiële eisen voor het ontwerp, de ontwikkeling en de productie van producten met digitale elementen, en verplichtingen voor marktdeelnemers met betrekking tot deze producten, op het gebied van cyberbeveiliging;

(c) essentiële eisen voor de procedures inzake de respons op kwetsbaarheden, die fabrikanten hebben ingesteld om de cyberbeveiliging van producten met digitale elementen gedurende de gehele levenscyclus te waarborgen, en verplichtingen voor marktdeelnemers met betrekking tot deze procedures;

(d) voorschriften inzake markttoezicht en handhaving van bovengenoemde regels en eisen.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op producten met digitale elementen waarvan het beoogde of redelijkerwijs voorzienbaar gebruik een directe of indirecte logische of fysieke gegevensverbinding met een apparaat of netwerk omvat.

2. Deze verordening is niet van toepassing op producten met digitale elementen waarop de volgende handelingen van de Unie van toepassing zijn:

   (a) Verordening (EU) 2017/745;

   (b) Verordening (EU) 2017/746;

   (c) Verordening (EU) 2019/2144.

3. Deze verordening is niet van toepassing op producten met digitale elementen die zijn gecertificeerd overeenkomstig Verordening (EU) 2018/1139.

4. De toepassing van deze verordening op producten met digitale elementen die vallen onder andere voorschriften van de Unie tot vaststelling van eisen die betrekking hebben op alle of een deel van de risico's die door de essentiële eisen van bijlage I worden bestreken, kan worden beperkt of uitgesloten indien:

   (a) een dergelijke beperking of uitsluiting strookt met het algemene regelgevingskader dat op die producten van toepassing is; en

   (b) de sectorale voorschriften hetzelfde beschermingsniveau bieden als deze verordening.

De Commissie is bevoegd overeenkomstig artikel 50 gedelegeerde handelingen vast te stellen tot wijziging van deze verordening, waarin nader wordt bepaald of een dergelijke beperking of uitsluiting noodzakelijk is en met vermelding van de betrokken producten en regels en, in voorkomend geval, het toepassingsgebied van de beperking.

5. Deze verordening is niet van toepassing op producten met digitale elementen die uitsluitend voor doeleinden van nationale veiligheid of voor militaire doeleinden zijn ontwikkeld, noch op producten die specifiek zijn ontworpen voor de verwerking van gerubriceerde informatie.

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "product met digitale elementen": elk software- of hardwareproduct en de oplossingen voor gegevensverwerking op afstand, met inbegrip van software- of hardwarecomponenten die afzonderlijk in de handel worden gebracht;

(2) "gegevensverwerking op afstand": elke gegevensverwerking op afstand waarvoor de software is ontworpen en ontwikkeld door de fabrikant of onder de verantwoordelijkheid van de fabrikant, en bij gebreke waarvan het product met digitale elementen een van zijn functies niet zou kunnen vervullen;

(3) "kritiek product met digitale elementen": een product met digitale elementen dat een cyberbeveiligingsrisico vormt overeenkomstig de criteria van artikel 6, lid 2, en waarvan de belangrijkste functionaliteit is vastgesteld in bijlage III;

(4) "zeer kritiek product met digitale elementen": een product met digitale elementen dat een cyberbeveiligingsrisico vormt overeenkomstig de in artikel 6, lid 5, vastgestelde criteria;

(5) "operationele technologie": programmeerbare digitale systemen of apparaten die in wisselwerking staan met de fysieke omgeving of apparaten beheren die in wisselwerking staan met de fysieke omgeving;

(6) "software": het deel van een elektronisch informatiesysteem dat uit computercode bestaat;

(7) "hardware": een fysiek elektronisch informatiesysteem, of delen daarvan, dat digitale gegevens kan verwerken, opslaan of verzenden;

(8) "component": software of hardware die bedoeld is om in een elektronisch informatiesysteem te worden geïntegreerd;

(9) "elektronisch informatiesysteem": elk systeem, met inbegrip van elektrische of elektronische apparatuur, dat digitale gegevens kan verwerken, opslaan of verzenden;

(10) "logische verbinding": een virtuele weergave van een gegevensverbinding die wordt geïmplementeerd via een software-interface;

(11) "fysieke verbinding": elke verbinding tussen elektronische informatiesystemen of componenten die met behulp van fysieke middelen tot stand wordt gebracht, onder meer via elektrische of mechanische interfaces, draden of radiogolven;

(12) “indirecte verbinding”: een verbinding met een apparaat of netwerk die niet direct plaatsvindt, maar als onderdeel van een groter systeem dat een directe verbinding kan maken met dat apparaat of netwerk;

(13) “privilege”: een toegangsrecht dat aan bepaalde gebruikers of programma’s wordt verleend om binnen een elektronisch informatiesysteem voor de beveiliging relevante activiteiten uit te voeren;

(14) “hoger privilege”: een toegangsrecht dat aan bepaalde gebruikers of programma’s wordt verleend om een uitgebreide reeks voor de beveiliging relevante activiteiten uit te voeren binnen een elektronisch informatiesysteem dat, indien het wordt misbruikt of gecompromitteerd, een kwaadwillige actor in staat zou kunnen stellen ruimere toegang te krijgen tot de middelen van een systeem of organisatie;

(15) “eindpunt”: een apparaat dat op een netwerk is aangesloten en als toegangspunt tot dat netwerk fungeert;

(16) “netwerk- of computingmiddelen”: gegevens- of hardware- of softwarefunctionaliteit die lokaal of via een netwerk of een ander verbonden apparaat toegankelijk is;

(17) “marktdeelnemer”: de fabrikant, de gemachtigde vertegenwoordiger, de importeur, de distributeur of een andere natuurlijke of rechtspersoon op wie de bij deze verordening vastgestelde verplichtingen van toepassing zijn;

(18) “fabrikant”: een natuurlijke of rechtspersoon die producten met digitale elementen ontwikkelt of vervaardigt of die producten met digitale elementen laat ontwerpen, ontwikkelen of vervaardigen, en die onder zijn naam of merknaam in de handel brengt, al dan niet tegen betaling;

(19) “gemachtigde vertegenwoordiger”: een in de Unie gevestigde natuurlijke of rechtspersoon die schriftelijk door een fabrikant is gemachtigd om namens hem specifieke taken te vervullen;

(20) “importeur”: een in de Unie gevestigde natuurlijke of rechtspersoon die een product met digitale elementen in de handel brengt dat de naam of merknaam van een buiten de Unie gevestigde natuurlijke of rechtspersoon draagt;

(21) “distributeur”: een andere natuurlijke of rechtspersoon in de toeleveringsketen dan de fabrikant of de importeur, die een product met digitale elementen in de Unie op de markt aanbiedt zonder de eigenschappen hiervan te beïnvloeden;

(22) “in de handel brengen”: een product met digitale elementen voor het eerst in de Unie op de markt aanbieden;

(23) “op de markt aanbieden”: het in het kader van een handelsactiviteit, al dan niet tegen betaling, verstrekken van een product met digitale elementen met het oog op distributie of gebruik op de markt van de Unie;

(24) “beoogd doel”: het gebruik waarvoor een product met digitale elementen door de fabrikant is bedoeld, met inbegrip van de specifieke context en voorwaarden van het gebruik, zoals gespecificeerd in de informatie die door de fabrikant in de gebruiksinstructies, reclame- of verkoopmaterialen en verklaringen, alsook in de technische documentatie is verstrekt;

(25) “redelijkerwijs voorzienbaar gebruik”: gebruik dat niet noodzakelijk het beoogde doel is dat door de fabrikant in de gebruiksinstructies, reclame- of verkoopmaterialen en verklaringen, alsook in de technische documentatie is verstrekt, maar dat

waarschijnlijk voortvloeit uit redelijkerwijs voorzienbaar menselijk gedrag of redelijkerwijs voorzienbare technische handelingen of interacties;

(26) “redelijkerwijs voorzienbaar verkeerd gebruik”: het gebruik van een product met digitale elementen op een wijze die niet in overeenstemming is met het beoogde doel, maar die kan voortvloeien uit redelijkerwijs te voorzien menselijk gedrag of de redelijkerwijs voorzienbare interactie met andere systemen;

(27) “aanmeldende autoriteit”: de nationale autoriteit die verantwoordelijk is voor het opzetten en uitvoeren van de noodzakelijke procedures voor de beoordeling, aanwijzing en kennisgeving van de conformiteitsbeoordelingsinstanties en de monitoring hiervan;

(28) “conformiteitsbeoordeling”: het proces waarbij wordt nagegaan of aan de essentiële eisen van bijlage I is voldaan;

(29) “conformiteitsbeoordelingsinstantie”: een instantie als gedefinieerd in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;

(30) “aangemelde instantie”: een conformiteitsbeoordelingsinstantie die overeenkomstig artikel 33 van deze verordening en andere relevante harmonisatiewetgeving van de Unie is aangewezen;

(31) “ingrijpende wijziging”: een wijziging van het product met digitale elementen nadat het in de handel is gebracht, die gevolgen heeft voor de conformiteit van het product met digitale elementen met de essentiële eisen van afdeling 1 van bijlage I of leidt tot een wijziging van het beoogde gebruik waarvoor het product met digitale elementen is beoordeeld;

(32) “CE-markering”: een markering waarmee een fabrikant aangeeft dat een product met digitale elementen en de door de fabrikant ingestelde processen in overeenstemming zijn met de essentiële eisen van bijlage I en andere toepasselijke wetgeving van de Unie tot harmonisatie van de voorwaarden voor het in de handel brengen van producten (“harmonisatiewetgeving van de Unie”) die in het aanbrengen ervan voorziet;

(33) “markttoezichtautoriteit”: de autoriteit in de zin van artikel 3, punt 4, van Verordening (EU) 2019/1020;

(34) “geharmoniseerde norm”: een geharmoniseerde norm in de zin van artikel 2, punt 1, c), van Verordening (EU) nr. 1025/2012;

(35) “cyberbeveiligingsrisico”: risico in de zin van artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)];

(36) “significant cyberbeveiligingsrisico”: een cyberbeveiligingsrisico waarvan op basis van de technische kenmerken kan worden aangenomen dat het zeer waarschijnlijk is dat zich een incident voordoet met ernstige negatieve gevolgen, onder meer door aanzienlijke materiële of immateriële verliezen of verstoringen te veroorzaken;

(37) “softwarestuklijst”: een formeel register met gegevens en relaties in de toeleveringsketen van componenten die zijn opgenomen in de software-elementen van een product met digitale elementen;

(38) “kwetsbaarheid”: kwetsbaarheid in de zin van artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)];

(39) “actief uitgebuite kwetsbaarheid”: een kwetsbaarheid waarvoor betrouwbare bewijzen bestaan dat een actor kwaadwillige code heeft uitgevoerd op een systeem zonder toestemming van de systeemeigenaar;

(40) “persoonsgegevens”: gegevens in de zin van artikel 4, punt 1, van Verordening (EU) 2016/679.

Artikel 4

Vrij verkeer

1. Voor de onder deze verordening vallende aangelegenheden belemmeren de lidstaten niet dat producten met digitale elementen die aan deze verordening voldoen, op de markt worden aangeboden.

2. De lidstaten beletten niet dat op handelsbeurzen, tentoonstellingen en demonstraties of soortgelijke evenementen een product met digitale elementen wordt gepresenteerd en gebruikt dat niet aan deze verordening voldoet.

3. De lidstaten beletten niet dat onafgewerkte software die niet aan deze verordening voldoet, wordt aangeboden, op voorwaarde dat de software slechts voor een beperkte periode die nodig is voor testdoeleinden wordt aangeboden en dat een zichtbaar teken duidelijk aangeeft dat de software niet aan deze verordening voldoet en niet voor andere doeleinden dan tests op de markt zal worden aangeboden.

Artikel 5

Eisen voor producten met digitale elementen

Producten met digitale elementen worden alleen op de markt aangeboden indien:

(1) zij voldoen aan de essentiële eisen van afdeling 1 van bijlage I, op voorwaarde dat zij op passende wijze worden geïnstalleerd, onderhouden, gebruikt voor het beoogde doel of in redelijkerwijs voorzienbare omstandigheden en, indien van toepassing, worden bijgewerkt, en

(2) de door de fabrikant ingestelde processen voldoen aan de essentiële eisen van afdeling 2 van bijlage I.

Artikel 6

Kritieke producten met digitale elementen

1. Producten met digitale elementen die behoren tot een categorie die is opgenomen in bijlage III, worden beschouwd als kritieke producten met digitale elementen. Producten met de belangrijkste functionaliteit van een categorie die is opgenomen in bijlage III bij deze verordening, worden geacht onder die categorie te vallen. De categorieën kritieke producten met digitale elementen worden ingedeeld in klasse I en klasse II, zoals vastgesteld in bijlage III, naargelang van het niveau van het cyberbeveiligingsrisico in verband met deze producten.

2. De Commissie is bevoegd om overeenkomstig artikel 50 gedelegeerde handelingen vast te stellen om bijlage III te wijzigen door in de lijst van categorieën kritieke producten met digitale elementen een nieuwe categorie op te nemen of een bestaande categorie van die lijst te schrappen. Bij de beoordeling van de noodzaak om de lijst in bijlage III te wijzigen houdt de Commissie rekening met het niveau van het

cyberbeveiligingsrisico in verband met de categorie producten met digitale elementen. Bij het bepalen van het niveau van het cyberbeveiligingsrisico wordt rekening gehouden met een of meer van de volgende criteria:

(a) de aan cyberbeveiliging gerelateerde functionaliteit van het product met digitale elementen, en of het product met digitale elementen ten minste één van de volgende eigenschappen heeft:

  (i) het is ontworpen om te functioneren met hogere privileges of voor privilegebeheer;

  (ii) het heeft directe of geprivilegieerde toegang tot netwerk- of computingmiddelen;

  (iii) het is ontworpen om de toegang tot gegevens of operationele technologie te regelen;

  (iv) het vervult een functie die van cruciaal belang is voor het vertrouwen, met name beveiligingsfuncties zoals netwerkbeheer, eindpuntbeveiliging en netwerkbeveiliging;

(b) het beoogde gebruik in gevoelige omgevingen, onder meer in industriële omgevingen of door essentiële entiteiten van het type zoals bedoeld in bijlage [bijlage I] bij Richtlijn [Richtlijn XXX/XXXX (NIS2)];

(c) het beoogde gebruik van kritieke of gevoelige functies, zoals de verwerking van persoonsgegevens;

(d) de potentiële omvang van een nadelig effect, met name wat betreft de intensiteit ervan en de mogelijkheid dat meerdere personen worden getroffen;

(e) de mate waarin het gebruik van producten met digitale elementen reeds tot materiële of immateriële verliezen of verstoringen heeft geleid of aanleiding heeft gegeven tot aanzienlijke bezorgdheid in verband met het ontstaan van een nadelig effect.

3. De Commissie is gemachtigd om overeenkomstig artikel 50 een gedelegeerde handeling vast te stellen teneinde deze verordening aan te vullen door de in bijlage III opgenomen definities van de productcategorieën van de klassen I en II te specificeren. De gedelegeerde handeling wordt [uiterlijk 12 maanden na de inwerkingtreding van deze verordening] vastgesteld.

4. Kritieke producten met digitale elementen worden onderworpen aan de conformiteitsbeoordelingsprocedures als bedoeld in artikel 24, leden 2 en 3.

5. De Commissie is bevoegd om overeenkomstig artikel 50 gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen door de categorieën zeer kritieke producten met digitale elementen te specificeren waarvoor de fabrikanten een Europees cyberbeveiligingscertificaat moeten verkrijgen in het kader van een Europese cyberbeveiligingscertificeringsregeling overeenkomstig Verordening (EU) 2019/881 om de conformiteit met de essentiële eisen van bijlage I of delen daarvan aan te tonen. Bij het bepalen van dergelijke categorieën zeer kritieke producten met digitale elementen houdt de Commissie rekening met het niveau van het cyberbeveiligingsrisico in verband met de categorie producten met digitale elementen, in het licht van een of meer van de in lid 2 vermelde criteria, alsook met het oog op de beoordeling of die categorie producten:

(a) wordt gebruikt of ingeroepen door de essentiële entiteiten van het type als bedoeld in bijlage [bijlage I] bij Richtlijn [Richtlijn XXX/XXXX (NIS2)] of in de toekomst van belang kan zijn voor de activiteiten van deze entiteiten; of

(b) relevant is voor de veerkracht van de gehele toeleveringsketen van producten met digitale elementen tegen verstorende gebeurtenissen.

Artikel 7

Algemene productveiligheid

In afwijking van artikel 2, lid 1, derde alinea, punt b), van Verordening [verordening inzake algemene productveiligheid] en indien producten met digitale elementen niet onderworpen zijn aan specifieke eisen die zijn vastgesteld bij andere harmonisatiewetgeving van de Unie in de zin van [artikel 3, punt 25, van de verordening inzake algemene productveiligheid], zijn hoofdstuk III, punt 1, hoofdstukken V en VII, en de hoofdstukken IX, X en XI van Verordening [verordening inzake algemene productveiligheid] van toepassing op die producten met betrekking tot veiligheidsrisico's die niet onder deze verordening vallen.

Artikel 8

AI-systemen met een hoog risico

1. Producten met digitale elementen die overeenkomstig artikel [artikel 6] van Verordening [de AI-verordening] als AI-systemen met een hoog risico worden aangemerkt en die binnen het toepassingsgebied van deze verordening vallen en voldoen aan de essentiële eisen van afdeling 1 van bijlage I bij deze verordening, en waarvoor de door de fabrikant ingestelde processen in overeenstemming zijn met de essentiële eisen van afdeling 2 van bijlage I, worden geacht in overeenstemming te zijn met de in artikel [artikel 15] van Verordening [de AI-verordening] vastgestelde eisen inzake cyberbeveiliging, onverminderd de andere eisen inzake nauwkeurigheid en robuustheid die zijn opgenomen in bovengenoemd artikel, en voor zover de verwezenlijking van het door die eisen vereiste beveiligingsniveau wordt aangetoond door de in het kader van deze verordening afgegeven EU-conformiteitsverklaring.

2. Op de in lid 1 bedoelde producten en cyberbeveiligingsvereisten is de relevante conformiteitsbeoordelingsprocedure zoals voorgeschreven bij artikel [artikel 43] van Verordening [AI-verordening] van toepassing. Voor die beoordeling hebben aangemelde instanties die volgens Verordening [AI-verordening] het recht hebben om de conformiteit van de AI-systemen met een hoog risico te controleren, ook het recht om de conformiteit van de AI-systemen met een hoog risico binnen het toepassingsgebied van deze verordening met de eisen van bijlage I bij deze verordening te controleren, mits de naleving door die aangemelde instanties van de voorschriften van artikel 29 van deze verordening in het kader van de aanmeldingsprocedure volgens Verordening [AI-verordening] is beoordeeld.

3. In afwijking van lid 2 zijn kritieke producten met digitale elementen die zijn opgenomen in bijlage III bij deze verordening, waarvoor de conformiteitsbeoordelingsprocedures als bedoeld in artikel 24, lid 2, punt a), artikel 24, lid 2, punt b), artikel 24, lid 3, punt a), en artikel 24, lid 3, punt b), uit hoofde van deze verordening moeten worden toegepast en die ook worden aangemerkt als AI-systemen met een hoog risico overeenkomstig artikel [artikel 6] van de verordening [AI-verordening] en waarop de in bijlage [bijlage VI] bij Verordening [de AI-verordening] bedoelde conformiteitsbeoordelingsprocedure op

basis van interne controle van toepassing is, onderworpen aan de bij deze verordening vereiste conformiteitsbeoordelingsprocedures voor zover het de essentiële eisen van deze verordening betreft.

Artikel 9

Machineproducten

Machineproducten die binnen het toepassingsgebied van Verordening [voorstel voor een machineverordening] vallen en die producten met digitale elementen zijn in de zin van deze verordening en waarvoor op grond van deze verordening een EU-conformiteitsverklaring is afgegeven, worden geacht in overeenstemming te zijn met de essentiële veiligheids- en gezondheidseisen van bijlage [punten 1.1.9 en 1.2.1 van bijlage III] bij Verordening [voorstel voor een machineverordening], wat betreft de bescherming tegen corruptie en de veiligheid en betrouwbaarheid van besturingssystemen, en voor zover in de krachtens deze verordening afgegeven EU-conformiteitsverklaring wordt aangetoond dat het door die eisen vereiste beveiligingsniveau wordt bereikt.

HOOFDSTUK II

VERPLICHTINGEN VAN MARKTDEELNEMERS

Artikel 10

Verplichtingen van fabrikanten

1. Wanneer fabrikanten een product met digitale elementen in de handel brengen, zorgen zij ervoor dat het is ontworpen, ontwikkeld en geproduceerd overeenkomstig de essentiële eisen van afdeling 1 van bijlage I.

2. Met het oog op de naleving van de in lid 1 vastgestelde verplichting beoordelen fabrikanten de cyberbeveiligingsrisico's die verbonden zijn aan een product met digitale elementen, en houden zij rekening met het resultaat van die beoordeling tijdens de plannings-, ontwerp-, ontwikkelings-, productie-, leverings- en onderhoudsfase van het product met digitale elementen, teneinde de cyberbeveiligingsrisico's tot een minimum te beperken, beveiligingsincidenten te voorkomen en de gevolgen van dergelijke incidenten tot een minimum te beperken, onder meer met betrekking tot de gezondheid en veiligheid van gebruikers.

3. Wanneer de fabrikant een product met digitale elementen in de handel brengt, neemt hij een beoordeling van de cyberbeveiligingsrisico's op in de technische documentatie als bedoeld in artikel 23 en bijlage V. Voor producten met digitale elementen als bedoeld in artikel 8 en artikel 24, lid 4, die ook onder andere handelingen van de Unie vallen, kan de beoordeling van de cyberbeveiligingsrisico's deel uitmaken van de risicobeoordeling die op grond van die respectieve handelingen van de Unie vereist is. Indien bepaalde essentiële eisen niet van toepassing zijn op het in de handel gebrachte product met digitale elementen, neemt de fabrikant in die documentatie een duidelijke motivering op.

4. Met het oog op de naleving van de in lid 1 vastgestelde verplichting betrachten fabrikanten de nodige zorgvuldigheid bij de integratie van van derden afkomstige componenten in producten met digitale elementen. Zij zorgen ervoor dat dergelijke

componenten de veiligheid van het product met digitale elementen niet in gevaar brengen.

5. De fabrikant documenteert systematisch, op een wijze die in verhouding staat tot de aard en de cyberbeveiligingsrisico's, relevante cyberbeveiligingsaspecten met betrekking tot het product met digitale elementen, met inbegrip van kwetsbaarheden waarvan hij kennisneemt en alle relevante informatie die door derden wordt verstrekt, en werkt, indien van toepassing, de risicobeoordeling van het product bij.

6. Wanneer fabrikanten een product met digitale elementen in de handel brengen en gedurende de verwachte levensduur van het product of gedurende een periode van vijf jaar vanaf het in de handel brengen van het product, indien dit korter is, zorgen zij ervoor dat de kwetsbaarheden van dat product doeltreffend en in overeenstemming met de essentiële eisen van afdeling 2 van bijlage I worden aangepakt.

   Fabrikanten beschikken over passende beleidslijnen en procedures, met inbegrip van een gecoördineerd beleid inzake openbaarmaking van kwetsbaarheden, als bedoeld in afdeling 2, punt 5, van bijlage I, om potentiële kwetsbaarheden in het product met digitale elementen die door interne of externe bronnen zijn gemeld, te behandelen en te verhelpen.

7. Alvorens een product met digitale elementen in de handel te brengen, stellen fabrikanten de in artikel 23 bedoelde technische documentatie op.

   Zij voeren de in artikel 24 bedoelde gekozen conformiteitsbeoordelingsprocedures uit of laten deze uitvoeren.

   Wanneer met die conformiteitsbeoordelingsprocedure is aangetoond dat het product met digitale elementen voldoet aan de essentiële eisen van afdeling 1 van bijlage I en dat de door de fabrikant ingestelde processen voldoen aan de essentiële eisen van afdeling 2 van bijlage I, stellen de fabrikanten de EU-conformiteitsverklaring op overeenkomstig artikel 20 en brengen zij de CE-markering aan overeenkomstig artikel 22.

8. Fabrikanten houden de technische documentatie en de EU-conformiteitsverklaring, indien van toepassing, tot tien jaar nadat het product met digitale elementen in de handel is gebracht ter beschikking van de markttoezichtautoriteiten.

9. Fabrikanten voeren procedures in om de conformiteit te waarborgen van producten met digitale elementen die deel uitmaken van een productiereeks. De fabrikant houdt naar behoren rekening met veranderingen in het ontwikkelings- en productieproces of in het ontwerp of de kenmerken van het product met digitale elementen en met wijzigingen in de geharmoniseerde normen, Europese cyberbeveiligingscertificeringsregelingen of de in artikel 19 bedoelde gemeenschappelijke specificaties waarnaar wordt verwezen in de conformiteitsverklaring van het product met digitale elementen of op grond waarvan de conformiteit van het product wordt geverifieerd.

10. Fabrikanten zorgen ervoor dat producten met digitale elementen vergezeld gaan van de in bijlage II vermelde informatie en instructies, in elektronische of fysieke vorm. Deze informatie en instructies worden verstrekt in een taal die de gebruikers gemakkelijk kunnen begrijpen. Zij moeten duidelijk, begrijpelijk en leesbaar zijn. Zij maken een veilige installatie, een veilige werking en een veilig gebruik van de producten met digitale elementen mogelijk.

11. Fabrikanten verstrekken de EU-conformiteitsverklaring bij het product met digitale elementen of vermelden in de instructies en informatie in de zin van bijlage II het internetadres waarop de EU-conformiteitsverklaring kan worden geraadpleegd.

12. Vanaf het in de handel brengen en gedurende de verwachte levensduur van het product of gedurende een periode van vijf jaar nadat een product met digitale elementen in de handel is gebracht, indien dit korter is, nemen fabrikanten die weten of die redenen hebben om aan te nemen dat het product met digitale elementen of de door de fabrikant ingestelde processen niet in overeenstemming zijn met de essentiële eisen van bijlage I, onmiddellijk de nodige corrigerende maatregelen om het product met digitale elementen of de processen van de fabrikant in overeenstemming te brengen, of om het product zo nodig uit de handel te nemen of terug te roepen.

13. Fabrikanten verstrekken op een met redenen omkleed verzoek van een markttoezichtautoriteit aan die autoriteit, in een taal die zij gemakkelijk kan begrijpen, alle informatie en documentatie, schriftelijk of in elektronische vorm, die nodig is om de conformiteit van het product met digitale elementen en van de door de fabrikant ingestelde processen met de essentiële eisen van bijlage I aan te tonen. Zij verlenen op verzoek van die autoriteit medewerking aan alle maatregelen die zijn genomen om de cyberbeveiligingsrisico's van het product met digitale elementen dat zij in de handel hebben gebracht, weg te nemen.

14. Een fabrikant die zijn activiteiten stopzet en daardoor niet in staat is aan de verplichtingen van deze verordening te voldoen, stelt de betrokken markttoezichtautoriteiten, voordat de stopzetting van de activiteiten van kracht wordt, in kennis van deze situatie, alsook, met alle beschikbare middelen en voor zover mogelijk, de gebruikers van de betrokken producten met digitale elementen die in de handel zijn gebracht.

15. De Commissie kan door middel van uitvoeringshandelingen het formaat en de elementen van de in afdeling 2, punt 1, van bijlage I vastgestelde softwarestuklijst specificeren. Die uitvoeringshandelingen worden overeenkomstig de in artikel 51, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 11

Rapportageverplichtingen van fabrikanten

1. De fabrikant stelt Enisa onverwijld en in elk geval binnen 24 uur nadat hij er kennis van heeft genomen, in kennis van elke actief uitgebuite kwetsbaarheid in het product met digitale elementen. De kennisgeving bevat bijzonderheden over die kwetsbaarheid en, in voorkomend geval, alle genomen corrigerende of risicobeperkende maatregelen. Enisa zendt de kennisgeving na ontvangst zonder onnodig uitstel, tenzij daar gegronde redenen voor zijn in verband met cyberbeveiligingsrisico's, door naar het CSIRT van de betrokken lidstaten dat is aangewezen met het oog op gecoördineerde bekendmaking van kwetsbaarheden overeenkomstig artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)] en stelt de markttoezichtautoriteit in kennis van de gemelde kwetsbaarheid.

2. De fabrikant stelt Enisa onverwijld en in elk geval binnen 24 uur nadat hij er kennis van heeft genomen, in kennis van elk incident dat gevolgen heeft voor de veiligheid van het product met digitale elementen. Enisa zendt de kennisgevingen zonder onnodige vertraging, tenzij er gegronde redenen zijn in verband met

cyberbeveiligingsrisico's, door naar het centrale contactpunt dat is aangewezen overeenkomstig artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)] van de betrokken lidstaten en stelt de markttoezichtautoriteit in kennis van de gemelde incidenten. De melding van incidenten omvat informatie over de ernst en de gevolgen van het incident en vermeldt in voorkomend geval of de fabrikant vermoedt dat het incident het gevolg is van onwettige of kwaadwillige handelingen of van mening is dat het een grensoverschrijdend effect heeft.

3. Enisa zendt de krachtens de leden 1 en 2 meegedeelde informatie naar het Europees Netwerk van verbindingsorganisaties voor cybercrises (CyCLONe), opgericht bij artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)], indien die informatie relevant is voor het gecoördineerde beheer van grootschalige cyberincidenten en -crises op operationeel niveau.

4. De fabrikant stelt de gebruikers van het product met digitale elementen onverwijld en nadat hij er kennis van heeft genomen, op de hoogte van het incident en, indien nodig, van de corrigerende maatregelen die de gebruiker kan nemen om de gevolgen van het incident te beperken.

5. De Commissie kan door middel van uitvoeringshandelingen het soort informatie, het formaat en de procedure van de krachtens de leden 1 en 2 ingediende kennisgevingen nader specificeren. Die uitvoeringshandelingen worden overeenkomstig de in artikel 51, lid 2, bedoelde onderzoeksprocedure vastgesteld.

6. Enisa stelt, op basis van de krachtens de leden 1 en 2 ontvangen kennisgevingen, om de twee jaar een technisch verslag op over opkomende trends met betrekking tot cyberbeveiligingsrisico's in producten met digitale elementen en dient dit in bij de samenwerkingsgroep als bedoeld in artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)]. Het eerste verslag wordt ingediend binnen 24 maanden nadat de in de leden 1 en 2 vastgestelde verplichtingen van toepassing worden.

7. Bij de vaststelling van een kwetsbaarheid in een component, met inbegrip van een opensourcecomponent, die in het product met digitale elementen is geïntegreerd, melden fabrikanten de kwetsbaarheid aan de persoon of entiteit die de component onderhoudt.

Artikel 12

Gemachtigde vertegenwoordigers

1. Een fabrikant kan een gemachtigde vertegenwoordiger aanwijzen door middel van een schriftelijk mandaat.

2. De verplichtingen uit hoofde van artikel 10, leden 1 tot en met 7, eerste streepje, en lid 9, maken geen deel uit van het mandaat van de gemachtigde vertegenwoordiger.

3. Een gemachtigde vertegenwoordiger voert de taken uit die gespecificeerd zijn in het mandaat dat hij van de fabrikant heeft ontvangen. Het mandaat stelt de gemachtigde vertegenwoordiger in staat ten minste het volgende te doen:

   (a) hij houdt de EU-conformiteitsverklaring als bedoeld in artikel 20 en de technische documentatie als bedoeld in artikel 23 tot tien jaar nadat het product met digitale elementen in de handel is gebracht, ter beschikking van de markttoezichtautoriteiten;

(b) hij verstrekt een markttoezichtautoriteit, wanneer die autoriteit daartoe een met redenen omkleed verzoek indient, alle benodigde informatie en documentatie om de conformiteit van het product met digitale elementen aan te tonen;

(c) hij verleent op verzoek van de markttoezichtautoriteiten medewerking aan alle genomen maatregelen om de risico's van een product met digitale elementen die onder het mandaat van de gemachtigde vertegenwoordiger vallen, weg te nemen.

Artikel 13

Verplichtingen van importeurs

1. Importeurs brengen uitsluitend producten met digitale elementen in de handel die voldoen aan de essentiële eisen van afdeling 1 van bijlage I, en indien de door de fabrikant ingestelde processen voldoen aan de essentiële eisen van afdeling 2 van bijlage I.

2. Alvorens een product met digitale elementen in de handel te brengen, zorgen importeurs ervoor dat:

(a) de fabrikant de juiste conformiteitsbeoordelingsprocedures als bedoeld in artikel 24 heeft uitgevoerd;

(b) de fabrikant de technische documentatie heeft opgesteld;

(c) het product met digitale elementen is voorzien van de in artikel 22 bedoelde CE-markering en vergezeld gaat van de in bijlage II vastgestelde informatie en instructies.

3. Wanneer een importeur van mening is of redenen heeft om aan te nemen dat een product met digitale elementen of de door de fabrikant ingestelde processen niet in overeenstemming zijn met de essentiële eisen van bijlage I, brengt de importeur het product niet in de handel voordat dat product of de door de fabrikant ingestelde processen in overeenstemming zijn gebracht met de essentiële eisen van bijlage I. Bovendien brengt de importeur, indien het product met digitale elementen een significant cyberbeveiligingsrisico inhoudt, de fabrikant en de markttoezichtautoriteiten hiervan op de hoogte.

4. Importeurs vermelden hun naam, geregistreerde handelsnaam of geregistreerde merknaam, het postadres en het e-mailadres waarop contact met hen kan worden opgenomen op het product met digitale elementen, of wanneer dit niet mogelijk is, op de verpakking of in een bij het product met digitale elementen gevoegd document. De contactgegevens worden gesteld in een voor de gebruikers en de markttoezichtautoriteiten gemakkelijk te begrijpen taal.

5. Importeurs zorgen ervoor dat het product met digitale elementen vergezeld gaat van de instructies en informatie van bijlage II, in een voor de gebruikers gemakkelijk te begrijpen taal.

6. Importeurs die weten of redenen hebben om aan te nemen dat een door hen in de handel gebracht product met digitale elementen of de door de fabrikant ingestelde processen niet in overeenstemming is/zijn met de essentiële eisen van bijlage I, nemen onmiddellijk de nodige corrigerende maatregelen om het product met digitale elementen of de door de fabrikant ingestelde processen in overeenstemming te

brengen met de essentiële eisen van bijlage I of om het product zo nodig uit de handel te nemen of terug te roepen.

Wanneer importeurs een kwetsbaarheid in het product met digitale elementen vaststellen, stellen zij de fabrikant onverwijld in kennis van die kwetsbaarheid. Bovendien brengen importeurs, indien het product met digitale elementen een significant cyberbeveiligingsrisico inhoudt, de markttoezichtautoriteiten van de lidstaten waar zij het product met digitale elementen op de markt hebben aangeboden, hiervan onmiddellijk op de hoogte, waarbij zij in het bijzonder de non-conformiteit en alle genomen corrigerende maatregelen uitvoerig beschrijven.

7. Importeurs houden gedurende tien jaar nadat het product met digitale elementen in de handel is gebracht, een exemplaar van de EU-conformiteitsverklaring ter beschikking van de markttoezichtautoriteiten en zorgen ervoor dat de technische documentatie op verzoek aan die autoriteiten kan worden verstrekt.

8. Importeurs verstrekken op een met redenen omkleed verzoek van een markttoezichtautoriteit aan deze autoriteit alle benodigde informatie en documentatie, schriftelijk of in elektronische vorm, om de conformiteit van het product met digitale elementen met de essentiële eisen van afdeling 1 van bijlage I, en van de processen die de fabrikant heeft ingesteld met de essentiële eisen van afdeling 2 van bijlage I aan te tonen, in een voor die autoriteit gemakkelijk te begrijpen taal. Op verzoek van die autoriteit verlenen zij medewerking aan alle maatregelen die zijn genomen om de cyberbeveiligingsrisico's van een product met digitale elementen dat zij in de handel hebben gebracht, weg te nemen.

9. Wanneer de importeur van een product met digitale elementen er kennis van neemt dat de fabrikant van dat product zijn activiteiten heeft stopgezet en daardoor niet in staat is aan de verplichtingen van deze verordening te voldoen, stelt de importeur de betrokken markttoezichtautoriteiten in kennis van deze situatie, alsook, met alle beschikbare middelen en voor zover mogelijk, de gebruikers van de producten met digitale elementen die in de handel zijn gebracht.

Artikel 14

Verplichtingen van distributeurs

1. Distributeurs die een product met digitale elementen op de markt aanbieden, betrachten de nodige zorgvuldigheid in verband met de eisen van deze verordening.

2. Alvorens een product met digitale elementen op de markt aan te bieden, gaan distributeurs na of:

   (a) het product met digitale elementen is voorzien van de CE-markering;

   (b) de fabrikant en de importeur hebben voldaan aan de verplichtingen van respectievelijk artikel 10, lid 10, artikel 10, lid 11, en artikel 13, lid 4.

3. Wanneer een distributeur van mening is of redenen heeft om aan te nemen dat een product met digitale elementen of de door de fabrikant ingestelde processen niet in overeenstemming zijn met de essentiële eisen in bijlage I, mag de distributeur het product met digitale elementen niet op de markt aanbieden voordat dat product of de door de fabrikant ingestelde processen in overeenstemming zijn gebracht. Bovendien brengt de distributeur, indien het product met digitale elementen een significant cyberbeveiligingsrisico inhoudt, de fabrikant en de markttoezichtautoriteiten hiervan op de hoogte.

4. Distributeurs die weten of redenen hebben om aan te nemen dat een door hen op de markt aangeboden product met digitale elementen of de door de fabrikant ingestelde processen niet in overeenstemming is/zijn met de essentiële eisen in bijlage I, zorgen ervoor dat de nodige corrigerende maatregelen worden genomen om het product met digitale elementen of de door de fabrikant ingestelde processen in overeenstemming te brengen, of om het product zo nodig uit de handel te nemen of terug te roepen.

   Wanneer distributeurs een kwetsbaarheid in het product met digitale elementen vaststellen, stellen zij de fabrikant onverwijld in kennis van die kwetsbaarheid. Bovendien brengen distributeurs, indien het product met digitale elementen een significant cyberbeveiligingsrisico inhoudt, de markttoezichtautoriteiten van de lidstaten waar zij het product met digitale elementen op de markt hebben aangeboden hiervan onmiddellijk op de hoogte, waarbij zij in het bijzonder de non-conformiteit en alle genomen corrigerende maatregelen uitvoerig beschrijven.

5. Distributeurs verstrekken op een met redenen omkleed verzoek van een markttoezichtautoriteit aan deze autoriteit alle benodigde informatie en documentatie, schriftelijk of in elektronische vorm, om de conformiteit van het product met digitale elementen en van de processen die de fabrikant heeft ingesteld met de essentiële eisen van bijlage I, aan te tonen, in een voor die autoriteit gemakkelijk te begrijpen taal. Op verzoek van die autoriteit verlenen zij medewerking aan alle maatregelen die zijn genomen om de cyberbeveiligingsrisico's van een product met digitale elementen dat zij op de markt hebben aangeboden, weg te nemen.

6. Wanneer de distributeur van een product met digitale elementen er kennis van neemt dat de fabrikant van dat product zijn activiteiten heeft stopgezet en daardoor niet in staat is aan de verplichtingen van deze verordening te voldoen, stelt de distributeur de betrokken markttoezichtautoriteiten in kennis van deze situatie, alsook, met alle beschikbare middelen en voor zover mogelijk, de gebruikers van de producten met digitale elementen die in de handel zijn gebracht.

Artikel 15

Gevallen waarin de verplichtingen van fabrikanten van toepassing zijn op importeurs en distributeurs

Een importeur of distributeur wordt voor de toepassing van deze verordening als een fabrikant beschouwd en moet aan de in artikel 10 en artikel 11, leden 1, 2, 4 en 7, vermelde verplichtingen van de fabrikant voldoen wanneer die importeur of distributeur een product met digitale elementen onder zijn naam of merknaam in de handel brengt of een ingrijpende wijziging uitvoert aan het reeds in de handel gebrachte product met digitale elementen.

Artikel 16

Andere gevallen waarin de verplichtingen van fabrikanten van toepassing zijn

Een andere natuurlijke of rechtspersoon dan de fabrikant, de importeur of de distributeur die een ingrijpende wijziging uitvoert aan het product met digitale elementen, wordt voor de toepassing van deze verordening als fabrikant beschouwd.

Die persoon moet aan de in artikel 10 en artikel 11, leden 1, 2, 4 en 7, vermelde verplichtingen van de fabrikant voldoen voor het deel van het product waarop de ingrijpende

wijziging betrekking heeft of, indien de ingrijpende wijziging gevolgen heeft voor de cyberbeveiliging van het product met digitale elementen als geheel, voor het gehele product.

Artikel 17

Identificatie van marktdeelnemers

1. Marktdeelnemers verstrekken de markttoezichtautoriteiten op verzoek en indien de informatie beschikbaar is, de volgende informatie:

   (a) naam en adres van alle marktdeelnemers die hun een product met digitale elementen hebben geleverd;

   (b) naam en adres van alle marktdeelnemers aan wie zij een product met digitale elementen hebben geleverd.

2. Marktdeelnemers moeten de in lid 1 bedoelde informatie kunnen verstrekken tot tien jaar nadat het product met digitale elementen bij hen is geleverd, en tot tien jaar nadat zij het product met digitale elementen hebben geleverd.

HOOFDSTUK III

CONFORMITEIT VAN HET PRODUCT MET DIGITALE ELEMENTEN

Artikel 18

Vermoeden van conformiteit

1. Producten met digitale elementen en processen die door de fabrikant zijn ingesteld en in overeenstemming zijn met geharmoniseerde normen of delen daarvan waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, worden geacht in overeenstemming te zijn met de essentiële eisen die door die normen of delen daarvan worden bestreken, zoals beschreven in bijlage I.

2. Producten met digitale elementen en processen die door de fabrikant zijn ingesteld en in overeenstemming zijn met de in artikel 19 bedoelde gemeenschappelijke specificaties, worden geacht in overeenstemming te zijn met de in bijlage I beschreven essentiële eisen, voor zover die eisen door die gemeenschappelijke specificaties worden bestreken.

3. Producten met digitale elementen en processen die door de fabrikant zijn ingesteld en waarvoor een EU-conformiteitsverklaring of -certificaat is afgegeven in het kader van een krachtens Verordening (EU) 2019/881 vastgestelde en overeenkomstig lid 4 gespecificeerde Europese cyberbeveiligingscertificeringsregeling, worden geacht in overeenstemming te zijn met de in bijlage I beschreven essentiële eisen, voor zover die eisen door de EU-conformiteitsverklaring of het cyberbeveiligingscertificaat, of delen daarvan, worden bestreken.

4. De Commissie is bevoegd om door middel van uitvoeringshandelingen de krachtens Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregelingen te specificeren die kunnen worden gebruikt om de conformiteit met de in bijlage I beschreven essentiële eisen of delen daarvan aan te tonen. Bovendien specificeert de Commissie, indien van toepassing, of door een op grond van dergelijke regelingen afgegeven cyberbeveiligingscertificaat de verplichting van een fabrikant om een conformiteitsbeoordeling door derden te laten

verrichten voor de overeenkomstige eisen, zoals uiteengezet in artikel 24, lid 2, punten a) en b), en lid 3, punten a) en b), vervalt. Die uitvoeringshandelingen worden overeenkomstig de in artikel 51, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 19

Gemeenschappelijke specificaties

Wanneer er geen geharmoniseerde normen als bedoeld in artikel 18 bestaan of wanneer de Commissie van oordeel is dat de desbetreffende geharmoniseerde normen niet volstaan om aan de eisen van deze verordening of aan het normalisatieverzoek van de Commissie te voldoen, of wanneer de normalisatieprocedure te veel vertraging oploopt of wanneer het verzoek van de Commissie om geharmoniseerde normen niet door de Europese normalisatieorganisaties is aanvaard, is de Commissie bevoegd om door middel van uitvoeringshandelingen gemeenschappelijke specificaties vast te stellen met betrekking tot de essentiële eisen van bijlage I. Die uitvoeringshandelingen worden overeenkomstig de in artikel 51, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 20

EU-conformiteitsverklaring

1. De EU-conformiteitsverklaring wordt door fabrikanten opgesteld overeenkomstig artikel 10, lid 7, en vermeldt dat is aangetoond dat aan de toepasselijke essentiële eisen van bijlage I is voldaan.

2. De EU-conformiteitsverklaring komt qua structuur overeen met het model in bijlage IV en bevat de in de desbetreffende conformiteitsbeoordelingsprocedures van bijlage VI vermelde elementen. Een dergelijke verklaring wordt voortdurend bijgewerkt. Zij wordt beschikbaar gesteld in de taal of talen zoals voorgeschreven door de lidstaat waar het product met digitale elementen in de handel wordt gebracht of op de markt wordt aangeboden.

3. Wanneer voor een product met digitale elementen uit hoofde van meer dan één handeling van de Unie een EU-conformiteitsverklaring vereist is, wordt één EU-conformiteitsverklaring met betrekking tot al die handelingen van de Unie opgesteld. In die verklaring worden de betrokken handelingen van de Unie vermeld, met inbegrip van de publicatiereferenties ervan.

4. Met het opstellen van de EU-conformiteitsverklaring neemt de fabrikant de verantwoordelijkheid voor de conformiteit van het product op zich.

5. De Commissie is bevoegd overeenkomstig artikel 50 gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen door elementen toe te voegen aan de minimaal vereiste inhoud van de EU-conformiteitsverklaring in bijlage IV om rekening te houden met technologische ontwikkelingen.

Artikel 21

Algemene beginselen van de CE-markering

De in artikel 3, punt 32, bedoelde CE-markering is onderworpen aan de algemene beginselen van artikel 30 van Verordening (EG) nr. 765/2008.

Artikel 22

Regels en voorwaarden voor het aanbrengen van de CE-markering

1. De CE-markering wordt zichtbaar, leesbaar en onuitwisbaar op het product met digitale elementen aangebracht. Wanneer dit gezien de aard van het product met digitale elementen niet mogelijk of gerechtvaardigd is, wordt de markering aangebracht op de verpakking en op de in artikel 20 bedoelde EU-conformiteitsverklaring die het product met digitale elementen vergezelt. Voor producten met digitale elementen in de vorm van software wordt de CE-markering aangebracht hetzij op de in artikel 20 bedoelde EU-conformiteitsverklaring, hetzij op de website die bij het softwareproduct hoort.

2. Gezien de aard van het product met digitale elementen mag de hoogte van de CE-markering die op het product met digitale elementen wordt aangebracht, minder dan 5 mm bedragen, mits de markering zichtbaar en leesbaar blijft.

3. De CE-markering wordt aangebracht voordat het product met digitale elementen in de handel wordt gebracht. Het kan worden gevolgd door een pictogram of een ander merkteken dat wijst op een bijzonder risico of gebruik, zoals bepaald in de in lid 6 bedoelde uitvoeringshandelingen.

4. De CE-markering wordt gevolgd door het identificatienummer van de aangemelde instantie, indien die instantie betrokken is bij de conformiteitsbeoordelingsprocedure op basis van volledige kwaliteitsborging (op basis van module H) als bedoeld in artikel 24.

   Het identificatienummer van de aangemelde instantie wordt aangebracht door die instantie zelf dan wel overeenkomstig haar instructies door de fabrikant of diens gemachtigde vertegenwoordiger.

5. De lidstaten bouwen voort op bestaande mechanismen om de correcte toepassing van de regeling inzake de CE-markering te waarborgen en nemen passende maatregelen in geval van oneigenlijk gebruik van die markering. Indien het product met digitale elementen onderworpen is aan andere wetgeving van de Unie die ook voorziet in het aanbrengen van de CE-markering, geeft de CE-markering aan dat het product ook aan de eisen van die andere wetgeving voldoet.

6. De Commissie kan door middel van uitvoeringshandelingen technische specificaties vaststellen voor pictogrammen of andere merktekens die verband houden met de beveiliging van producten met digitale elementen, alsmede mechanismen om het gebruik ervan te bevorderen. Die uitvoeringshandelingen worden overeenkomstig de in artikel 51, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 23

Technische documentatie

1. De technische documentatie bevat alle relevante gegevens of bijzonderheden over de middelen die de fabrikant gebruikt om ervoor te zorgen dat het product met digitale elementen en de door de fabrikant ingestelde processen aan de essentiële eisen van bijlage I voldoen. De technische documentatie bevat ten minste de in bijlage V vermelde elementen.

2. De technische documentatie wordt opgesteld voordat het product met digitale elementen in de handel wordt gebracht en wordt in voorkomend geval voortdurend

bijgewerkt tijdens de verwachte levensduur van het product of gedurende een periode van vijf jaar nadat een product met digitale elementen in de handel is gebracht, indien dat korter is.

3. Voor producten met digitale elementen als bedoeld in artikel 8 en artikel 24, lid 4, die ook onder andere handelingen van de Unie vallen, wordt één set van technische documentatie opgesteld die de in bijlage V bij deze verordening bedoelde informatie en de bij die respectieve handelingen van de Unie vereiste informatie bevat.

4. De technische documentatie en de correspondentie met betrekking tot een conformiteitsbeoordelingsprocedure worden gesteld in een officiële taal van de lidstaat waar de aangemelde instantie is gevestigd of in een voor die instantie aanvaardbare taal.

5. De Commissie is bevoegd overeenkomstig artikel 50 gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen met de elementen die moeten worden opgenomen in de in bijlage V vermelde technische documentatie, teneinde rekening te houden met technologische ontwikkelingen en ontwikkelingen die zich tijdens het uitvoeringsproces van deze verordening voordoen.

Artikel 24

Conformiteitsbeoordelingsprocedures voor product met digitale elementen

1. De fabrikant voert een conformiteitsbeoordeling uit van het product met digitale elementen en van de processen die de fabrikant heeft ingesteld, om te bepalen of aan de essentiële eisen van bijlage I is voldaan. De fabrikant of diens gemachtigde vertegenwoordiger moet de conformiteit met de essentiële eisen aantonen aan de hand van een van de volgende procedures:

   (a) de procedure voor interne controle (op basis van module A) van bijlage VI; of

   (b) de procedure voor EU-typeonderzoek (op basis van module B) van bijlage VI, gevolgd door conformiteit met het EU-type op basis van interne productiecontrole (op basis van module C) zoals beschreven in bijlage VI; of

   (c) conformiteitsbeoordeling op basis van volledige kwaliteitsborging (op basis van module H) zoals beschreven in bijlage VI.

2. Wanneer de fabrikant of diens gemachtigde vertegenwoordiger bij de beoordeling van de conformiteit van het kritieke product met digitale elementen van klasse I zoals vastgesteld in bijlage III en van de door de fabrikant ingestelde processen met de essentiële eisen van bijlage I, geen geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen als bedoeld in artikel 18 heeft toegepast of slechts gedeeltelijk heeft toegepast, of indien dergelijke geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen niet bestaan, worden het betrokken product met digitale elementen en de door de fabrikant ingestelde processen met betrekking tot die essentiële eisen aan een van de volgende procedures onderworpen:

   (a) de procedure voor EU-typeonderzoek (op basis van module B) van bijlage VI, gevolgd door conformiteit met het EU-type op basis van interne productiecontrole (op basis van module C) zoals beschreven in bijlage VI; of

   (b) conformiteitsbeoordeling op basis van volledige kwaliteitsborging (op basis van module H) zoals beschreven in bijlage VI.

3. Indien het product een kritiek product met digitale elementen van klasse II is zoals beschreven in bijlage III, toont de fabrikant of diens gemachtigde vertegenwoordiger de conformiteit met de essentiële eisen van bijlage I aan door middel van een van de volgende procedures:

   (a) de procedure voor EU-typeonderzoek (op basis van module B) van bijlage VI, gevolgd door conformiteit met het EU-type op basis van interne productiecontrole (op basis van module C) zoals beschreven in bijlage VI; of

   (b) conformiteitsbeoordeling op basis van volledige kwaliteitsborging (op basis van module H) zoals beschreven in bijlage VI.

4. Fabrikanten van producten met digitale elementen die binnen het toepassingsgebied van Verordening [verordening betreffende de Europese ruimte voor gezondheidsgegevens] als EPD-systemen worden aangemerkt, tonen aan dat zij voldoen aan de essentiële eisen van bijlage I bij deze verordening door middel van de desbetreffende conformiteitsbeoordelingsprocedure zoals vereist bij Verordening [hoofdstuk III van de verordening betreffende de Europese ruimte voor gezondheidsgegevens].

5. Aangemelde instanties houden bij het vaststellen van de vergoedingen voor conformiteitsbeoordelingsprocedures rekening met de specifieke belangen en behoeften van kleine en middelgrote ondernemingen (kmo's) en verlagen die vergoedingen in verhouding tot hun specifieke belangen en behoeften.

HOOFDSTUK IV

AANMELDING VAN CONFORMITEITSBEOORDELINGSINSTANTIES

Artikel 25

Aanmelding

De lidstaten stellen de Commissie en de andere lidstaten in kennis van de conformiteitsbeoordelingsinstanties die bevoegd zijn om conformiteitsbeoordelingen overeenkomstig deze verordening te verrichten.

Artikel 26

Aanmeldende autoriteiten

1. De lidstaten wijzen een aanmeldende autoriteit aan die verantwoordelijk is voor de instelling en uitvoering van de nodige procedures voor de beoordeling en aanmelding van conformiteitsbeoordelingsinstanties en het toezicht op de aangemelde instanties, met inbegrip van de naleving van artikel 31.

2. De lidstaten kunnen besluiten dat de beoordeling en het toezicht als bedoeld in lid 1 moeten worden uitgevoerd door een nationale accreditatie-instantie in de zin van en overeenkomstig Verordening (EG) nr. 765/2008.

Artikel 27

Eisen met betrekking tot aanmeldende autoriteiten

1. Een aanmeldende autoriteit is zodanig opgericht dat zich geen belangenconflicten met conformiteitsbeoordelingsinstanties voordoen.

2. Een aanmeldende autoriteit wordt zodanig georganiseerd en functioneert zodanig dat de objectiviteit en onpartijdigheid van haar activiteiten gewaarborgd zijn.

3. Aanmeldende autoriteiten worden zodanig georganiseerd dat elk besluit in verband met de aanmelding van een conformiteitsbeoordelingsinstantie wordt genomen door bekwame personen die de beoordeling niet hebben verricht.

4. Een aanmeldende autoriteit biedt of verricht geen activiteiten die worden uitgevoerd door conformiteitsbeoordelingsinstanties, en verleent geen adviezen op commerciële of concurrentiële basis.

5. Een aanmeldende autoriteit waarborgt dat de verkregen informatie vertrouwelijk wordt behandeld.

6. Een aanmeldende autoriteit beschikt over een voldoende aantal bekwame personeelsleden om haar taken naar behoren uit te voeren.

Artikel 28

Informatieverplichting voor aanmeldende autoriteiten

1. De lidstaten brengen de Commissie op de hoogte van hun procedures voor de beoordeling en aanmelding van conformiteitsbeoordelingsinstanties en voor het toezicht op aangemelde instanties, en van alle wijzigingen daarop.

2. De Commissie maakt deze informatie openbaar.

Artikel 29

Eisen met betrekking tot aangemelde instanties

1. Om te kunnen worden aangemeld, moeten conformiteitsbeoordelingsinstanties aan de eisen van de leden 2 tot en met 12 voldoen.

2. Een conformiteitsbeoordelingsinstantie is naar intern recht opgericht en heeft rechtspersoonlijkheid.

3. Een conformiteitsbeoordelingsinstantie is een derde partij die onafhankelijk is van de door haar beoordeelde organisaties of producten.

   Een instantie die lid is van een ondernemersorganisatie of van een beroepsvereniging die ondernemingen vertegenwoordigt die betrokken zijn bij het ontwerp, de ontwikkeling, de productie, de levering, de assemblage, het gebruik of het onderhoud van producten met digitale elementen die zij beoordeelt, kan als een dergelijke instantie worden beschouwd, op voorwaarde dat haar onafhankelijkheid en de afwezigheid van belangenconflicten worden aangetoond.

4. Een conformiteitsbeoordelingsinstantie, haar hoogste leidinggevenden en de medewerkers die de conformiteitsbeoordelingstaken verrichten, mogen niet de ontwerper, fabrikant, leverancier, installateur, koper, eigenaar, gebruiker of onderhouder zijn van de producten met digitale elementen die worden beoordeeld, noch de gemachtigde vertegenwoordiger van één van die partijen. Dat belet echter

niet het gebruik van beoordeelde producten die nodig zijn voor de activiteiten van de conformiteitsbeoordelingsinstantie of voor het gebruik van dergelijke producten voor persoonlijke doeleinden.

Een conformiteitsbeoordelingsinstantie, haar hoogste leidinggevenden en de medewerkers die de conformiteitsbeoordelingstaken verrichten, zijn noch rechtstreeks noch als vertegenwoordiger van de partijen betrokken bij het ontwerpen, ontwikkelen, vervaardigen, op de markt brengen, installeren, gebruiken of onderhouden van die producten. Zij verrichten geen activiteiten die hun onafhankelijk oordeel of integriteit in het gedrang kunnen brengen met betrekking tot de conformiteitsbeoordelingswerkzaamheden waarvoor zij zijn aangemeld. Dit geldt met name voor adviesdiensten.

Conformiteitsbeoordelingsinstanties zorgen ervoor dat de activiteiten van hun dochterondernemingen of onderaannemers geen afbreuk doen aan de vertrouwelijkheid, objectiviteit of onpartijdigheid van hun conformiteitsbeoordelingswerkzaamheden.

5. Conformiteitsbeoordelingsinstanties en hun personeel voeren conformiteitsbeoordelingswerkzaamheden uit met de grootste mate van beroepsintegriteit en met de vereiste technische bekwaamheid op het specifieke gebied en zijn vrij van elke druk en beïnvloeding, met name van financiële aard, die hun oordeel of de resultaten van hun conformiteitsbeoordelingswerkzaamheden zouden kunnen beïnvloeden, in het bijzonder te aanzien van personen of groepen van personen die belang hebben bij de resultaten van deze activiteiten.

6. Een conformiteitsbeoordelingsinstantie is in staat alle in bijlage VI bedoelde conformiteitsbeoordelingstaken te verrichten waarvoor zij is aangemeld, ongeacht of die taken door de conformiteitsbeoordelingsinstantie zelf dan wel namens haar en onder haar verantwoordelijkheid worden verricht.

Een conformiteitsbeoordelingsinstantie beschikt te allen tijde, voor elke conformiteitsbeoordelingsprocedure en voor elke soort of elke categorie producten met digitale elementen waarvoor zij is aangemeld, over:

(a) personeel met technische kennis en voldoende geschikte ervaring om de conformiteitsbeoordelingstaken te verrichten;

(b) beschrijvingen van de procedures voor de uitvoering van de conformiteitsbeoordeling, waarbij de transparantie en de mogelijkheid tot reproductie van deze procedures worden gewaarborgd. Zij beschikt over passend beleid en geschikte procedures om een onderscheid te maken tussen taken die zij als aangemelde instantie verricht en andere werkzaamheden;

(c) procedures voor de uitoefening van haar werkzaamheden, die naar behoren rekening houden met de omvang van een onderneming, de sector waarin deze actief is, de structuur ervan, de relatieve complexiteit van de technologie van het betrokken product en het massa- of seriële karakter van het productieproces.

Zij heeft de nodige middelen om de technische en administratieve taken in verband met de conformiteitsbeoordelingswerkzaamheden op passende wijze uit te voeren en heeft toegang tot alle vereiste apparatuur of faciliteiten.

7. Het voor de uitvoering van de conformiteitsbeoordelingswerkzaamheden verantwoordelijke personeel beschikt over:

(a) een gedegen technische en beroepsopleiding die alle relevante conformiteitsbeoordelingswerkzaamheden omvat waarvoor de conformiteitsbeoordelingsinstantie is aangemeld;

(b) toereikende kennis van de eisen inzake de beoordelingen die zij verrichten en voldoende bevoegdheid om die beoordelingen uit te voeren;

(c) voldoende kennis van en inzicht in de essentiële eisen, de toepasselijke geharmoniseerde normen en de relevante bepalingen van de harmonisatiewetgeving van de Unie en de uitvoeringshandelingen daarvan;

(d) de bekwaamheid om certificaten, dossiers en rapporten op te stellen die aantonen dat de beoordelingen zijn verricht.

8. De onpartijdigheid van de conformiteitsbeoordelingsinstanties, hun hoogste leidinggevenden en het beoordelingspersoneel moet worden gewaarborgd.

De beloning van de hoogste leidinggevenden en het beoordelingspersoneel van een conformiteitsbeoordelingsinstantie hangt niet af van het aantal uitgevoerde beoordelingen of van de resultaten daarvan.

9. Conformiteitsbeoordelingsinstanties sluiten een aansprakelijkheidsverzekering af, tenzij aansprakelijkheid op grond van het interne recht door de lidstaat wordt gedekt of de lidstaat zelf rechtstreeks verantwoordelijk is voor de conformiteitsbeoordeling.

10. Het personeel van een conformiteitsbeoordelingsinstantie is gebonden aan het beroepsgeheim ten aanzien van alle informatie waarvan het kennisneemt bij de uitoefening van de taken uit hoofde van bijlage VI of van bepalingen van het interne recht die daaraan uitvoering geven, behalve ten aanzien van de markttoezichtautoriteiten van de lidstaat waar de activiteiten plaatsvinden. De eigendomsrechten worden beschermd. De conformiteitsbeoordelingsinstantie beschikt over gedocumenteerde procedures om de naleving van dit lid te waarborgen.

11. Conformiteitsbeoordelingsinstanties nemen deel aan, of zorgen ervoor dat hun beoordelingspersoneel op de hoogte is van de desbetreffende normalisatieactiviteiten en de activiteiten van de uit hoofde van artikel 40 opgerichte coördinatiegroep van aangemelde instanties, en hanteren de door die groep genomen administratieve beslissingen en geproduceerde documenten als algemene richtsnoeren.

12. Conformiteitsbeoordelingsinstanties handelen overeenkomstig een reeks consistente, billijke en redelijke voorwaarden, waarbij met name rekening wordt gehouden met de belangen van kleine en middelgrote ondernemingen met betrekking tot vergoedingen.

Artikel 30

Vermoeden van conformiteit van aangemelde instanties

Wanneer een conformiteitsbeoordelingsinstantie aantoont dat zij voldoet aan de criteria die zijn vastgelegd in de ter zake doende geharmoniseerde normen of delen daarvan, waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, wordt zij geacht aan de in artikel 29 beschreven eisen te voldoen, voor zover deze eisen door de van toepassing zijnde geharmoniseerde normen worden bestreken.

Artikel 31

Dochterondernemingen van en uitbesteding door aangemelde instanties

1. Wanneer een aangemelde instantie specifieke taken in verband met de conformiteitsbeoordeling uitbesteedt of door een dochteronderneming laat uitvoeren, waarborgt zij dat de onderaannemer of dochteronderneming aan de in artikel 29 beschreven eisen voldoet, en brengt zij de aanmeldende autoriteit hiervan op de hoogte.

2. Aangemelde instanties nemen de volledige verantwoordelijkheid op zich voor de taken die worden verricht door onderaannemers of dochterondernemingen, ongeacht waar deze gevestigd zijn.

3. Activiteiten mogen uitsluitend met instemming van de fabrikant worden uitbesteed of door een dochteronderneming worden uitgevoerd.

4. Aangemelde instanties houden de relevante documenten over de beoordeling van de kwalificaties van de onderaannemer of de dochteronderneming en over de door de onderaannemer of dochteronderneming krachtens deze verordening uitgevoerde werkzaamheden ter beschikking van de aanmeldende autoriteit.

Artikel 32

Verzoek om aanmelding

1. Een conformiteitsbeoordelingsinstantie dient een verzoek om aanmelding in bij de aanmeldende autoriteit van de lidstaat waar zij is gevestigd.

2. Het verzoek om aanmelding gaat vergezeld van een beschrijving van de conformiteitsbeoordelingswerkzaamheden, de conformiteitsbeoordelingsprocedures en het product of de producten waarvoor de conformiteitsbeoordelingsinstantie verklaart bekwaam te zijn en, indien dit bestaat, van een accreditatiecertificaat dat is afgegeven door een nationale accreditatie-instantie, waarin wordt verklaard dat de conformiteitsbeoordelingsinstantie voldoet aan de eisen van artikel 29.

3. Wanneer de betrokken conformiteitsbeoordelingsinstantie geen accreditatiecertificaat kan overleggen, verschaft zij de aanmeldende autoriteit alle bewijsstukken die nodig zijn om de naleving van de eisen van artikel 29 te onderzoeken, te erkennen en regelmatig te monitoren.

Artikel 33

Aanmeldingsprocedure

1. Aanmeldende autoriteiten mogen uitsluitend conformiteitsbeoordelingsinstanties aanmelden die aan de eisen van artikel 29 voldoen.

2. De aanmeldende autoriteit stelt de Commissie en de andere lidstaten in kennis van het door de Commissie ontwikkelde en beheerde Nando-informatiesysteem (New Approach Notified and Designated Organisations).

3. Bij de aanmelding worden de conformiteitsbeoordelingsactiviteiten, de conformiteitsbeoordelingsmodules, de betrokken producten en het relevante bekwaamheidsattest uitvoerig beschreven.

4. Wanneer een aanmelding niet is gebaseerd op een accreditatiecertificaat als bedoeld in artikel 32, lid 2, verschaft de aanmeldende autoriteit de Commissie en de andere

lidstaten de bewijsstukken waaruit de bekwaamheid van de conformiteitsbeoordelingsinstantie blijkt, evenals de regeling die waarborgt dat de instantie regelmatig wordt gecontroleerd en zal blijven voldoen aan de eisen van artikel 29.

5. De betrokken instantie mag de activiteiten van een aangemelde instantie alleen verrichten als de Commissie of de andere lidstaten geen bezwaren hebben ingediend binnen twee weken na een aanmelding indien een accreditatiecertificaat wordt gebruikt of binnen twee maanden na een aanmelding indien geen accreditatiecertificaat wordt gebruikt.

   Alleen een dergelijke instantie wordt voor de toepassing van deze verordening als een aangemelde instantie beschouwd.

6. De Commissie en de andere lidstaten worden in kennis gesteld van alle relevante latere wijzigingen in de aanmelding.

Artikel 34

Identificatienummers en lijsten van aangemelde instanties

1. De Commissie kent de aangemelde instantie een identificatienummer toe.

   Zij kent per instantie slechts één nummer toe, ook als de instantie uit hoofde van diverse handelingen van de Unie is aangemeld.

2. De Commissie maakt de lijst van krachtens deze verordening aangemelde instanties openbaar, onder vermelding van de hun toegekende identificatienummers en de activiteiten waarvoor zij zijn aangemeld.

   De Commissie zorgt ervoor dat de lijst actueel blijft.

Artikel 35

Wijzigingen in de aanmelding

1. Als de aanmeldende autoriteit tot de conclusie komt of heeft vernomen dat een aangemelde instantie niet meer aan de eisen van artikel 29 voldoet of haar verplichtingen niet nakomt, wordt de aanmelding door de aanmeldende autoriteit beperkt, geschorst of ingetrokken, afhankelijk van de ernst van het niet-voldoen aan die eisen of het niet-nakomen van die verplichtingen. Zij brengt daar de Commissie en de andere lidstaten onmiddellijk van op de hoogte.

2. Wanneer de aanmelding wordt beperkt, geschorst of ingetrokken, of de aangemelde instantie haar activiteiten heeft gestaakt, doet de aanmeldende lidstaat het nodige om ervoor te zorgen dat de dossiers van die instantie hetzij door een andere aangemelde instantie worden verwerkt, hetzij aan de verantwoordelijke aanmeldende en markttoezichtautoriteiten op hun verzoek ter beschikking kunnen worden gesteld.

Artikel 36

Betwisting van de bekwaamheid van aangemelde instanties

1. De Commissie onderzoekt alle gevallen waarin zij twijfelt of in kennis wordt gesteld van twijfels over de bekwaamheid van een aangemelde instantie of over de vraag of een aangemelde instantie nog aan de eisen voldoet en haar verantwoordelijkheden nakomt.

2. De aanmeldende lidstaat verstrekt de Commissie op verzoek alle informatie over de grondslag van de aanmelding of de handhaving van de bekwaamheid van de betrokken instantie.

3. De Commissie ziet erop toe dat alle gevoelige informatie die zij in de loop van haar onderzoeken ontvangt, vertrouwelijk wordt behandeld.

4. Wanneer de Commissie vaststelt dat een aangemelde instantie niet of niet meer aan de aanmeldingseisen voldoet, brengt zij de aanmeldende lidstaat daarvan op de hoogte en verzoekt zij deze lidstaat de nodige corrigerende maatregelen te nemen en zo nodig de aanmelding in te trekken.

Artikel 37

Operationele verplichtingen van aangemelde instanties

1. Aangemelde instanties voeren conformiteitsbeoordelingen uit volgens de conformiteitsbeoordelingsprocedures van artikel 24 en bijlage VI.

2. De conformiteitsbeoordelingen worden op evenredige wijze uitgevoerd, waarbij wordt voorkomen dat de marktdeelnemers onnodig worden belast. Conformiteitsbeoordelingsinstanties houden bij de uitoefening van hun werkzaamheden naar behoren rekening met de omvang van een onderneming, de sector waarin deze actief is, de structuur ervan, de relatieve complexiteit van de technologie van het betrokken product en het massa- of seriële karakter van het productieproces.

3. Aangemelde instanties nemen echter de striktheid en het beveiligingsniveau in acht die vereist zijn om ervoor te zorgen dat het product aan de bepalingen van de verordening voldoet.

4. Wanneer een aangemelde instantie vaststelt dat een fabrikant niet heeft voldaan aan de eisen in bijlage I of in de overeenkomstige geharmoniseerde normen of in de gemeenschappelijke specificaties als bedoeld in artikel 19, verlangt zij van die fabrikant dat hij passende corrigerende maatregelen neemt en geeft zij geen conformiteitscertificaat af.

5. Wanneer een aangemelde instantie bij het toezicht op de conformiteit na de afgifte van een certificaat vaststelt dat een product niet langer aan de eisen van deze verordening voldoet, verlangt zij van de fabrikant dat hij passende corrigerende maatregelen neemt en schorst zij het certificaat zo nodig of trekt zij het certificaat in.

6. Wanneer geen corrigerende maatregelen worden genomen of de genomen maatregelen niet het vereiste effect hebben, worden de certificaten door de aangemelde instantie naargelang van het geval beperkt, opgeschort of ingetrokken.

Artikel 38

Informatieverplichtingen voor aangemelde instanties

1. Aangemelde instanties brengen de aanmeldende autoriteit op de hoogte van:

   (a) elke weigering, beperking, opschorting of intrekking van een certificaat;

   (b) omstandigheden die van invloed zijn op het toepassingsgebied van en de voorwaarden voor de aanmelding;

(c) verzoeken om informatie over conformiteitsbeoordelingsactiviteiten die zij van markttoezichtautoriteiten ontvangen;

(d) op verzoek, de binnen het toepassingsgebied van hun aanmelding verrichte conformiteitsbeoordelingsactiviteiten en andere activiteiten, waaronder grensoverschrijdende activiteiten en uitbestede activiteiten.

2. Aangemelde instanties verstrekken de andere uit hoofde van deze verordening aangemelde instanties die soortgelijke conformiteitsbeoordelingsactiviteiten voor dezelfde producten verrichten, relevante informatie over negatieve conformiteitsbeoordelingsresultaten, en op verzoek over positieve conformiteitsbeoordelingsresultaten.

Artikel 39

Uitwisseling van ervaringen

De Commissie organiseert de uitwisseling van ervaringen tussen de nationale autoriteiten van de lidstaten die verantwoordelijk zijn voor het aanmeldingsbeleid.

Artikel 40

Coördinatie van aangemelde instanties

1. De Commissie zorgt voor passende coördinatie en samenwerking tussen aangemelde instanties in de vorm van een sectoroverschrijdende groep van aangemelde instanties.

2. De lidstaten zorgen ervoor dat de door hen aangemelde instanties rechtstreeks of via aangestelde vertegenwoordigers aan de werkzaamheden van die groep deelnemen.

HOOFDSTUK V

MARKTTOEZICHT EN HANDHAVING

Artikel 41

Markttoezicht op en controle van producten met digitale elementen op de markt van de Unie

1. Verordening (EU) 2019/1020 is van toepassing op de producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen.

2. Elke lidstaat wijst een of meer markttoezichtautoriteiten aan om de doeltreffende uitvoering van deze verordening te waarborgen. De lidstaten kunnen een bestaande of nieuwe autoriteit aanwijzen om voor deze verordening als markttoezichtautoriteit op te treden.

3. In voorkomend geval werken de markttoezichtautoriteiten samen met de krachtens artikel 58 van Verordening (EU) 2019/881 aangewezen cyberbeveiligingscertificeringsautoriteiten en wisselen zij regelmatig informatie uit. Met betrekking tot het toezicht op de uitvoering van de rapportageverplichtingen uit hoofde van artikel 11 van deze verordening werken de aangewezen markttoezichtautoriteiten samen met Enisa.

4. In voorkomend geval werken de markttoezichtautoriteiten samen met andere markttoezichtautoriteiten die op basis van andere harmonisatiewetgeving van de

Unie voor andere producten zijn aangewezen, en wisselen zij regelmatig informatie uit.

5. De markttoezichtautoriteiten werken in voorkomend geval samen met de autoriteiten die toezicht houden op de wetgeving inzake gegevensbescherming van de Unie. Deze samenwerking omvat het informeren van deze autoriteiten over bevindingen die relevant zijn voor de uitoefening van hun bevoegdheden, onder meer bij het verstrekken van richtsnoeren en advies overeenkomstig lid 8 van dit artikel, indien die richtsnoeren en adviezen betrekking hebben op de verwerking van persoonsgegevens.

   De autoriteiten die toezicht houden op de wetgeving inzake gegevensbescherming van de Unie hebben de bevoegdheid om alle krachtens deze verordening gecreëerde of bewaarde documentatie op te vragen en in te zien wanneer toegang tot die documentatie noodzakelijk is voor de uitvoering van hun taken. Zij stellen de aangewezen markttoezichtautoriteiten van de betrokken lidstaat in kennis van een dergelijk verzoek.

6. De lidstaten zorgen ervoor dat de aangewezen markttoezichtautoriteiten over voldoende financiële en personele middelen beschikken om hun taken uit hoofde van deze verordening uit te voeren.

7. De Commissie bevordert de uitwisseling van ervaringen tussen de aangewezen markttoezichtautoriteiten.

8. Markttoezichtautoriteiten kunnen marktdeelnemers richtsnoeren en advies verstrekken over de uitvoering van deze verordening, met de steun van de Commissie.

9. De markttoezichtautoriteiten brengen jaarlijks verslag uit aan de Commissie over de resultaten van relevante markttoezichtactiviteiten. De aangewezen markttoezichtautoriteiten brengen onverwijld verslag uit aan de Commissie en de betrokken nationale mededingingsautoriteiten over alle tijdens markttoezichtactiviteiten verkregen informatie die potentieel van belang kan zijn voor de toepassing van het mededingingsrecht van de Unie.

10. Voor producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen en overeenkomstig artikel [artikel 6] van Verordening [de AI-verordening] als AI-systemen met een hoog risico worden aangemerkt, zijn de voor de toepassing van Verordening [de AI-verordening] aangewezen markttoezichtautoriteiten de autoriteiten die belast zijn met het markttoezicht uit hoofde van deze verordening. De krachtens Verordening [de AI-verordening] aangewezen markttoezichtautoriteiten werken in voorkomend geval samen met de krachtens deze verordening aangewezen markttoezichtautoriteiten en, met betrekking tot het toezicht op de uitvoering van de rapportageverplichtingen uit hoofde van artikel 11, met Enisa. De krachtens Verordening [de AI-verordening] aangewezen markttoezichtautoriteiten stellen met name de krachtens deze verordening aangewezen markttoezichtautoriteiten in kennis van alle bevindingen die relevant zijn voor hun taken in verband met de uitvoering van deze verordening.

11. Voor de uniforme toepassing van deze verordening wordt overeenkomstig artikel 30, lid 2, van Verordening (EU) 2019/1020 een speciale administratievesamenwerkingsgroep (ADCO) opgericht. Deze ADCO bestaat uit vertegenwoordigers van de aangewezen markttoezichtautoriteiten en, indien relevant, vertegenwoordigers van verbindingsbureaus.

Artikel 42

Toegang tot gegevens en documentatie

Indien dat nodig is om de conformiteit van producten met digitale elementen en de door de fabrikanten ervan ingestelde processen met de essentiële eisen van bijlage I te beoordelen, krijgen de markttoezichtautoriteiten op een met redenen omkleed verzoek toegang tot de gegevens die nodig zijn om het ontwerp, de ontwikkeling, de productie en de respons op kwetsbaarheden van dergelijke producten te beoordelen, met inbegrip van de daarmee verband houdende interne documentatie van de desbetreffende marktdeelnemer.

Artikel 43

Procedure op nationaal niveau voor producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden

1. Indien de markttoezichtautoriteit van een lidstaat voldoende redenen heeft om aan te nemen dat een product met digitale elementen, met inbegrip van de respons op de kwetsbaarheden ervan, een significant cyberbeveiligingsrisico inhoudt, beoordeelt zij of het betrokken product met digitale elementen voldoet aan alle eisen van deze verordening. De desbetreffende marktdeelnemers werken zo nodig samen met de markttoezichtautoriteit.

   Indien de markttoezichtautoriteit bij deze beoordeling vaststelt dat het product met digitale elementen niet aan de eisen van deze verordening voldoet, gelast zij de betrokken marktdeelnemer onverwijld alle passende corrigerende maatregelen te nemen om het product binnen een door haar vast te stellen redelijke termijn, die evenredig is met de aard van het risico, in overeenstemming te brengen met die eisen, uit de handel te nemen of terug te roepen.

   De markttoezichtautoriteit stelt de betrokken aangemelde instantie daarvan in kennis. Artikel 18 van Verordening (EU) 2019/1020 is van toepassing op de passende corrigerende maatregelen.

2. Indien de markttoezichtautoriteit van mening is dat de non-conformiteit niet beperkt blijft tot haar nationale grondgebied, brengt zij de Commissie en de andere lidstaten op de hoogte van de resultaten van de beoordeling en van de maatregelen die zij de marktdeelnemer heeft opgelegd.

3. De fabrikant zorgt ervoor dat alle passende corrigerende maatregelen worden genomen ten aanzien van alle betrokken producten met digitale elementen hij in de Unie op de markt heeft aangeboden.

4. Indien de fabrikant van een product met digitale elementen geen doeltreffende corrigerende actie onderneemt binnen de in lid 1, tweede alinea, bedoelde termijn, neemt de markttoezichtautoriteit alle passende voorlopige maatregelen om het op haar nationale markt aanbieden van dat product te verbieden of te beperken, dan wel het product in de betrokken lidstaat uit de handel te nemen of terug te roepen.

   Die autoriteit brengt de Commissie en de andere lidstaten onverwijld van deze maatregelen op de hoogte.

5. De in lid 4 bedoelde informatie omvat alle beschikbare bijzonderheden, met name de gegevens die nodig zijn om de non-conforme producten met digitale elementen te identificeren, de oorsprong van het product met digitale elementen, de aard van de beweerde non-conformiteit en van het risico, en de aard en de duur van de genomen

nationale maatregelen, evenals de argumenten die worden aangevoerd door de desbetreffende marktdeelnemer. De markttoezichtautoriteit vermeldt met name of de non-conformiteit een of meer van de volgende redenen heeft:

(a) het product of de door de fabrikant ingestelde processen voldoen niet aan de essentiële eisen van bijlage I;

(b) tekortkomingen in de in artikel 18 bedoelde geharmoniseerde normen, cyberbeveiligingscertificeringsregelingen of gemeenschappelijke specificaties.

6. De andere markttoezichtautoriteiten van de lidstaten dan de markttoezichtautoriteit van de lidstaat die de procedure in gang heeft gezet, brengen de Commissie en de andere lidstaten onverwijld op de hoogte van door hen genomen maatregelen en van aanvullende informatie over de non-conformiteit van het betrokken product waarover zij beschikken, en van hun bezwaren indien zij het niet eens zijn met de aangemelde nationale maatregel.

7. Indien binnen drie maanden na ontvangst van de in lid 4 bedoelde informatie door een lidstaat of de Commissie geen bezwaar tegen een voorlopige maatregel van een lidstaat is ingediend, wordt die maatregel geacht gerechtvaardigd te zijn. Dit doet geen afbreuk aan de procedurele rechten van de betrokken marktdeelnemer overeenkomstig artikel 18 van Verordening (EU) 2019/1020.

8. De markttoezichtautoriteiten van alle lidstaten zorgen ervoor dat ten aanzien van het betrokken product onverwijld de passende beperkende maatregelen worden genomen, zoals het uit de handel nemen van het product op hun markt.

Artikel 44

Vrijwaringsprocedure van de Unie

1. Indien een lidstaat binnen drie maanden na ontvangst van de in artikel 43, lid 4, bedoelde kennisgeving bezwaar maakt tegen een door een andere lidstaat genomen maatregel of wanneer de Commissie de maatregel in strijd acht met de wetgeving van de Unie, treedt de Commissie onverwijld in overleg met de betrokken lidstaat en de marktdeelnemers en evalueert zij de nationale maatregel. Op grond van de resultaten van die evaluatie besluit de Commissie binnen negen maanden na ontvangst van de in artikel 43, lid 4, bedoelde kennisgeving of de nationale maatregel al dan niet gerechtvaardigd is en stelt zij de betrokken lidstaat in kennis van dat besluit.

2. Indien de nationale maatregel gerechtvaardigd wordt geacht, nemen alle lidstaten de nodige maatregelen om het non-conforme product met digitale elementen uit de handel te nemen en stellen zij de Commissie daarvan in kennis. Indien de nationale maatregel niet gerechtvaardigd wordt geacht, trekt de betrokken lidstaat de maatregel in.

3. Indien de nationale maatregel gerechtvaardigd wordt geacht en de non-conformiteit van het product met digitale elementen wordt toegeschreven aan tekortkomingen in de geharmoniseerde normen, past de Commissie de procedure van artikel 10 van Verordening (EU) nr. 1025/2012 toe.

4. Indien de nationale maatregel gerechtvaardigd wordt geacht en de non-conformiteit van het product met digitale elementen wordt toegeschreven aan tekortkomingen in een Europese cyberbeveiligingscertificeringsregeling als bedoeld in artikel 18, onderzoekt de Commissie of de uitvoeringshandeling als bedoeld in artikel 18, lid 4,

die het vermoeden van conformiteit met betrekking tot die certificeringsregeling specificeert, moet worden gewijzigd of ingetrokken.

5. Indien de nationale maatregel gerechtvaardigd wordt geacht en de non-conformiteit van het product met digitale elementen wordt toegeschreven aan tekortkomingen in de gemeenschappelijke specificaties als bedoeld in artikel 19, onderzoekt de Commissie of de in artikel 19 bedoelde uitvoeringshandeling tot vaststelling van die gemeenschappelijke specificaties moet worden gewijzigd of ingetrokken.

Artikel 45

Procedure op EU-niveau voor producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden

1. Indien de Commissie voldoende redenen heeft om, onder meer op basis van door Enisa verstrekte informatie, aan te nemen dat een product met digitale elementen dat een significant cyberbeveiligingsrisico inhoudt, niet in overeenstemming is met de eisen van deze verordening, kan zij de betrokken markttoezichtautoriteiten verzoeken een conformiteitsbeoordeling uit te voeren en de in artikel 43 bedoelde procedures te volgen.

2. In uitzonderlijke omstandigheden die een onmiddellijk optreden rechtvaardigen om de goede werking van de interne markt te vrijwaren, en wanneer de Commissie voldoende redenen heeft om aan te nemen dat het in lid 1 bedoelde product nog steeds niet aan de eisen van deze verordening voldoet en de betrokken markttoezichtautoriteiten geen doeltreffende maatregelen hebben genomen, kan de Commissie Enisa verzoeken een conformiteitsbeoordeling uit te voeren. De Commissie stelt de betrokken markttoezichtautoriteiten daarvan in kennis. De desbetreffende marktdeelnemers werken zo nodig samen met Enisa.

3. Op basis van de beoordeling van Enisa kan de Commissie besluiten dat een corrigerende of beperkende maatregel op het niveau van de Unie noodzakelijk is. Daartoe raadpleegt zij onverwijld de betrokken lidstaten en marktdeelnemers.

4. Op basis van het in lid 3 bedoelde overleg kan de Commissie uitvoeringshandelingen vaststellen om te besluiten tot corrigerende of beperkende maatregelen op het niveau van de Unie, onder meer door te gelasten om binnen een redelijke termijn in verhouding tot de aard van het risico producten uit de handel te nemen of terug te roepen. Die uitvoeringshandelingen worden overeenkomstig de in artikel 51, lid 2, bedoelde onderzoeksprocedure vastgesteld.

5. De Commissie stelt de betrokken marktdeelnemers onmiddellijk in kennis van het in lid 4 bedoelde besluit. De lidstaten voeren de in lid 4 bedoelde handelingen onverwijld uit en stellen de Commissie daarvan in kennis.

6. De leden 2 tot en met 5 zijn van toepassing voor de duur van de uitzonderlijke situatie die het optreden van de Commissie rechtvaardigde en zolang het betrokken product niet in overeenstemming is gebracht met deze verordening.

Artikel 46

Conforme producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden

1. Wanneer de markttoezichtautoriteit van een lidstaat na uitvoering van een evaluatie overeenkomstig artikel 43 vaststelt dat, hoewel een product met digitale elementen

en de door de fabrikant ingestelde processen in overeenstemming zijn met deze verordening, zij een significant cyberbeveiligingsrisico inhouden en bovendien een risico vormen voor de gezondheid of veiligheid van personen, voor de naleving van verplichtingen uit hoofde van het Unierecht of het interne recht ter bescherming van de grondrechten, de beschikbaarheid, de authenticiteit, de integriteit of de vertrouwelijkheid van diensten die via een elektronisch informatiesysteem worden aangeboden door essentiële entiteiten van het type als bedoeld in [bijlage I bij Richtlijn XXX/XXXX (NIS2)] of voor andere aspecten van de bescherming van het algemeen belang, verlangt zij van de betrokken marktdeelnemer dat hij alle passende maatregelen neemt om ervoor te zorgen dat het product met digitale elementen en de door de betrokken fabrikant ingestelde processen, wanneer het product in de handel wordt gebracht, dat risico niet meer inhouden, of dat het product met digitale elementen uit de handel wordt genomen of wordt teruggeroepen binnen een redelijke termijn, die evenredig is met de aard van het risico.

2. De fabrikant of andere betrokken marktdeelnemers zorgen ervoor dat binnen de door de markttoezichtautoriteit van de lidstaat vastgestelde termijn als bedoeld in lid 1, corrigerende maatregelen worden genomen ten aanzien van de betrokken producten met digitale elementen die zij in de Unie op de markt hebben aangeboden.

3. De lidstaat stelt de Commissie en de andere lidstaten onmiddellijk in kennis van de overeenkomstig lid 1 genomen maatregelen. Die informatie omvat alle bekende bijzonderheden, met name de gegevens die nodig zijn om de betrokken producten met digitale elementen te identificeren, alsook de oorsprong en de toeleveringsketen van die producten met digitale elementen, de aard van het risico en de aard en de duur van de nationale maatregelen.

4. De Commissie treedt onverwijld in overleg met de lidstaten en de betrokken marktdeelnemer en beoordeelt de genomen nationale maatregelen. Aan de hand van die beoordeling besluit de Commissie of de maatregel al dan niet gerechtvaardigd is, en stelt zij zo nodig passende maatregelen voor.

5. De Commissie deelt haar besluit aan de lidstaten mee.

6. Indien de Commissie voldoende redenen heeft om, onder meer op basis van door Enisa verstrekte informatie, aan te nemen dat een product met digitale elementen, hoewel het in overeenstemming is met deze verordening, de in lid 1 bedoelde risico's inhoudt, kan zij de betrokken markttoezichtautoriteiten verzoeken een conformiteitsbeoordeling uit te voeren en de in artikel 43 en de leden 1, 2 en 3 van dit artikel bedoelde procedures te volgen.

7. In uitzonderlijke omstandigheden die een onmiddellijk optreden rechtvaardigen om de goede werking van de interne markt te vrijwaren, en wanneer de Commissie voldoende redenen heeft om aan te nemen dat het in lid 6 bedoelde product nog steeds de in lid 1 bedoelde risico's inhoudt en de betrokken nationale markttoezichtautoriteiten geen doeltreffende maatregelen hebben genomen, kan de Commissie Enisa verzoeken een beoordeling uit te voeren van de risico's die dat product inhoudt en stelt zij de betrokken markttoezichtautoriteiten daarvan in kennis. De desbetreffende marktdeelnemers werken zo nodig samen met Enisa.

8. Op basis van de in lid 7 bedoelde beoordeling van Enisa kan de Commissie vaststellen dat een corrigerende of beperkende maatregel op het niveau van de Unie noodzakelijk is. Daartoe raadpleegt zij onverwijld de betrokken lidstaten en marktdeelnemers.

9. Op basis van het in lid 8 bedoelde overleg kan de Commissie uitvoeringshandelingen vaststellen om te besluiten tot corrigerende of beperkende maatregelen op het niveau van de Unie, onder meer door te gelasten om binnen een redelijke termijn in verhouding tot de aard van het risico producten uit de handel te nemen of terug te roepen. Die uitvoeringshandelingen worden overeenkomstig de in artikel 51, lid 2, bedoelde onderzoeksprocedure vastgesteld.

10. De Commissie stelt de betrokken marktdeelnemers onmiddellijk in kennis van het in lid 9 bedoelde besluit. De lidstaten voeren zulke handelingen onverwijld uit en stellen de Commissie daarvan in kennis.

11. De leden 6 tot en met 10 zijn van toepassing voor de duur van de uitzonderlijke situatie die het optreden van de Commissie rechtvaardigde en zolang het betrokken product de in lid 1 bedoelde risico's inhoudt.

Artikel 47

Formele non-conformiteit

1. Indien de markttoezichtautoriteit van een lidstaat een van de volgende feiten vaststelt, verlangt zij van de betrokken fabrikant dat deze een einde maakt aan de non-conformiteit:

   (a) de conformiteitsmarkering is in strijd met artikel 21 en artikel 22 aangebracht;

   (b) de conformiteitsmarkering is niet aangebracht;

   (c) de EU-conformiteitsverklaring is niet opgesteld;

   (d) de EU-conformiteitsverklaring is niet correct opgesteld;

   (e) het identificatienummer van de aangemelde instantie, die betrokken is bij de conformiteitsbeoordelingsprocedure, in voorkomend geval, is niet aangebracht;

   (f) de technische documentatie is niet beschikbaar of onvolledig.

2. Indien de in lid 1 bedoelde non-conformiteit voortduurt, neemt de betrokken lidstaat alle passende maatregelen om het op de markt aanbieden van het product met digitale elementen te beperken of te verbieden, of het product terug te roepen of uit de handel te nemen.

Artikel 48

Gezamenlijke activiteiten van markttoezichtautoriteiten

1. Markttoezichtautoriteiten kunnen met andere betrokken autoriteiten overeenkomen gezamenlijke activiteiten uit te voeren die gericht zijn op het waarborgen van cyberbeveiliging en consumentenbescherming met betrekking tot specifieke producten met digitale elementen die in de handel worden gebracht of op de markt worden aangeboden, met name producten waarvan vaak wordt vastgesteld dat zij cyberbeveiligingsrisico's inhouden.

2. De Commissie of Enisa kan gezamenlijke activiteiten inzake toezicht op de naleving van deze verordening voorstellen, te verrichten door markttoezichtautoriteiten op basis van indicaties of informatie dat binnen het toepassingsgebied van deze verordening vallende producten in verschillende lidstaten mogelijk niet in overeenstemming zijn met de eisen van deze verordening.

3. De markttoezichtautoriteiten en, in voorkomend geval, de Commissie zorgen ervoor dat de afspraak om gezamenlijke activiteiten uit te voeren niet leidt tot oneerlijke concurrentie tussen marktdeelnemers en geen negatieve gevolgen heeft voor de objectiviteit, onafhankelijkheid en onpartijdigheid van de partijen bij de overeenkomst.

4. Een markttoezichtautoriteit kan alle informatie gebruiken die voortvloeit uit de activiteiten die zij verricht in het kader van een door haar uitgevoerd onderzoek.

5. De betrokken markttoezichtautoriteit en de Commissie, indien van toepassing, stellen de afspraak over gezamenlijke activiteiten, met inbegrip van de namen van de betrokken partijen, ter beschikking van het publiek.

Artikel 49

Bezemacties

1. Markttoezichtautoriteiten kunnen besluiten gelijktijdige gecoördineerde controleacties (“bezemacties”) uit te voeren voor bepaalde producten met digitale elementen of categorieën daarvan om de naleving van deze verordening te controleren of inbreuken op deze verordening op te sporen.

2. Tenzij de betrokken markttoezichtautoriteiten anders overeenkomen, worden bezemacties gecoördineerd door de Commissie. De coördinator van de bezemactie kan de geaggregeerde resultaten in voorkomend geval openbaar maken.

3. Enisa kan bij de uitvoering van zijn taken, onder meer op basis van de overeenkomstig artikel 11, leden 1 en 2, ontvangen kennisgevingen, categorieën producten aanwijzen waarvoor bezemacties kunnen worden georganiseerd. Het voorstel voor bezemacties wordt aan de in lid 2 bedoelde potentiële coördinator voorgelegd ter overweging door de markttoezichtautoriteiten.

4. Bij het uitvoeren van bezemacties kunnen de betrokken markttoezichtautoriteiten gebruikmaken van de onderzoeksbevoegdheden als bedoeld in de artikelen 41 tot en met 47 en van alle andere bevoegdheden die hun bij het interne recht zijn verleend.

5. Markttoezichtautoriteiten kunnen ambtenaren van de Commissie en andere begeleidende personen die door de Commissie zijn gemachtigd, uitnodigen om deel te nemen aan bezemacties.

HOOFDSTUK VI

BEVOEGDHEIDSDELEGATIE EN COMITÉPROCEDURE

Artikel 50

Uitoefening van de delegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De in artikel 2, lid 4, artikel 6, lid 2, artikel 6, lid 3, artikel 6, lid 5, artikel 20, lid 5, en artikel 23, lid 5, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen wordt toegekend aan de Commissie.

3. Het Europees Parlement of de Raad kan de in artikel 2, lid 4, artikel 6, lid 2, artikel 6, lid 3, artikel 6, lid 5, artikel 20, lid 5, en artikel 23, lid 5, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Een besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het besluit wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het besluit laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven.

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, geeft zij daarvan gelijktijdig kennis aan het Europees Parlement en de Raad.

6. Een overeenkomstig artikel 2, lid 4, artikel 6, lid 2, artikel 6, lid 3, artikel 6, lid 5, artikel 20, lid 5, en artikel 23, lid 5, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad vóór het verstrijken van die termijn de Commissie hebben meegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of van de Raad met twee maanden verlengd.

Artikel 51

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dit comité is een comité in de zin van Verordening (EU) nr. 182/2011.

2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

3. Wanneer het advies van het comité via een schriftelijke procedure dient te worden verkregen, wordt die procedure zonder gevolg beëindigd indien, binnen de termijn voor het uitbrengen van het advies, de voorzitter van het comité daartoe besluit of een lid van het comité daarom verzoekt.

HOOFDSTUK VII

VERTROUWELIJKHEID EN SANCTIES

Artikel 52

Vertrouwelijkheid

1. Alle partijen die betrokken zijn bij de toepassing van deze verordening, eerbiedigen de vertrouwelijke aard van informatie en gegevens die zij hebben verkregen tijdens het uitvoeren van hun taken en activiteiten met het oog op de bescherming van:

   (a) intellectuele-eigendomsrechten, en vertrouwelijke bedrijfsinformatie of bedrijfsgeheimen van een natuurlijke of rechtspersoon, met inbegrip van

broncode, uitgezonderd de in artikel 5 van Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad[24] genoemde gevallen;

(b) de doeltreffende uitvoering van deze verordening, met name de uitvoering van inspecties, onderzoeken of audits;

(c) openbare en nationale veiligheidsbelangen;

(d) de integriteit van strafrechtelijke of bestuursrechtelijke procedures.

2. Onverminderd lid 1 wordt informatie die op vertrouwelijke basis tussen de markttoezichtautoriteiten onderling en tussen de markttoezichtautoriteiten en de Commissie wordt uitgewisseld, niet openbaar gemaakt zonder voorafgaande toestemming van de markttoezichtautoriteit van oorsprong.

3. De leden 1 en 2 doen geen afbreuk aan de rechten en verplichtingen van de Commissie, de lidstaten en de aangemelde instanties met betrekking tot de uitwisseling van informatie en de verspreiding van waarschuwingen, alsook de verplichtingen van de betrokken personen om in het kader van het strafrecht van de lidstaten informatie te verstrekken.

4. De Commissie en de lidstaten kunnen indien nodig gevoelige informatie uitwisselen met regelgevingsinstanties van derde landen waarmee zij bilaterale of multilaterale geheimhoudingsovereenkomsten hebben gesloten die een passend beschermingsniveau waarborgen.

Artikel 53

Sancties

1. De lidstaten stellen de regels vast voor de sancties die van toepassing zijn op inbreuken van marktdeelnemers op deze verordening, en nemen alle maatregelen om te waarborgen dat zij worden gehandhaafd. De sancties zijn doeltreffend, evenredig en afschrikkend.

2. De lidstaten stellen de Commissie onverwijld van die regels en maatregelen in kennis en delen haar onverwijld alle latere wijzigingen daarvan mee.

3. De niet-naleving van de in bijlage I vastgestelde essentiële cyberbeveiligingsvereisten en de in de artikelen 10 en 11 vastgestelde verplichtingen wordt bestraft met administratieve geldboeten tot 15 000 000 EUR of, als de overtreder een onderneming is, tot 2,5 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, als dat hoger is.

4. De niet-naleving van andere verplichtingen uit hoofde van deze verordening wordt bestraft met administratieve geldboeten tot 10 000 000 EUR of, als de overtreder een onderneming is, tot 2 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, als dat hoger is.

5. Voor het verstrekken van onjuiste, onvolledige of misleidende informatie aan aangemelde instanties en markttoezichtautoriteiten in antwoord op een verzoek, worden administratieve geldboeten opgelegd tot 5 000 000 EUR of, als de overtreder

[24] Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan (PB L 157 van 15.6.2016, blz. 1).

een onderneming is, tot 1 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, als dat hoger is.

6. Bij het bepalen van het bedrag van de administratieve geldboete per geval worden alle relevante omstandigheden van de specifieke situatie in aanmerking genomen en wordt terdege rekening gehouden met het volgende:

   (a) de aard, ernst en duur van de inbreuk en de gevolgen ervan;

   (b) of administratieve geldboeten reeds door andere markttoezichtautoriteiten voor een soortgelijke inbreuk op dezelfde marktdeelnemer zijn toegepast;

   (c) de omvang en het marktaandeel van de marktdeelnemer die de inbreuk pleegt.

7. Markttoezichtautoriteiten die administratieve geldboeten opleggen, delen deze informatie met de markttoezichtautoriteiten van andere lidstaten via het in artikel 34 van Verordening (EU) 2019/1020 bedoelde informatie- en communicatiesysteem.

8. Elke lidstaat stelt regels vast betreffende de vraag of en in hoeverre administratieve geldboeten kunnen worden opgelegd aan in die lidstaat gevestigde overheidsinstanties en -organen.

9. Afhankelijk van het rechtsstelsel van de lidstaten kunnen de regels voor administratieve geldboeten zodanig worden toegepast dat de boeten worden opgelegd door bevoegde nationale rechtbanken of andere instanties, overeenkomstig de bevoegdheden die op nationaal niveau in die lidstaten zijn vastgesteld. De toepassing van zulke regels in die lidstaten heeft een gelijkwaardig effect.

10. Naargelang van de omstandigheden van elk afzonderlijk geval kunnen administratieve geldboeten worden opgelegd naast eventuele andere corrigerende of beperkende maatregelen die de markttoezichtautoriteiten voor dezelfde inbreuk toepassen.

HOOFDSTUK VIII

OVERGANGS- EN SLOTBEPALINGEN

Artikel 54

Wijziging van Verordening (EU) 2019/1020

Aan bijlage I bij Verordening (EU) 2019/1020 wordt het volgende punt toegevoegd:

“71. [Verordening XXX] [verordening cyberweerbaarheid]”.

Artikel 55

Overgangsbepalingen

1. Certificaten van EU-typeonderzoek en goedkeuringsbesluiten die zijn afgegeven met betrekking tot cyberbeveiligingsvereisten voor onder andere harmonisatiewetgeving van de Unie vallende producten met digitale elementen, blijven geldig tot [42 maanden na de datum van inwerkingtreding van deze verordening], tenzij zij vóór die datum vervallen, of tenzij anders bepaald in andere wetgeving van de Unie, in welk geval zij geldig blijven als bedoeld in die wetgeving van de Unie.

2. Voor producten met digitale elementen die vóór [de in artikel 57 bedoelde datum van toepassing van deze verordening] in de handel zijn gebracht, gelden de eisen van deze verordening alleen indien het ontwerp of het beoogde doel van die producten vanaf die datum ingrijpend worden gewijzigd.

3. In afwijking van lid 2 zijn de in artikel 11 vastgestelde verplichtingen van toepassing op alle producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen en die vóór [de in artikel 57 bedoelde datum van toepassing van deze verordening] in de handel zijn gebracht.

Artikel 56

Evaluatie en toetsing

Uiterlijk [36 maanden na de datum van toepassing van deze verordening] en vervolgens om de vier jaar dient de Commissie bij het Europees Parlement en de Raad een verslag in over de evaluatie en de toetsing van deze verordening. De verslagen worden openbaar gemaakt.

Artikel 57

Inwerkingtreding en toepassing

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is van toepassing met ingang van [24 maanden na de datum van de inwerkingtreding van deze verordening]. Artikel 11 is evenwel van toepassing vanaf [12 maanden na de datum van de inwerkingtreding van deze verordening].

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

1.2. Betrokken beleidsterrein(en)

1.3. Het voorstel/initiatief betreft:

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

1.4.2. Specifieke doelstelling(en)

1.4.3. Verwachte resulta(a)t(en) en gevolg(en)

1.4.4. Prestatie-indicatoren

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief

1.5.2. Toegevoegde waarde van de betrokkenheid van de Unie (deze kan het resultaat zijn van verschillende factoren, bv. coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder "toegevoegde waarde van de betrokkenheid van de Unie" verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die zou zijn gecreëerd indien alleen de lidstaat een maatregel had getroffen.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

1.5.4. Verenigbaarheid met het meerjarige financiële kader en eventuele synergie met andere passende instrumenten

1.5.5. Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking

1.6. Duur en financiële gevolgen van het voorstel/initiatief

1.7. Geplande beheersvorm(en)

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

2.2. Beheers- en controlesyste(e)m(en)

2.2.1. Rechtvaardiging van de voorgestelde beheersvorm(en), uitvoeringsmechanisme(n) voor financiering, betalingsvoorwaarden en controlestrategie

2.2.2. Informatie over de geïdentificeerde risico's en het (de) systeem (systemen) voor interne controle dat is (die zijn) opgezet om die risico's te beperken

2.2.3. Raming en motivering van de kosteneffectiviteit van de controles (verhouding van de controlekosten tot de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting)

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

3.2. Geraamde financiële gevolgen van het voorstel inzake kredieten

3.2.1. Samenvatting van de geraamde gevolgen voor de beleidskredieten

3.2.2. Geraamde output, gefinancierd met beleidskredieten

3.2.3. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

3.2.4. Verenigbaarheid met het huidige meerjarige financiële kader

3.2.5. Bijdragen van derden

3.3. Geraamde gevolgen voor de ontvangsten

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen (verordening cyberweerbaarheid)

1.2. Betrokken beleidsterrein(en)

Communicatienetwerken, inhoud en technologie

1.3. Het voorstel/initiatief betreft:

× **een nieuwe actie**

☐ **een nieuwe actie na een proefproject/een voorbereidende actie**[37]

☐ **de verlenging van een bestaande actie**

☐ **de samenvoeging of ombuiging van een of meer acties naar een andere/een nieuwe actie**

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

Het voorstel heeft twee hoofddoelstellingen om de goede werking van de interne markt te waarborgen: 1) **voorwaarden scheppen voor de ontwikkeling van veilige producten met digitale elementen** door ervoor te zorgen dat hardware- en softwareproducten met minder kwetsbaarheden in de handel worden gebracht en dat fabrikanten de veiligheid gedurende de hele levenscyclus van een product serieus nemen; en 2) **voorwaarden scheppen die gebruikers in staat stellen rekening te houden met cyberbeveiliging bij het selecteren en gebruiken van producten met digitale elementen**.

1.4.2. Specifieke doelstelling(en)

Er werden **vier specifieke doelstellingen** voor het voorstel geformuleerd: i) ervoor zorgen dat fabrikanten de beveiliging van producten met digitale elementen verbeteren vanaf de ontwerp- en ontwikkelingsfase en gedurende de gehele levenscyclus; ii) zorgen voor een samenhangend cyberbeveiligingskader, waardoor de naleving voor hardware- en softwarefabrikanten wordt vergemakkelijkt; iii) de beveiligingskenmerken van producten met digitale elementen transparanter maken, en iv) bedrijven en consumenten in staat stellen producten met digitale elementen veilig te gebruiken.

Verwachte resulta(a)t(en) en gevolg(en)

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben op de begunstigden/doelgroepen

Het voorstel zou aanzienlijke voordelen opleveren voor de verschillende belanghebbenden. Voor bedrijven zouden uiteenlopende beveiligingsregels voor producten met digitale elementen worden voorkomen en zouden de nalevingskosten

[37] In de zin van artikel 58, lid 2, punt a) of b), van het Financieel Reglement.

op het gebied van de betrokken cyberbeveiligingswetgeving dalen. Het aantal cyberincidenten, de kosten voor incidentenbehandeling en de reputatieschade zouden worden beperkt. Voor de hele EU kan het initiatief naar schatting leiden tot een kostenvermindering met ongeveer 180 miljard tot 290 miljard EUR per jaar[38] als gevolg van incidenten die bedrijven treffen. Dit zou leiden tot een hogere omzet als gevolg van de vraag naar producten met digitale elementen. Het zou de wereldwijde reputatie van bedrijven verbeteren, waardoor ook de vraag van buiten de EU zou stijgen. Voor gebruikers zou de voorkeursoptie de transparantie van de beveiligingseigenschappen vergroten en het gebruik van producten met digitale elementen vergemakkelijken. Consumenten en burgers zouden ook een betere bescherming genieten van hun grondrechten, zoals privacy en gegevensbescherming.

Tegelijkertijd zou het voorstel leiden tot hogere nalevings- en handhavingskosten voor bedrijven, aangemelde instanties en overheidsinstanties, met inbegrip van accreditatie- en markttoezichtautoriteiten. Voor softwareontwikkelaars en hardwarefabrikanten zal dit directe nalevingskosten met zich meebrengen voor nieuwe beveiligingseisen, conformiteitsbeoordelings-, documentatie- en rapportageverplichtingen, waardoor de totale nalevingskosten oplopen tot ongeveer 29 miljard EUR bij een geraamde marktwaarde van 1 485 miljard EUR aan omzet[39]. Gebruikers, met inbegrip van zakelijke gebruikers, consumenten en burgers, kunnen worden geconfronteerd met hogere prijzen van producten met digitale elementen. Zij moeten echter worden gezien tegen de achtergrond van de aanzienlijke voordelen zoals hierboven beschreven.

1.4.3. Prestatie-indicatoren

Specificeer de indicatoren voor het monitoren van de voortgang en de verwezenlijkingen.

Om na te gaan of fabrikanten de beveiliging van hun producten met digitale elementen verbeteren vanaf de ontwerp- en ontwikkelingsfase en gedurende de gehele levenscyclus van die producten, kunnen verschillende indicatoren in aanmerking worden genomen. Het kan hierbij gaan om het aantal significante incidenten in de Unie als gevolg van kwetsbaarheden, het aandeel van hardware- en softwarefabrikanten dat een systematische veilige ontwikkelingscyclus volgt, een kwalitatieve analyse van de beveiliging van producten met digitale elementen, een kwantitatieve en kwalitatieve beoordeling van kwetsbaarheidsdatabases, de frequentie van de door fabrikanten beschikbaar gestelde beveiligingspatches of het gemiddelde aantal dagen tussen het opsporen van kwetsbaarheden en het aanbieden van beveiligingspatches.

Een indicator voor een samenhangend cyberbeveiligingskader zou het ontbreken van gerichte productspecifieke nationale cyberbeveiligingswetgeving kunnen zijn.

Een indicator voor een grotere transparantie met betrekking tot de beveiligingseigenschappen van producten met digitale elementen zou het aandeel producten met digitale elementen kunnen zijn dat wordt verzonden met informatie over beveiligingseigenschappen. Bovendien kan het aandeel producten met digitale elementen dat met een gebruiksaanwijzing voor veilig gebruik wordt geleverd,

[38] Zie [werkdocument van de diensten van de Commissie over de effectbeoordeling bij de verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen].

[39] Zie [werkdocument van de diensten van de Commissie over de effectbeoordeling bij de verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen].

worden gebruikt als indicator voor de vraag of organisaties en consumenten in staat zijn producten met digitale elementen veilig te gebruiken.

Wat het toezicht op het effect van de verordening betreft, zouden voor dit doel bepaalde indicatoren in aanmerking worden genomen, die door de Commissie moeten worden beoordeeld, in voorkomend geval met de steun van Enisa. Afhankelijk van de te verwezenlijken operationele doelstelling zijn enkele van de monitoringindicatoren op basis waarvan het succes van de horizontale cyberbeveiligingsvereisten zou worden beoordeeld, als volgt:

Voor het beoordelen van het cyberbeveiligingsniveau van producten met digitale elementen:

– Statistieken en kwalitatieve analyses van incidenten met producten met digitale elementen en de manier waarop hiermee werd omgegaan. Deze kunnen worden verzameld en beoordeeld door de Commissie, met steun van Enisa.

– Registers van bekende kwetsbaarheden en analyses van de wijze waarop deze zijn aangepakt. Een dergelijke analyse kan worden uitgevoerd door Enisa, op basis van de Europese kwetsbaarheidsdatabase die is opgezet op basis van [Richtlijn XXX/XXXX (NIS2)].

– Enquêtes onder fabrikanten van hardware en software om de vooruitgang te monitoren.

Voor het beoordelen van het niveau van informatie over beveiligingskenmerken, beveiligingsondersteuning, het einde van de levensduur en de zorgplicht: resultaten van door de Commissie, met steun van Enisa, uit te voeren enquêtes voor zowel gebruikers als bedrijven.

Bij de beoordeling van de uitvoering streeft de Commissie ernaar te waarborgen dat de conformiteitsbeoordelingen daadwerkelijk worden uitgevoerd. Daartoe zal een normalisatieverzoek worden ingediend en zal de uitvoering ervan worden gevolgd. De Commissie zal ook de capaciteit van de aangemelde instanties en, indien van toepassing, van de certificerende instanties controleren.

Wat de toepassing betreft, zal de Commissie door middel van de verslagen van de lidstaten nagaan of de nationale initiatieven geen betrekking hebben op aspecten die onder de verordening vallen.

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief

De verordening moet 24 maanden na de inwerkingtreding ervan volledig van toepassing zijn. Elementen van de governancestructuur moeten echter eerder zijn ingevoerd. Met name hebben de lidstaten bestaande autoriteiten aangewezen en/of nieuwe autoriteiten opgericht die de in de wetgeving gestelde taken vervullen.

1.5.2. Toegevoegde waarde van de betrokkenheid van de Unie (deze kan het resultaat zijn van verschillende factoren, bv. coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder "toegevoegde waarde van de betrokkenheid van de Unie" verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die zou zijn gecreëerd indien alleen de lidstaat een maatregel had getroffen.

De sterke grensoverschrijdende aard van cyberbeveiliging en de toenemende incidenten met spillover-effecten over grenzen, sectoren en producten heen betekenen dat de doelstellingen niet doeltreffend door de lidstaten afzonderlijk kunnen worden verwezenlijkt. Gezien het mondiale karakter van markten voor producten met digitale elementen, lopen de lidstaten dezelfde risico's voor hetzelfde product met digitale elementen op hun grondgebied. Een opkomend versnipperd kader van potentieel uiteenlopende nationale voorschriften dreigt een open en concurrerende eengemaakte markt voor producten met digitale elementen in de weg te staan. Een gezamenlijk optreden op EU-niveau is dan ook noodzakelijk om een hoog niveau van vertrouwen onder de gebruikers tot stand te brengen en de aantrekkelijkheid van EU-producten met digitale elementen te vergroten. Het zou ook de interne markt ten goede komen door rechtszekerheid te bieden en een gelijk speelveld tot stand te brengen voor verkopers van producten met digitale elementen.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

De verordening cyberweerbaarheid is de eerste verordening in haar soort en introduceert cyberbeveiligingsvereisten voor het in de handel brengen van producten met digitale elementen. Zij bouwt echter voort op de opzet van het nieuwe wetgevingskader en de lessen die zijn getrokken uit het uitvoeringsproces van de bestaande harmonisatiewetgeving van de Unie voor verschillende producten, met name wat betreft de voorbereiding op de uitvoering, met inbegrip van aspecten zoals de opstelling van geharmoniseerde normen.

1.5.4. Verenigbaarheid met het meerjarige financiële kader en eventuele synergie met andere passende instrumenten

In de verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen worden nieuwe cyberbeveiligingsvereisten vastgesteld voor alle producten met digitale elementen die in de EU in de handel worden gebracht, die verder gaan dan de eisen waarin de bestaande wetgeving voorziet. Tegelijkertijd bouwt het voorstel voort op het bestaande kader van de NWK-wetgeving. Daarom zou het voortbouwen op bestaande NWK-structuren en -procedures, zoals de samenwerking tussen aangemelde instanties en markttoezicht, conformiteitsbeoordelingsmodules en de ontwikkeling van geharmoniseerde normen. Het nieuwe voorstel zou ook steunen op bepaalde structuren die zijn ontwikkeld overeenkomstig andere cyberbeveiligingswetgeving, zoals Richtlijn (EU) 2016/1148 (NIS-richtlijn), respectievelijk [Richtlijn XXX/XXXX (NIS2)] of Verordening (EU) 2019/881 (de cyberbeveiligingsverordening).

1.5.5. Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking

Het beheer van de aan Enisa toegewezen actiegebieden sluit aan bij het bestaande mandaat en de algemene taken. Voor deze actiegebieden kunnen specifieke profielen of nieuwe opdrachten nodig zijn, maar deze zouden niet opvallend zijn en kunnen worden opgevangen door de bestaande middelen van Enisa, en kunnen worden

opgelost door middel van hertoewijzing of koppeling van verschillende opdrachten. Een van de belangrijkste actiegebieden die aan Enisa zijn toegewezen, betreft bijvoorbeeld het verzamelen en verwerken van kennisgevingen van fabrikanten over uitgebuite kwetsbaarheden van producten. Bij [Richtlijn XXX/XXXX (NIS2)] heeft Enisa reeds de opdracht gekregen een Europese kwetsbaarheidsdatabase op te zetten waarin algemeen bekende kwetsbaarheden op vrijwillige basis openbaar kunnen worden gemaakt en geregistreerd, zodat gebruikers passende risicobeperkende maatregelen kunnen nemen. De daartoe toegewezen middelen kunnen ook worden gebruikt voor de nieuwe bovengenoemde opdrachten in verband met kennisgevingen van kwetsbaarheden van producten. Dat kan zorgen voor een doeltreffend gebruik van de bestaande middelen en zou ook de nodige synergieën tussen dergelijke opdrachten creëren die de analyses van Enisa van cyberbeveiligingsrisico's en -dreigingen beter kunnen onderbouwen.

1.6. Duur en financiële gevolgen van het voorstel/initiatief

☐ **beperkte geldigheidsduur**

– ☐ van kracht vanaf [DD/MM]JJJJ tot en met [DD/MM]JJJJ;

– ☐ financiële gevolgen vanaf JJJJ tot en met JJJJ voor vastleggingskredieten en vanaf JJJJ tot en met JJJJ voor betalingskredieten;

× **onbeperkte geldigheidsduur;**

– uitvoering met een opstartperiode vanaf 2025;

– gevolgd door een volledige uitvoering.

1.7. Geplande beheersvorm(en)[40]

☐ **Direct beheer** door de Commissie

– × door haar diensten, waaronder het personeel in de delegaties van de Unie;

– ☐ door de uitvoerende agentschappen;

☐ **Gedeeld beheer** met de lidstaten

☐ **Indirect beheer** door begrotingsuitvoeringstaken te delegeren aan:

– ☐ derde landen of de door hen aangewezen organen;

– ☐ internationale organisaties en hun agentschappen (geef aan welke);

– ☐ de EIB en het Europees Investeringsfonds;

– ☐ de in de artikelen 70 en 71 van het Financieel Reglement bedoelde organen;

– ☐ publiekrechtelijke organen;

– ☐ privaatrechtelijke organen met een openbare dienstverleningstaak, voor zover zij voldoende financiële garanties bieden;

– ☐ privaatrechtelijke organen van een lidstaat, waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die voldoende financiële garanties bieden;

– ☐ personen aan wie de uitvoering van specifieke maatregelen op het gebied van het GBVB in het kader van titel V van het VEU is toevertrouwd en die worden genoemd in de betrokken basishandeling.

– *Verstrek, indien meer dan een beheersvorm is aangekruist, extra informatie onder "Opmerkingen".*

Opmerkingen

Bij deze verordening worden bepaalde acties toegewezen aan Enisa, in overeenstemming met zijn bestaande mandaat, en met name artikel 3, lid 2 van Verordening (EU) 2019/881, waarin is bepaald dat Enisa de taken moet verrichten die hem worden toegewezen bij rechtshandelingen van de Unie tot vaststelling van maatregelen voor de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die betrekking hebben op cyberbeveiliging. Enisa is met name belast met het ontvangen van kennisgevingen van fabrikanten van actief uitgebuite kwetsbaarheden in producten met digitale elementen, alsook

[40] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

van incidenten die gevolgen hebben voor de beveiliging van die producten. Enisa moet deze kennisgevingen ook doorsturen naar de betrokken CSIRT's of, respectievelijk, naar het desbetreffende centrale contactpunt dat is aangewezen overeenkomstig artikel [artikel X] van Richtlijn [Richtlijn XXX/XXXX (NIS2)] van de lidstaten, en moet de markttoezichtautoriteiten hier eveneens van in kennis stellen. Op basis van de informatie die het verzamelt, moet Enisa om de twee jaar een technisch verslag opstellen over opkomende trends met betrekking tot cyberbeveiligingsrisico's in producten met digitale elementen en dit verslag voorleggen aan de NIS-samenwerkingsgroep. Voorts kan Enisa, gezien zijn deskundigheid, verzamelde informatie en dreigingsanalyses, het uitvoeringsproces van deze verordening ondersteunen door gezamenlijke activiteiten voor te stellen die door nationale markttoezichtautoriteiten moeten worden uitgevoerd op basis van indicaties of informatie over mogelijke niet-naleving van deze verordening van producten met digitale elementen in verschillende lidstaten, of door categorieën producten aan te wijzen waarvoor gelijktijdige gecoördineerde controleacties kunnen worden georganiseerd. De Commissie kan Enisa verzoeken evaluaties te verrichten voor specifieke producten in uitzonderlijke omstandigheden met betrekking tot producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden en waarbij een onmiddellijk optreden nodig is om de goede werking van de interne markt te vrijwaren.

Voor al deze opdrachten zouden naar schatting ongeveer 4,5 vte uit de bestaande middelen van Enisa nodig zijn, voortbouwend op de expertise en de voorbereidende werkzaamheden die momenteel door Enisa worden verricht, onder meer ter ondersteuning van de komende uitvoering van [Richtlijn XXX/XXXX (NIS2)], waarvoor de middelen van Enisa zijn aangevuld.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld de frequentie en de voorwaarden.

Uiterlijk 36 maanden na de datum van toepassing van deze verordening en vervolgens om de vier jaar dient de Commissie bij het Europees Parlement en de Raad een verslag in over de evaluatie en de toetsing van deze verordening. De verslagen worden openbaar gemaakt.

2.2. Beheers- en controlesyste(e)m(en)

2.2.1. Rechtvaardiging van de voorgestelde beheersvorm(en), uitvoeringsmechanisme(n) voor financiering, betalingsvoorwaarden en controlestrategie

Bij deze verordening wordt een nieuw beleid vastgesteld met betrekking tot geharmoniseerde cyberbeveiligingsvereisten voor producten met digitale elementen die op de interne markt worden gebracht en die gelden voor hun gehele levenscyclus . De rechtshandeling zal worden gevolgd door verzoeken van de Commissie aan de Europese normalisatie-instellingen om normen te ontwikkelen.

Om deze nieuwe taken te kunnen oppakken, moeten de diensten van de Commissie over voldoende middelen beschikken. Voor de handhaving van de nieuwe verordening zullen naar schatting 7 vte (waarvan één END) de volgende taken moeten uitvoeren:

- voorbereiding van het normalisatieverzoek en/of gemeenschappelijke specificaties door middel van uitvoeringshandelingen indien niet met succes een normalisatieproces is afgerond;
- opstellen van een gedelegeerde handeling [binnen 12 maanden na de inwerkingtreding van de verordening] tot nadere bepaling van de definities van de kritieke producten met digitale elementen;
- mogelijke voorbereiding van gedelegeerde handelingen voor het bijwerken van de lijst van kritieke producten van klasse I en II; te specificeren of een beperking of uitsluiting noodzakelijk is voor producten met digitale elementen die worden gedekt door andere regels van de Unie tot vaststelling van eisen die hetzelfde beschermingsniveau bieden als deze verordening; de certificering verplicht te stellen van bepaalde zeer kritieke producten met digitale elementen op basis van de in deze verordening vastgestelde criteria; specificeren van de minimaal vereiste inhoud van de EU-conformiteitsverklaring en het aanvullen van de elementen die in de technische documentatie moeten worden opgenomen;
- mogelijke voorbereiding van uitvoeringshandelingen met betrekking tot het formaat of de elementen van de rapportageverplichtingen, de softwarestuklijst, gemeenschappelijke specificaties of het aanbrengen van de CE-markering;
- mogelijke voorbereiding van een onmiddellijk optreden voor het opleggen van corrigerende of beperkende maatregelen in uitzonderlijke omstandigheden om de goede werking van de interne markt te vrijwaren, met inbegrip van de voorbereiding van een uitvoeringshandeling;
- organisatie en coördinatie van de aanmeldingen door de lidstaten van aangemelde instanties en de coördinatie van de aangemelde instanties;

– ondersteuning van de coördinatie van de markttoezichtautoriteiten van de lidstaten.

2.2.2. Informatie over de geïdentificeerde risico's en het (de) systeem (systemen) voor interne controle dat is (die zijn) opgezet om die risico's te beperken

Om ervoor te zorgen dat aangemelde instanties en markttoezichtautoriteiten informatie uitwisselen en goed samenwerken, is de Commissie belast met de coördinatie. Voor de technische en marktexpertise wordt een deskundigengroep opgericht.

2.2.3. Raming en motivering van de kosteneffectiviteit van de controles (verhouding van de controlekosten tot de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting)

2.3. Voor de uitgaven voor vergaderingen lijken gezien de lage waarde per transactie (bv. terugbetaling van reiskosten voor een afgevaardigde voor een vergadering) standaardcontroleprocedures afdoende. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande of geplande preventie- en beveiligingsmaatregelen, bv. in het kader van de fraudebestrijdingsstrategie.

De voor deze verordening vereiste aanvullende kredieten zullen onder de bestaande fraudepreventiemaatregelen vallen die van toepassing zijn op de Commissie.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

- Bestaande begrotingsonderdelen

Schema

- Te creëren nieuwe begrotingsonderdelen

N.v.t.

3.2. Geraamde financiële gevolgen van het voorstel inzake kredieten

3.2.1. Samenvatting van de geraamde gevolgen voor de beleidskredieten

– ☑ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☐ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

in miljoen EUR (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	Nummer	

DG: <…….>			Jaar **N**[41]	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			**TOTAAL**
• Beleidskredieten										
Begrotingsonderdeel[42]	Vastleggingen	(1a)								
	Betalingen	(2a)								
Begrotingsonderdeel	Vastleggingen	(1b)								
	Betalingen	(2b)								
Uit het budget van specifieke programma's gefinancierde administratieve kredieten[43]										
Begrotingsonderdeel		(3)								
TOTAAL kredieten	Vastleggingen	=1a+1b +3								

41 N is het jaar waarin met de uitvoering van het voorstel/initiatief wordt begonnen. Vervang "N" door het verwachte eerste jaar van uitvoering (bijvoorbeeld: 2021). Hetzelfde voor de volgende jaren.

42 Volgens de officiële begrotingsnomenclatuur.

43 Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

voor DG <…….>	Betalingen	=2a+2b +3								

•TOTAAL beleidskredieten	Vastleggingen	(4)								
	Betalingen	(5)								
• TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)								
TOTAAL kredieten onder RUBRIEK <…> van het meerjarig financieel kader	Vastleggingen	=4+6								
	Betalingen	=5+6								

Wanneer het voorstel/initiatief gevolgen heeft voor meerdere beleidsrubrieken, herhaal bovenstaand deel:

• TOTAAL beleidskredieten (alle beleidsrubrieken)	Vastleggingen	(4)								
	Betalingen	(5)								
TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten (alle beleidsrubrieken)		(6)								
TOTAAL kredieten onder RUBRIEKEN 1 tot en met 6 van het meerjarig financieel kader (referentiebedrag)	Vastleggingen	=4+6								
	Betalingen	=5+6								

Rubriek van het meerjarig financieel kader	7	"Administratieve uitgaven"

Dit deel moet worden ingevuld aan de hand van de "administratieve begrotingsgegevens", die eerst moeten worden opgenomen in de bijlage bij het financieel memorandum (bijlage V bij de interne voorschriften), te uploaden in DECIDE met het oog op overleg tussen de diensten.

in miljoen EUR (tot op drie decimalen)

		Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
DG: CNECT						
• Personele middelen		1,030	1,030	1,030	1,030	**4,120**
• Andere administratieve uitgaven		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
TOTAAL DG CNECT	Kredieten	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

TOTAAL kredieten voor RUBRIEK 7 van het meerjarig financieel kader	(Totaal vastleggingen = totaal betalingen)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

in miljoen EUR (tot op drie decimalen)

		Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	**TOTAAL**
TOTAAL kredieten onder RUBRIEKEN 1 tot en met 7 van het meerjarig financieel kader	Vastleggingen	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Betalingen	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Geraamde output, gefinancierd met beleidskredieten

Vastleggingskredieten in miljoen EUR (tot op drie decimalen)

Vermeld doelstellingen en outputs ⇩			Jaar **N**		Jaar **N+1**		Jaar **N+2**		Jaar **N+3**		zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)						**TOTAAL**	
	OUTPUTS																	
	Soort [44]	Gem. kosten	Nee	Kosten	Nee	Kosten	Nee	Kosten	Nee	Kosten	Nee	Kosten	Nee	Kosten	Nee	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING nr. 1[45]…																		
– Output																		
– Output																		
– Output																		
Subtotaal voor specifieke doelstelling nr. 1																		
SPECIFIEKE DOELSTELLING NR. 2…																		
– Output																		
Subtotaal voor specifieke doelstelling nr. 2																		
TOTAAL																		

[44] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen enz.).

[45] Zoals beschreven in punt 1.4.2. “Specifieke doelstelling(en)…”

3.2.3. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig.

– ☑ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

in miljoen EUR (tot op drie decimalen)

	Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**	
RUBRIEK 7 van het meerjarig financieel kader					
Personele middelen	1,030	1,030	1,030	1,030	**4,120**
Andere administratieve uitgaven	0,222	0,222	0,222	0,222	**0,888**
Subtotaal RUBRIEK 7 van het meerjarig financieel kader	1,252	1,252	1,252	1,252	**5,008**
Buiten RUBRIEK 7[46] **van het meerjarig financieel kader**					
Personele middelen					
Andere administratieve uitgaven					
Subtotaal buiten RUBRIEK 7 van het meerjarig financieel kader					
TOTAAL	1,252	1,252	1,252	1,252	**5,008**

De benodigde kredieten voor personeel en andere administratieve uitgaven zullen worden gefinancierd uit de kredieten van het DG die reeds voor het beheer van deze actie zijn toegewezen en/of binnen het DG zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

[46] Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

3.2.3.1. Geraamde personeelsbehoeften

– ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig.

– ☑ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in voltijdequivalenten

		Jaar **2024**	Jaar **2025**	Jaar **2026**	Jaar **2027**
20 01 02 01 (zetel en vertegenwoordigingen van de Commissie)		6	6	6	6
20 01 02 03 (delegaties)					
01 01 01 01 (onderzoek door derden)					
01 01 01 11 (eigen onderzoek)					
Ander begrotingsonderdeel (geef aan welk)					
• Extern personeel (in voltijdequivalenten: vte)[47]					
20 02 01 (AC, END, INT van de "totale financiële middelen")		1	1	1	1
20 02 03 (AC, AL, END, INT en JPD in de delegaties)					
XX 01 xx **yy zz** [48]	– zetel				
	– delegaties				
01 01 01 02 (AC, END, INT – onderzoek door derden)					
01 01 01 12 (AC, END, INT – eigen onderzoek)					
Ander begrotingsonderdeel (geef aan welk)					
TOTAAL		**7**	**7**	**7**	**7**

XX is het beleidsterrein of de begrotingstitel.

Voor de benodigde personele middelen zal een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel 6 vte's x 157 000 EUR/jaar = 942 000 EUR	Zoals beschreven in punt 2.2.1: – voorbereiding van het normalisatieverzoek en/of gemeenschappelijke specificaties door middel van uitvoeringshandelingen indien niet met succes een normalisatieproces is afgerond; – opstellen van een gedelegeerde handeling [binnen 12 maanden na de inwerkingtreding van de verordening] tot nadere bepaling van de definities van de kritieke producten met digitale elementen; – mogelijke voorbereiding van gedelegeerde handelingen voor het bijwerken van de lijst van kritieke producten van klasse I en II; te specificeren of een beperking of uitsluiting noodzakelijk is voor producten met digitale elementen die worden gedekt door andere regels van de Unie tot vaststelling van eisen die hetzelfde beschermingsniveau bieden als deze verordening; de certificering verplicht te stellen van bepaalde zeer kritieke producten met digitale elementen op basis van de in deze verordening vastgestelde criteria; specificeren van de minimaal vereiste inhoud van de EU-

[47] AC = agent contractuel (arbeidscontractant); AL = agent local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT = intérimaire (uitzendkracht); JPD = junior professionals in delegatie.

[48] Subplafond voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

	conformiteitsverklaring en het aanvullen van de elementen die in de technische documentatie moeten worden opgenomen; – mogelijke voorbereiding van uitvoeringshandelingen met betrekking tot het formaat of de elementen van de rapportageverplichtingen, de softwarestuklijst, gemeenschappelijke specificaties of het aanbrengen van de CE-markering; – mogelijke voorbereiding van een onmiddellijk optreden voor het opleggen van corrigerende of beperkende maatregelen in uitzonderlijke omstandigheden om de goede werking van de interne markt te vrijwaren, met inbegrip van de voorbereiding van een uitvoeringshandeling; – organisatie en coördinatie van de aanmeldingen door de lidstaten van aangemelde instanties en de coördinatie van de aangemelde instanties; – ondersteuning van de coördinatie van de markttoezichtautoriteiten van de lidstaten.
Extern personeel 1 END x 88 000 EUR/jaar	Zoals beschreven in punt 2.2.1: – voorbereiding van het normalisatieverzoek en/of gemeenschappelijke specificaties door middel van uitvoeringshandelingen indien niet met succes een normalisatieproces is afgerond; – opstellen van een gedelegeerde handeling [binnen 12 maanden na de inwerkingtreding van de verordening] tot nadere bepaling van de definities van de kritieke producten met digitale elementen; – mogelijke voorbereiding van gedelegeerde handelingen voor het bijwerken van de lijst van kritieke producten van klasse I en II; te specificeren of een beperking of uitsluiting noodzakelijk is voor producten met digitale elementen die worden gedekt door andere regels van de Unie tot vaststelling van eisen die hetzelfde beschermingsniveau bieden als deze verordening; de certificering verplicht te stellen van bepaalde zeer kritieke producten met digitale elementen op basis van de in deze verordening vastgestelde criteria; specificeren van de minimaal vereiste inhoud van de EU-conformiteitsverklaring en het aanvullen van de elementen die in de technische documentatie moeten worden opgenomen; – mogelijke voorbereiding van uitvoeringshandelingen met betrekking tot het formaat of de elementen van de rapportageverplichtingen, de softwarestuklijst, gemeenschappelijke specificaties of het aanbrengen van de CE-markering; – mogelijke voorbereiding van een onmiddellijk optreden voor het opleggen van corrigerende of beperkende maatregelen in uitzonderlijke omstandigheden om de goede werking van de interne markt te vrijwaren, met inbegrip van de voorbereiding van een uitvoeringshandeling; – organisatie en coördinatie van de aanmeldingen door de lidstaten van aangemelde instanties en de coördinatie van de aangemelde instanties; – ondersteuning van de coördinatie van de markttoezichtautoriteiten van de lidstaten.

3.2.4. Verenigbaarheid met het huidige meerjarige financiële kader

Het voorstel/initiatief:

– x kan volledig worden gefinancierd door middel van herschikking binnen de relevante rubriek van het meerjarig financieel kader (MFK).

Er is geen herprogrammering nodig.

– ☐ hiervoor moet een beroep worden gedaan op de niet-toegewezen marge in de desbetreffende rubriek van het MFK en/of op de speciale instrumenten zoals gedefinieerd in de MFK-verordening.

–

– ☐ hiervoor is een herziening van het MFK nodig.

–

3.2.5. Bijdragen van derden

Het voorstel/initiatief:

– x voorziet niet in medefinanciering door derden

– ☐ voorziet in medefinanciering door derden, zoals hieronder wordt geraamd:

Kredieten in miljoen EUR (tot op drie decimalen)

	Jaar **N**[49]	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			Totaal
Medefinancieringsbron								
TOTAAL medegefinancierde kredieten								

[49] N is het jaar waarin met de uitvoering van het voorstel/initiatief wordt begonnen. Vervang "N" door het verwachte eerste jaar van uitvoering (bijvoorbeeld: 2021). Hetzelfde voor de volgende jaren.

3.3. Geraamde gevolgen voor de ontvangsten

– ☐ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.

– ☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

  – ☐ voor de eigen middelen

  – ☐ voor de overige ontvangsten

  – Geef aan of de ontvangsten worden toegewezen aan de begrotingsonderdelen voor uitgaven ☐

in miljoen EUR (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief[50]						
		Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	zoveel jaren als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
Artikel ……								

Vermeld voor de toegewezen ontvangsten het (de) betrokken begrotingsonderde(e)l(en) voor uitgaven.

Andere opmerkingen (bv. over de methode/formule voor de berekening van de gevolgen voor de ontvangsten of andere informatie).

[50] Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. na aftrek van 20 % aan inningskosten.