Publicatieblad
van de Europese Unie

NL
L-serie

2024/2847

20.11.2024

VERORDENING (EU) 2024/2847 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 23 oktober 2024

betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid)

(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],

Na raadpleging van het Comité van de Regio's,

Handelend volgens de gewone wetgevingsprocedure [2],

Overwegende hetgeen volgt:

(1) Cyberbeveiliging is een van de belangrijkste uitdagingen voor de Unie. Verbonden apparaten zullen de komende jaren exponentieel toenemen in aantal en verscheidenheid. Cyberaanvallen zijn een zaak van algemeen belang, omdat zij niet alleen een kritieke impact hebben op de economie van de Unie, maar ook op de democratie en de veiligheid en gezondheid van de consument. De aanpak van de Unie op het gebied van cyberbeveiliging moet derhalve worden versterkt, de cyberweerbaarheid worden aangepakt op Unieniveau en de werking van de interne markt 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 die 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 die 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, bijvoorbeeld door de transparantie te verbeteren met betrekking tot de ondersteuningsperiode van producten met digitale elementen die op de markt worden aangeboden.

(3) Het relevante Unierecht dat 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. Het bestaande Unierecht met betrekking tot cyberbeveiliging, met inbegrip van Verordening (EU) 2019/881 van het Europees Parlement en de Raad [3] en Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad [4], heeft echter niet rechtstreeks betrekking op verplichte eisen voor de beveiliging van producten met digitale elementen.

---

[1] PB C 100 van 16.3.2023, blz. 101.

[2] Standpunt van het Europees Parlement van 12 maart 2024 (nog niet in het Publicatieblad bekendgemaakt) en besluit van de Raad van 10 oktober 2024.

[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] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).

(4) Hoewel het bestaande Unierecht 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 die producten toeneemt en bedrijven en organisaties onnodig worden belast om aan een groot aantal vereisten en verplichtingen voor soortgelijke producten te voldoen. De cyberbeveiliging van die producten heeft een sterke grensoverschrijdende dimensie, aangezien producten met digitale elementen die in één lidstaat of derde land worden vervaardigd, vaak door organisaties en consumenten op de gehele interne markt worden gebruikt. Dat maakt het noodzakelijk om het veld op het niveau van de Unie te reguleren, teneinde te zorgen voor een geharmoniseerd regelgevingskader en rechtszekerheid voor gebruikers, organisaties en bedrijven, met inbegrip van kleine, middelgrote en micro-ondernemingen zoals gedefinieerd in de bijlage bij Aanbeveling 2003/361/EG van de Commissie ([5]). Het regelgevingslandschap van de Unie moet worden geharmoniseerd door horizontale cyberbeveiligingsvereisten in te voeren voor producten met digitale elementen. Daarnaast zou er in de hele Unie moeten worden gezorgd voor rechtszekerheid voor marktdeelnemers en gebruikers en voor een betere harmonisatie van de interne markt, alsook evenredigheid voor kleine, middelgrote en micro-ondernemingen, waardoor de voorwaarden voor marktdeelnemers die die markt willen betreden, worden verbeterd.

(5) Wat betreft kleine, middelgrote en micro-ondernemingen, moeten bij het bepalen van de categorie waarin een onderneming valt, de bepalingen van de bijlage bij Aanbeveling 2003/361/EG in hun geheel worden toegepast. Daarom moeten bij de berekening van het aantal werkzame personen en van de financiële drempels ter bepaling van de categorieën ondernemingen ook de bepalingen worden toegepast van artikel 6 van de bijlage bij Aanbeveling 2003/361/EG inzake de vaststelling van de gegevens van een onderneming met inachtneming van specifieke soorten ondernemingen, zoals partnerondernemingen of verbonden ondernemingen.

(6) De Commissie moet richtsnoeren verstrekken om marktdeelnemers, in het bijzonder kleine, middelgrote en micro-ondernemingen, bij te staan bij de toepassing van deze verordening. Dergelijke richtsnoeren moeten onder meer betrekking hebben op het toepassingsgebied van deze verordening, met name gegevensverwerking op afstand en de gevolgen daarvan voor ontwikkelaars van vrije en opensourcesoftware, op de toepassing van de criteria die worden gebruikt om ondersteuningsperioden te bepalen voor producten met digitale elementen, op de wisselwerking tussen deze verordening en ander Unierecht, en de notie van ingrijpende wijziging.

(7) Op het niveau van de Unie wordt in diverse programmatische en politieke documenten, zoals de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 16 december 2020 getiteld "De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk", de conclusies van de Raad van 2 december 2020 over de cyberbeveiliging van verbonden apparaten en van 23 mei 2022 over de ontwikkeling van de cyberstrategie van de Europese Unie en de resolutie van het Europees Parlement van 10 juni 2021 over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk ([6]), aangedrongen op specifieke cyberbeveiligingsvereisten van de Unie voor digitale of verbonden producten, in een context waarin verschillende derde landen maatregelen nemen om dat probleem op eigen initiatief aan te pakken. In het eindverslag van de Conferentie over de toekomst van Europa werd door de burgers gepleit voor "een sterkere rol voor de EU bij de bestrijding van cyberdreigingen". Om ervoor te zorgen dat de Unie een leidende internationale rol op het gebied van cyberbeveiliging kan spelen, is het van belang een ambitieus regelgevingskader tot stand te brengen.

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

(9) Onder bepaalde omstandigheden kunnen alle producten met digitale elementen die zijn geïntegreerd in of verbonden met een groter elektronisch informatiesysteem, als 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 worden ontworpen en ontwikkeld overeenkomstig de essentiële cyberbeveiligingsvereisten van deze verordening. Die verplichting heeft betrekking zowel op zowel producten die fysiek kunnen worden verbonden via hardware-interfaces als op 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 uitbuitingen van kwetsbaarheden, moeten fabrikanten ook zorgen voor de cyberbeveiliging van producten met digitale elementen die slechts indirect verbonden zijn met andere apparaten of netwerken.

([5]) Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

([6]) PB C 67 van 8.2.2022, blz. 81.

(10) Door cyberbeveiligingsvereisten vast te stellen voor het in de handel brengen van producten met digitale elementen, is het de bedoeling dat de cyberbeveiliging van die producten voor zowel consumenten als bedrijven wordt verbeterd. Die vereisten zullen er ook voor zorgen dat cyberbeveiliging in alle toeleveringsketens in aanmerking wordt genomen om eindproducten met digitale elementen en hun componenten veiliger te maken. Daaronder vallen ook eisen voor het in de handel brengen van consumentenproducten met digitale elementen die bestemd zijn voor kwetsbare consumenten, zoals speelgoed en babymonitoringsystemen. Consumentenproducten met digitale elementen die in deze verordening onder een categorie van belangrijke producten met digitale elementen vallen, houden een hoger cyberbeveiligingsrisico in doordat zij een functie vervullen die een aanzienlijk risico op nadelige effecten inhoudt door de intensiteit ervan en het vermogen om de gezondheid, beveiliging of veiligheid van gebruikers van dergelijke producten te schaden, en moeten aan een strengere conformiteitsbeoordelingsprocedure worden onderworpen. Dat geldt voor producten als slimme huizen met beveiligingsfuncties, met inbegrip van slimme deursloten, babymonitoringsystemen en alarmsystemen, verbonden speelgoed en persoonlijke wearables met gezondheidstechnologie. Daarnaast zullen de strengere conformiteitsbeoordelingsprocedures voor producten met digitale elementen die in deze verordening onder een categorie van belangrijke of kritieke producten met digitale elementen vallen, ertoe bijdragen dat voor consumenten de mogelijk negatieve gevolgen van uitbuiting van kwetsbaarheden worden vermeden.

(11) Het doel van deze verordening is voor een hoog niveau van cyberbeveiliging te zorgen voor producten met digitale elementen en hun geïntegreerde oplossingen voor gegevensverwerking op afstand. Dergelijke oplossingen voor gegevensverwerking op afstand moeten worden gedefinieerd als gegevensverwerking vanop een afstand, waarvoor de software is ontworpen en ontwikkeld door of namens de fabrikant van het betrokken product met digitale elementen, bij gebreke waarvan het product met digitale elementen een van zijn functies niet zou kunnen vervullen. Dankzij die aanpak worden dergelijke producten volledig en op passende wijze beveiligd door de fabrikanten, ongeacht of de gegevens worden verwerkt of lokaal worden opgeslagen op het apparaat van de gebruiker dan wel op afstand door de fabrikant. Tegelijkertijd valt de verwerking of opslag op afstand slechts binnen het toepassingsgebied van deze verordening voor zover dat noodzakelijk is opdat een product met digitale elementen zijn functies vervult. Een dergelijke verwerking of opslag op afstand heeft ook betrekking op situaties waarbij een mobiele applicatie toegang vereist tot een applicatieprogramma-interface of tot een databank die wordt geleverd door middel van een door de fabrikant ontwikkelde dienst. In dat geval valt die dienst binnen het toepassingsgebied van deze verordening als een oplossing voor gegevensverwerking op afstand. De vereisten met betrekking tot oplossingen voor gegevensverwerking op afstand die binnen het toepassingsgebied van deze verordening vallen, omvatten derhalve geen technische, operationele of organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen van een fabrikant als geheel te beheren.

(12) Bij cloudoplossingen gaat het enkel om oplossingen voor gegevensverwerking op afstand in de zin van deze verordening indien zij voldoen aan de definitie van deze verordening. Zo vallen voor de cloud geschikte functies van een fabrikant van slimme huishoudelijke apparaten die gebruikers in staat stellen het apparaat op afstand te bedienen, binnen het toepassingsgebied van deze verordening. Anderzijds vallen websites die de functionaliteit van een product met digitale elementen niet ondersteunen of clouddiensten die zijn ontworpen en ontwikkeld buiten de verantwoordelijkheid van een fabrikant van een product met digitale elementen, niet binnen het toepassingsgebied van deze verordening. Richtlijn (EU) 2022/2555 is van toepassing op cloudcomputerdiensten en cloudmodellen, zoals software als dienst (*Software as a Service* — SaaS), platform als dienst (*Platform as a Service* — PaaS) of infrastructuur als dienst (*Infrastructure as a Service* — IaaS). Entiteiten die cloudcomputerdiensten aanbieden in de Unie en die als middelgrote ondernemingen worden aangemerkt uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, of die de in lid 1 van dat artikel vastgestelde drempels voor middelgrote ondernemingen overschrijden, vallen binnen het toepassingsgebied van die richtlijn.

(13) Overeenkomstig de doelstelling van deze verordening om belemmeringen voor het vrije verkeer van producten met digitale elementen weg te nemen, mogen de lidstaten, met betrekking tot de onder deze verordening vallende aangelegenheden, niet beletten dat producten met digitale elementen die aan deze verordening voldoen, op de markt worden aangeboden. Daarom mogen de lidstaten voor aangelegenheden die door deze verordening worden geharmoniseerd, geen aanvullende cyberbeveiligingsvereisten opleggen voor het op de markt aanbieden van producten met digitale elementen. Elke publieke of private entiteit kan echter, naast de vereisten van deze verordening, aanvullende eisen vaststellen voor de aankoop of het gebruik van producten met digitale elementen voor haar specifieke doeleinden, en kan er daarom voor kiezen producten met digitale elementen te gebruiken die voldoen aan strengere of specifiekere cyberbeveiligingsvereisten dan die welke uit hoofde van deze verordening gelden voor het op de markt aanbieden ervan. Onverminderd de Richtlijnen 2014/24/EU ([7]) en 2014/25/EU ([8]) van het Europees Parlement en de Raad moeten de lidstaten er, bij de aankoop van producten met digitale elementen, die moeten voldoen aan de essentiële cyberbeveiligingsvereisten van deze verordening, met inbegrip van de eisen inzake

([7]) Richtlijn 2014/24/EU van het Europees Parlement de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65).

([8]) Richtlijn 2014/25/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van opdrachten in de sectoren water- en energievoorziening, vervoer en postdiensten en houdende intrekking van Richtlijn 2004/17/EG (PB L 94 van 28.3.2014, blz. 243).

de respons op kwetsbaarheden, voor zorgen dat bij het aankoopproces rekening wordt gehouden met dergelijke eisen en met het vermogen van de fabrikanten om cyberbeveiligingsmaatregelen doeltreffend toe te passen en cyberdreigingen te beheren. Voorts bevat Richtlijn (EU) 2022/2555 maatregelen voor het beheer van cyberbeveiligingsrisico's voor essentiële en belangrijke entiteiten als bedoeld in artikel 3 van die richtlijn, waaruit maatregelen voor de beveiliging van de toeleveringsketen kunnen voortvloeien waarbij dergelijke entiteiten producten met digitale elementen moeten gebruiken die voldoen aan strengere cyberbeveiligingsvereisten dan die van deze verordening. In overeenstemming met Richtlijn (EU) 2022/2555 en het daarin opgenomen beginsel van minimumharmonisatie, kunnen de lidstaten daarom aanvullende cyberbeveiligingsvereisten opleggen voor het gebruik van ICT (informatie- en communicatietechnologie) -producten door essentiële of belangrijke entiteiten op grond van die richtlijn, teneinde een hoger niveau van cyberbeveiliging te waarborgen, mits die vereisten stroken met de verplichtingen van de lidstaten die zijn vastgelegd in het Unierecht. Niet-technische factoren die verband houden met producten met digitale elementen en de fabrikanten ervan vallen bijvoorbeeld niet onder deze verordening. De lidstaten kunnen daarom nationale maatregelen vaststellen, met inbegrip van beperkingen op producten met digitale elementen of leveranciers van dergelijke producten, waarbij rekening wordt gehouden met niet-technische factoren. Van nationale maatregelen met betrekking tot dergelijke factoren wordt vereist dat zij in overeenstemming zijn met het Unierecht.

(14) Deze verordening mag geen afbreuk doen aan de verantwoordelijkheid van de lidstaten om in overeenstemming met het Unierecht maatregelen te nemen ter bescherming van de nationale veiligheid. De lidstaten moeten producten met digitale elementen die voor nationale veiligheids- of defensiedoeleinden worden aangekocht of gebruikt, aan aanvullende maatregelen kunnen onderwerpen, mits die maatregelen stroken met de verplichtingen van de lidstaten die zijn vastgelegd in het Unierecht.

(15) Deze verordening is alleen van toepassing op marktdeelnemers met betrekking tot producten met digitale elementen die op de markt worden aangeboden, en dus in het kader van een handelsactiviteit worden geleverd voor distributie of gebruik op de markt van de Unie. De levering in het kader van een handelsactiviteit wordt mogelijk niet alleen gekenmerkt door het in rekening brengen van een prijs voor een product met digitale elementen, maar ook door het in rekening brengen van een prijs voor technische ondersteuningsdiensten indien die prijs niet alleen dient om de gemaakte kosten te dekken, door een intentie van tegeldemaking, bijvoorbeeld door het aanbieden van een softwareplatform waarmee de fabrikant andere diensten te gelde maakt, door als voorwaarde voor gebruik de verwerking van persoonsgegevens te eisen voor andere redenen dan uitsluitend de verbetering van de beveiliging, compatibiliteit of interoperabiliteit van de software, of door donaties te accepteren die de kosten van het ontwerp, de ontwikkeling en de levering van een product met digitale elementen overstijgen. Het aanvaarden van schenkingen zonder winstoogmerk mag niet worden beschouwd als een handelsactiviteit.

(16) De levering van producten met digitale elementen in het kader van een dienstverrichting waarvoor uitsluitend een vergoeding wordt aangerekend om de werkelijke kosten te dekken die rechtstreeks verband houden met de verrichting van die dienst, bijvoorbeeld in het geval van bepaalde producten met digitale elementen die door overheidsinstanties worden geleverd, mogen niet alleen op basis daarvan als een handelsactiviteit worden beschouwd voor de toepassing van deze verordening. Bovendien mogen producten met digitale elementen die door een overheidsinstantie uitsluitend voor eigen gebruik worden ontwikkeld of gewijzigd, niet worden beschouwd als producten die op de markt worden aangeboden in de zin van deze verordening.

(17) Software en gegevens die openlijk worden gedeeld en die, of gewijzigde versies ervan, vrij toegankelijk, bruikbaar, wijzigbaar en herdistribueerbaar zijn door gebruikers, kunnen bijdragen aan onderzoek en innovatie op de markt. Om de ontwikkeling en uitrol van vrije en opensourcesoftware te bevorderen, met name door kleine, middelgrote en micro-ondernemingen, met inbegrip van start-ups, particulieren, organisaties zonder winstoogmerk en academische onderzoeksorganisaties, moet bij de toepassing van deze verordening op als vrije en opensourcesoftware aangemerkte producten met digitale elementen die in het kader van een handelsactiviteit worden geleverd voor distributie of gebruik, rekening worden gehouden met de aard van de verschillende ontwikkelingsmodellen voor software die worden gedistribueerd en ontwikkeld onder licenties voor vrije en opensourcesoftware.

(18) Vrije en opensourcesoftware wordt beschouwd als software waarvan de broncode openlijk wordt gedeeld en die beschikbaar wordt gesteld onder een licentie die voorziet in alle rechten om die vrijelijk toegankelijk, bruikbaar, wijzigbaar en herdistribueerbaar te maken. Vrije en opensourcesoftware wordt openlijk ontwikkeld, onderhouden en gedistribueerd, onder meer via onlineplatforms. Wat de marktdeelnemers betreft waarop deze verordening van toepassing is, mag alleen vrije en opensourcesoftware die op de markt wordt aangeboden en derhalve wordt geleverd voor distributie of gebruik in het kader van een handelsactiviteit, binnen het toepassingsgebied van deze verordening vallen. Bij het bepalen van het handels- of niet-handelskarakter van die activiteit mag derhalve geen rekening worden gehouden met de loutere omstandigheden waaronder het product met digitale elementen is ontwikkeld of met de wijze waarop de ontwikkeling ervan is gefinancierd. Meer in het bijzonder mag voor de toepassing van deze verordening en voor de marktdeelnemers die onder deze verordening vallen, om een duidelijk onderscheid te maken tussen de ontwikkelings- en leveringsfase, de levering van producten met digitale elementen die als vrije en

opensourcesoftware worden aangemerkt en die niet door de fabrikanten te gelde worden gemaakt, niet als een handelsactiviteit worden beschouwd. Voorts mag de levering van producten met digitale elementen die als componenten voor vrije en opensourcesoftware worden aangemerkt en bestemd zijn om door andere fabrikanten in hun eigen producten met digitale elementen te worden verwerkt, alleen worden beschouwd als het op de markt aanbieden indien de component door de oorspronkelijke fabrikant te gelde is gemaakt. Zo mag het loutere feit dat een opensourcesoftwareproduct met digitale elementen financiële steun ontvangt van fabrikanten of dat fabrikanten bijdragen aan de ontwikkeling van een dergelijk product, op zich niet bepalend zijn voor het handelskarakter van de activiteit. Bovendien mag het gegeven alleen dat er regelmatige releases voorkomen, niet tot de conclusie leiden dat een product met digitale elementen wordt geleverd in het kader van een handelsactiviteit. Ten slotte mag voor de toepassing van deze verordening, de ontwikkeling door non-profitorganisaties van producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt, niet als een handelsactiviteit worden beschouwd, mits de organisatie zodanig is opgezet dat alle inkomsten na aftrek van kosten worden aangewend om doelstellingen zonder winstoogmerk te verwezenlijken. Deze verordening is niet van toepassing op natuurlijke of rechtspersonen die met broncode bijdragen aan producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt en niet onder hun verantwoordelijkheid vallen.

(19) Gezien het belang voor cyberbeveiliging bij veel producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt en die worden gepubliceerd, maar niet op de markt worden aangeboden in de zin van deze verordening, moeten rechtspersonen die op langdurige basis de ontwikkeling ondersteunen van dergelijke producten die zijn bestemd voor handelsactiviteiten, en die een belangrijke rol spelen bij het waarborgen van de levensvatbaarheid van die producten (opensourcesoftwarestewards), worden onderworpen aan een minder restrictief en op maat gesneden regelgevingskader. Tot opensourcesoftwarestewards behoren bepaalde stichtingen en entiteiten die vrije en opensourcesoftware ontwikkelen en publiceren in een zakelijke context, met inbegrip van entiteiten zonder winstoogmerk. In het regelgevingskader moet rekening worden gehouden met de specifieke aard van die opensourcesoftwarestewards en met de verenigbaarheid met het soort verplichtingen dat wordt opgelegd. Het regelgevingskader mag enkel betrekking hebben op producten met digitale elementen die als vrije en opensourcesoftware kunnen worden aangemerkt en die uiteindelijk bestemd zijn voor handelsactiviteiten, zoals voor integratie in handelsdiensten of in te gelde gemaakte producten met digitale elementen. Voor de toepassing van dat regelgevingskader omvat een voornemen om producten met digitale elementen te integreren in producten die te gelde gemaakt worden, ook gevallen waarin fabrikanten die een component in hun eigen producten met digitale elementen integreren, regelmatig bijdragen tot de ontwikkeling van die component dan wel regelmatige financiële bijstand verlenen om de continuïteit van een softwareproduct te waarborgen. Het verlenen van langdurige ondersteuning voor de ontwikkeling van een product met digitale elementen omvat onder meer het hosten en beheren van samenwerkingsplatforms voor softwareontwikkeling, het hosten van broncodes of software, het besturen of beheren van producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt, alsook het aansturen van de ontwikkeling van dergelijke producten. Aangezien het minder restrictieve en op maat gesneden regelgevingskader niet dezelfde verplichtingen oplegt aan opensourcesoftwarestewards als aan fabrikanten uit hoofde van deze verordening, mag het opensourcesoftwarestewards niet worden toegestaan de CE-markering aan te brengen op producten met digitale elementen waarvan zij de ontwikkeling ondersteunen.

(20) Het louter hosten van producten met digitale elementen in open databases, onder meer via pakketbeheerders of op samenwerkingsplatforms, vormt op zich niet het op de markt aanbieden van een product met digitale elementen. Aanbieders van dergelijke diensten mogen alleen als distributeur worden beschouwd indien zij dergelijke software op de markt aanbieden en dus leveren voor distributie of gebruik op de markt van de Unie in het kader van een handelsactiviteit.

(21) Ter ondersteuning en vereenvoudiging van de passende zorgvuldigheid bij fabrikanten die componenten voor vrije en opensourcesoftware, die niet onder de essentiële cyberbeveiligingsvereisten van deze verordening vallen, integreren in hun producten met digitale elementen, moet de Commissie vrijwillige beveiligingsattestatieprogramma's kunnen opzetten, hetzij door middel van een gedelegeerde handeling ter aanvulling van deze verordening, hetzij door op grond van artikel 48 van Verordening (EU) 2019/881 te verzoeken een Europese cyberbeveiligingscertificeringsregeling op te stellen die rekening houdt met de specifieke kenmerken van de ontwikkelingsmodellen voor vrije en opensourcesoftware. De beveiligingsattestatieprogramma's moeten zodanig worden opgezet dat de beveiligingsattestatie niet alleen kan worden geïnitieerd of gefinancierd door natuurlijke of rechtspersonen die een als vrije en opensourcesoftware aangemerkt product met digitale elementen ontwikkelen of daartoe bijdragen, maar ook door derden, zoals fabrikanten die dergelijke producten met digitale elementen integreren in hun eigen producten, gebruikers of EU- en nationale overheidsdiensten.

(22) Gelet op de doelstellingen van deze verordening inzake publieke cyberbeveiliging en om het situationeel bewustzijn van de lidstaten te verbeteren met betrekking tot de afhankelijkheid van de Unie van softwarecomponenten, en in het bijzonder van componenten voor potentieel vrije en opensourcesoftware, moet een bij deze verordening opgerichte speciale administratievesamenwerkingsgroep (*administrative cooperation group*, ADCO) kunnen besluiten gezamenlijk een beoordeling uit te voeren over de afhankelijkheid van de Unie. Markttoezichtautoriteiten moeten fabrikanten van door de ADCO vastgestelde categorieën producten met digitale elementen kunnen verzoeken de softwarestuklijst van materialen in te dienen die zij op grond van deze verordening hebben gegenereerd. Om de vertrouwelijkheid van softwarestuklijsten te beschermen, moeten markttoezichtautoriteiten relevante informatie over afhankelijkheden op een geanonimiseerde en geaggregeerde manier aan de ADCO verstrekken.

(23) De doeltreffendheid van de uitvoering van deze verordening zal ook afhangen van de beschikbaarheid van passende vaardigheden op het gebied van cyberbeveiliging. Op het niveau van de Unie wordt in diverse programmatische en politieke documenten, waaronder de mededeling van de Commissie van 18 april 2023 over het wegwerken van het tekort aan cyberbeveiligingsprofessionals om het concurrentievermogen, de groei en de veerkracht van Europa te versterken en de conclusies van de Raad van 22 mei 2023 over het EU-beleid inzake cyberdefensie, bevestigd dat in de Unie een tekort bestaat aan vaardigheden op het gebied van cyberbeveiliging en dat dergelijke uitdagingen prioritair moeten worden aangepakt, zowel in de publieke als in de particuliere sector. Met het oog op een doeltreffende uitvoering van deze verordening moeten de lidstaten ervoor zorgen dat er voldoende middelen beschikbaar zijn om de markttoezichtautoriteiten en conformiteitsbeoordelingsinstanties naar behoren te voorzien van personeel, zodat zij hun in deze verordening vastgestelde taken kunnen uitvoeren. Die maatregelen moeten de mobiliteit van werknemers op het gebied van cyberbeveiliging en in aanverwante loopbaantrajecten vergroten. Evenzo moeten zij zorgen voor meer veerkracht en inclusiviteit, ook op het vlak van gender, bij het personeel op het gebied van cyberbeveiliging. De lidstaten moeten daarom maatregelen treffen om ervoor te zorgen dat die taken worden uitgevoerd door naar behoren opgeleide professionals met de nodige vaardigheden op het gebied van cyberbeveiliging. Evenzo moeten fabrikanten ervoor zorgen dat hun personeel over de nodige vaardigheden beschikt om hun verplichtingen zoals vastgelegd in deze verordening na te leven. De lidstaten en de Commissie moeten, in overeenstemming met hun prerogatieven en bevoegdheden en hun specifieke taken uit hoofde van deze verordening, maatregelen nemen ter ondersteuning van fabrikanten, en in het bijzonder kleine, middelgrote en micro-ondernemingen, met inbegrip van start-ups, ook op gebieden als de ontwikkeling van vaardigheden, ten behoeve van de nakoming van hun verplichtingen zoals vastgelegd in deze verordening. Daarnaast en aangezien de lidstaten op grond van Richtlijn (EU) 2022/2555 verplicht zijn, als onderdeel van hun nationale cyberbeveiligingsstrategieën, beleid vast te stellen ter bevordering en ontwikkeling van opleiding op het gebied van cyberbeveiliging en cyberbeveiligingsvaardigheden, kunnen zij bij de vaststelling van dergelijke strategieën ook overwegen tegemoet te komen aan de behoeften aan vaardigheden op het gebied van cyberbeveiliging die voortvloeien uit deze verordening, met inbegrip van de behoeften aan omscholing en bijscholing.

(24) Een veilig internet is onontbeerlijk voor de werking van kritieke infrastructuur en voor de samenleving als geheel. Richtlijn (EU) 2022/2555 heeft tot doel een hoog niveau van cyberbeveiliging te waarborgen van diensten die worden verleend door in artikel 3 van die richtlijn bedoelde essentiële en belangrijke entiteiten, waaronder aanbieders van digitale infrastructuur die de kernfuncties van het open internet ondersteunen, zorgen voor internettoegang en internetdiensten verlenen. 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 (EU) 2022/2555 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.

(25) Verordening (EU) 2017/745 van het Europees Parlement en de Raad ([9]) bevat voorschriften voor medische hulpmiddelen en Verordening (EU) 2017/746 van het Europees Parlement en de Raad ([10]) bevat voorschriften voor medische hulpmiddelen voor in-vitrodiagnostiek. Die 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 gehelelevenscyclusbenadering vallen ook onder die verordeningen. Die 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. Producten met digitale elementen waarop een van die verordeningen van toepassing is, mogen daarom niet onder deze verordening vallen.

(26) Producten met digitale elementen die uitsluitend voor doeleinden van nationale veiligheid of voor defensiedoeleinden zijn ontwikkeld of gewijzigd, of producten die specifiek zijn ontworpen voor de verwerking van gerubriceerde informatie, vallen buiten het toepassingsgebied van deze verordening. De lidstaten worden aangemoedigd om voor die producten hetzelfde of een hoger beschermingsniveau te waarborgen als voor producten die binnen het toepassingsgebied van deze verordening vallen.

([9]) 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).

([10]) 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 Besluit2010/227/EU van de Commissie (PB L 117 van 5.5.2017, blz. 176).

(27) Bij Verordening (EU) 2019/2144 van het Europees Parlement en de Raad ([11]) zijn voorschriften vastgesteld voor de typegoedkeuring van voertuigen en van de systemen 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 cyberbeveiligingsrisico'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, met name VN-Reglement nr. 155 inzake uniforme bepalingen voor de goedkeuring van voertuigen met betrekking tot cyberbeveiliging en het beheersysteem voor cyberbeveiliging ([12]), 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 ([13]) de totstandbrenging en instandhouding van een hoog, uniform veiligheidsniveau in de burgerluchtvaart in de Unie. Daarmee komt een kader tot stand voor essentiële eisen inzake luchtwaardigheid voor luchtvaartproducten, hun onderdelen en apparatuur, met inbegrip van software, waarin verplichtingen opgenomen zijn om te beschermen tegen bedreigingen van de informatiebeveiliging. Het certificeringsproces uit hoofde van Verordening (EU) 2018/1139 waarborgt het zekerheidsniveau dat met deze verordening wordt beoogd. Producten met digitale elementen waarop Verordening (EU) 2019/2144 van toepassing is en producten die zijn gecertificeerd overeenkomstig Verordening (EU) 2018/1139, mogen derhalve niet onderworpen zijn aan de in deze verordening vastgestelde essentiële cyberbeveiligingsvereisten en conformiteitsbeoordelingsprocedures.

(28) Bij deze verordening worden horizontale cyberbeveiligingsregels vastgesteld die niet specifiek zijn voor sectoren of voor 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 cyberbeveiligingsvereisten 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 cyberbeveiligingsvereisten van 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 minstens hetzelfde beschermingsniveau bieden als deze verordening. De Commissie moet de bevoegdheid krijgen gedelegeerde handelingen vast te stellen om deze verordening aan te vullen door dergelijke producten en voorschriften aan te wijzen. Deze verordening bevat specifieke bepalingen voor bestaand Unierecht waarvoor dergelijke beperkingen of uitsluitingen moeten gelden, om de relatie met dat Unierecht te verduidelijken.

(29) Om ervoor te zorgen dat producten met digitale elementen die op de markt worden aangeboden, doeltreffend kunnen worden gerepareerd en de duurzaamheid ervan kan worden verlengd, moet een vrijstelling worden verleend voor reserveonderdelen. Die vrijstelling moet zowel betrekking hebben op reserveonderdelen die bedoeld zijn voor de reparatie van oudere producten die vóór de datum van toepassing van deze verordening werden aangeboden, als op reserveonderdelen die reeds een conformiteitsbeoordelingsprocedure op grond van deze verordening hebben ondergaan.

(30) Bij Gedelegeerde Verordening (EU) 2022/30 van de Commissie ([14]) is gespecificeerd dat een aantal essentiële eisen van artikel 3, lid 3, punten d), e) en f), van Richtlijn 2014/53/EU van het Europees Parlement en de Raad ([15]) in verband met netwerkschade en misbruik van netwerkmiddelen, persoonsgegevens en privacy, en fraude, van toepassing is op bepaalde radioapparatuur. Uitvoeringsbesluit C(2022) 5637 van de Commissie van 5 augustus 2022 betreffende een normalisatieverzoek aan het Europees Comité voor normalisatie en het Europees Comité voor elektrotechnische normalisatie bevat voorschriften voor de ontwikkeling van specifieke normen waarin nader wordt gespecificeerd hoe die essentiële eisen moeten worden aangepakt. De bij deze verordening vastgestelde essentiële cyberbeveiligingsvereisten omvatten alle elementen van de in artikel 3, lid 3, punten d), e) en f), van Richtlijn 2014/53/EU bedoelde essentiële eisen. Daarnaast zijn de in deze verordening vastgestelde essentiële cyberbeveili-

([11]) 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).

([12]) PB L 82 van 9.3.2021, blz. 30.

([13]) 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).

([14]) Gedelegeerde Verordening (EU) 2022/30 van de Commissie van 29 oktober 2021 tot aanvulling van Richtlijn 2014/53/EU van het Europees Parlement en de Raad met betrekking tot de toepassing van de essentiële eisen als bedoeld in artikel 3, lid 3, punten d), e) en f), van die richtlijn (PB L 7 van 12.1.2022, blz. 6).

([15]) Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG (PB L 153 van 22.5.2014, blz. 62).

gingsvereisten afgestemd op de doelstellingen van de eisen voor specifieke normen die in dat normalisatieverzoek zijn opgenomen. Wanneer 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 zijn verricht om de uitvoering van deze verordening te vergemakkelijken. Tijdens de overgangsperiode voor de toepassing van deze verordening moet de Commissie richtsnoeren verstrekken aan fabrikanten die onder deze verordening en ook onder Gedelegeerde Verordening (EU) 2022/30 vallen, zodat het eenvoudiger wordt om aan te tonen dat beide verordeningen worden nageleefd.

(31) Richtlijn (EU) 2024/2853 van het Europees Parlement en de Raad ([16]) vormt een aanvulling op deze verordening. Die richtlijn bevat aansprakelijkheidsregels voor gebrekkige producten, zodat benadeelden schadevergoeding kunnen vorderen wanneer schade is veroorzaakt door gebrekkige producten. 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 daardoor 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.

(32) Deze verordening mag geen afbreuk doen aan Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([17]), 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 van cyberbeveiligingsaspecten moeten in aanmerking worden genomen in het kader van de samenwerking tussen de Commissie, de Europese normalisatieorganisaties, het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), het Europees Comité voor gegevensbescherming, 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 het gegevensbeschermingsrecht van de Unie worden gecreëerd. Daartoe moeten de krachtens deze verordening aangewezen nationale markttoezichtautoriteiten samenwerken met autoriteiten die toezicht houden op de toepassing van het gegevensbeschermingsrecht van de Unie. Ook moeten die laatsten toegang hebben tot informatie die relevant is voor de uitvoering van hun taken.

(33) Voor zover hun producten binnen het toepassingsgebied van deze verordening vallen, moeten aanbieders van Europese portemonnees voor digitale identiteit als bedoeld in artikel 5 bis, lid 2, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad ([18]) zowel voldoen aan de horizontale essentiële cyberbeveiligingsvereisten van deze verordening als aan de specifieke beveiligingsvereisten van artikel 5 bis van Verordening (EU) nr. 910/2014. Om de naleving te vergemakkelijken, moeten aanbieders van Europese portemonnees voor digitale identiteit kunnen aantonen dat die portemonnees voldoen aan de vereisten van respectievelijk deze verordening en Verordening (EU) nr. 910/2014, door hun producten te certificeren in het kader van een Europese cyberbeveiligingscertificeringsregeling die is vastgesteld uit hoofde van Verordening (EU) 2019/881 en waarvoor de Commissie door middel van gedelegeerdehandelingen heeft voorzien in een vermoeden van conformiteit met deze verordening, voor zover het certificaat, of delen daarvan, die vereisten dekt.

(34) Wanneer fabrikanten tijdens de ontwerp- en ontwikkelingsfase bij derden ingekochte componenten integreren in producten met digitale elementen, moeten zij, om ervoor te zorgen dat de producten worden ontworpen, ontwikkeld en vervaardigd in overeenstemming met de essentiële cyberbeveiligingsvereisten van deze verordening, de passende zorgvuldigheid betrachten ten aanzien van die componenten, met inbegrip van vrije en

([16]) Richtlijn (EU) 2024/2853 van het Europees Parlement en de Raad van 23 oktober 2024 inzake aansprakelijkheid voor gebrekkige producten en tot intrekking van Richtlijn 85/374/EEG (PB L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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).

([18]) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).

opensourcesoftwarecomponenten die niet op de markt zijn aangeboden. Het passendezorgvuldigheidsniveau hangt af van de aard en het niveau van het cyberbeveiligingsrisico dat aan een bepaalde component verbonden is, en daarom moet daar rekening worden gehouden met een of meer van de volgende maatregelen: in voorkomend geval nagaan of de fabrikant van een component heeft aangetoond deze verordening na te leven, onder meer door te controleren of de component reeds voorzien is van de CE-markering; nagaan of een component regelmatig beveiligingsupdates ontvangt, bijvoorbeeld door de geschiedenis van de beveiligingsupdates te controleren; verifiëren of een component vrij is van kwetsbaarheden die zijn geregistreerd in de op grond van artikel 12, lid 2, van Richtlijn (EU) 2022/2555 ingestelde Europese kwetsbaarheidsdatabase of andere openbaar toegankelijke kwetsbaarheidsdatabases; of aanvullende veiligheidstests uitvoeren. De in deze verordening vastgestelde verplichtingen inzake de respons op kwetsbaarheden waaraan fabrikanten moeten voldoen wanneer zij een product met digitale elementen in de handel brengen en voor de duur van de ondersteuningsperiode, zijn van toepassing op producten met digitale elementen in hun geheel, met inbegrip van alle geïntegreerde componenten. Wanneer de fabrikant van het product met digitale elementen bij het betrachten van de passende zorgvuldigheid een kwetsbaarheid in een component vaststelt, ook in een vrije en opensourcecomponent, moet hij de persoon of entiteit die de component vervaardigt of onderhoudt op de hoogte brengen, de kwetsbaarheid aanpakken en verhelpen en, indien van toepassing, de persoon of entiteit de toegepaste beveiligingsoplossing bezorgen.

(35) Onmiddellijk na de overgangsperiode voor de toepassing van deze verordening is het mogelijk dat een fabrikant van een product met digitale elementen met daarin een of meer componenten afkomstig van derden die ook onder deze verordening vallen, in het kader van zijn passendezorgvuldigheidsverplichting niet kan nagaan of de fabrikanten van die componenten de conformiteit met deze verordening hebben aangetoond door bijvoorbeeld te controleren of de componenten reeds van de CE-markering zijn voorzien. Dat kan gebeuren wanneer de componenten zijn geïntegreerd voordat deze verordening van toepassing wordt op de fabrikanten van die componenten. In dat geval moet een fabrikant die dergelijke componenten integreert, andere middelen inzetten om de passende zorgvuldigheid te betrachten.

(36) Op producten met digitale elementen moet de CE-markering zichtbaar, leesbaar en onuitwisbaar 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. De lidstaten mogen voorts niet beletten dat op handelsbeurzen, tentoonstellingen en demonstraties of soortgelijke evenementen een product met digitale elementen wordt gepresenteerd en gebruikt dat niet aan deze verordening voldoet, met inbegrip van prototypes daarvan, mits het product wordt gepresenteerd met een zichtbaar teken dat duidelijk aangeeft dat het product niet aan deze verordening voldoet en dat het pas op de markt mag worden aangeboden zodra het dat wel doet.

(37) Om ervoor te zorgen dat fabrikanten software voor testdoeleinden kunnen uitgeven alvorens hun producten met digitale elementen 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 niet-afgewerkte software slechts beschikbaar wordt gesteld voor de tijd die nodig is om die te testen en feedback te verzamelen. Fabrikanten moeten ervoor zorgen dat software die onder die voorwaarden beschikbaar wordt gesteld, pas na een risicobeoordeling wordt uitgegeven en voor zover mogelijk voldoet aan de beveiligingsvereisten van deze verordening met betrekking tot de kenmerken van producten met digitale elementen. Fabrikanten moeten ook de vereisten inzake de respons op kwetsbaarheden zo veel mogelijk toepassen. Fabrikanten mogen gebruikers niet dwingen om te upgraden naar versies die alleen voor testdoeleinden worden uitgegeven.

(38) 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 cyberbeveiligingsvereisten worden vastgesteld. Die essentiële cyberbeveiligingsvereisten, met inbegrip van de vereisten inzake de respons op kwetsbaarheidsbeheer, zijn van toepassing op elk afzonderlijk product met digitale elementen wanneer het in de handel wordt gebracht, ongeacht of het product met digitale elementen als een afzonderlijke eenheid of in serie wordt vervaardigd. Zo moet voor een productsoort elk afzonderlijk product met digitale elementen, wanneer het in de handel wordt gebracht, alle beschikbare beveiligingspatches of -updates hebben ontvangen om de relevante veiligheidsproblemen aan te pakken. Wanneer de producten met digitale elementen vervolgens met fysieke of digitale middelen worden gewijzigd op een wijze die niet door de fabrikant is voorzien in de initiële risicobeoordeling en die ertoe kan leiden dat zij niet langer aan de relevante essentiële cyberbeveiligingsvereisten voldoen, moet de wijziging als ingrijpend worden beschouwd. Reparaties kunnen bijvoorbeeld worden gelijkgesteld met onderhoudswerkzaamheden, mits zij een reeds in de handel gebracht product met digitale elementen niet zodanig wijzigen dat de naleving van de toepasselijke vereisten in het gedrang komt of dat het beoogde doel waarvoor het product is beoordeeld, wordt gewijzigd.

(39) Net als bij fysieke reparaties of wijzigingen moet een product met digitale elementen worden beschouwd als ingrijpend gewijzigd door een softwarewijziging indien de software-update het beoogde doel van het product wijzigt en die wijzigingen niet in de initiële risicobeoordeling waren voorzien door de fabrikant, of indien de aard van het risico is gewijzigd of het niveau van het cyberbeveiligingsrisico is toegenomen als gevolg van de software-update, en

de bijgewerkte versie van het product op de markt is aangeboden. Wanneer een beveiligingsupdate die is ontworpen om het cyberbeveiligingsrisico van een product met digitale elementen te verminderen, het beoogde doel van een product met digitale elementen niet wijzigt, wordt hij niet als een ingrijpende wijziging beschouwd. Het gaat daarbij gewoonlijk om situaties waarin een beveiligingsupdate slechts kleine aanpassingen van de broncode met zich meebrengt. Dat kan bijvoorbeeld gebeuren wanneer een beveiligingsupdate betrekking heeft op een bekende kwetsbaarheid, onder meer wanneer de functies of prestaties van een product met digitale elementen worden gewijzigd met als enig doel het niveau van het cyberbeveiligingsrisico te verminderen. Evenzo mag een kleine functionaliteitsupdate, zoals een visuele verbetering, de toevoeging van nieuwe pictogrammen of talen aan de gebruikersinterface, over het algemeen niet als een ingrijpende wijziging worden beschouwd. Omgekeerd moet een kenmerkupdate die de oorspronkelijke beoogde functies, het type product of de prestaties van een product met digitale elementen wijzigt en aan de bovenvermelde criteria voldoet, als een ingrijpende wijziging worden beschouwd, aangezien de toevoeging van nieuwe kenmerken doorgaans het aanvalsoppervlak vergroten, waardoor het cyberbeveiligingsrisico toeneemt. Dat kan bijvoorbeeld het geval zijn wanneer een nieuw input-element aan een toepassing wordt toegevoegd, waardoor de fabrikant de input naar behoren moet valideren. Bij de beoordeling of een kenmerkupdate als een ingrijpende wijziging wordt beschouwd, is het niet relevant of die wordt verstrekt als een afzonderlijke update of in combinatie met een beveiligingsupdate. De Commissie moet richtsnoeren uitvaardigen over de manier waarop moet worden bepaald wat een ingrijpende wijziging inhoudt.

(40) Gezien het iteratieve karakter van softwareontwikkeling moeten fabrikanten die achtereenvolgens verschillende versies van een softwareproduct in de handel hebben gebracht als gevolg van een latere ingrijpende wijziging van dat product, tijdens de ondersteuningsperiode enkel beveiligingsupdates kunnen verstrekken voor de laatste in de handel gebrachte versie van het softwareproduct. Dat geldt alleen op voorwaarde dat de gebruikers van de relevante eerdere versies van het product in kwestie toegang hebben tot de laatste versie van het product die in de handel werd gebracht en geen extra kosten hoeven te maken om aanpassingen te doen aan de hardware- of softwareomgeving waarin zij het product gebruiken. Dat is bijvoorbeeld het geval wanneer het upgraden van een desktopbesturingssysteem geen nieuwe hardware, zoals een snellere centrale verwerkingseenheid of een groter geheugen, vereist. Tijdens de ondersteuningsperiode moet de fabrikant niettemin blijven voldoen aan andere vereisten inzake de respons op kwetsbaarheden en bijvoorbeeld over een beleid beschikken inzake de gecoördineerde bekendmaking van kwetsbaarheden of maatregelen om het delen van informatie over mogelijke kwetsbaarheden te vergemakkelijken voor alle versies van het in de handel gebrachte softwareproduct die ingrijpend zijn gewijzigd. Fabrikanten moeten enkel voor de meest recente versie of subversie van een softwareproduct dat niet ingrijpend is gewijzigd, kleine beveiligings- of functionaliteitsupdates kunnen verstrekken die geen ingrijpende wijziging vormen. Tegelijkertijd moet de fabrikant, wanneer een hardwareproduct zoals een smartphone niet compatibel is met de meest recente versie van het besturingssysteem waarmee het oorspronkelijk is geleverd, beveiligingsupdates blijven verstrekken tijdens de ondersteuningsperiode, ten minste voor de meest recente compatibele versie van het besturingssysteem.

(41) 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 digitale elementen met deze verordening, of wanneer het beoogde doel van dat product verandert. Indien de fabrikant een conformiteitsbeoordeling uitvoert waarbij een derde partij betrokken is, moet een wijziging die mogelijk ingrijpend is, in voorkomend geval aan de derde partij worden gemeld.

(42) Het "opknappen", het "onderhoud" en de "reparatie" als gedefinieerd in artikel 2, punten 18), 19) en 20), van Verordening (EU) 2024/1781 van het Europees Parlement en de Raad ([19]) van een product met digitale elementen, leidt niet noodzakelijkerwijs tot een ingrijpende wijziging van het product, bijvoorbeeld als het beoogde doel en de functies niet worden gewijzigd en het risiconiveau ongewijzigd blijft. De verbetering van een product met digitale elementen door de fabrikant kan echter leiden tot veranderingen in het ontwerp en de ontwikkeling van dat product en kan derhalve van invloed zijn op het beoogde doel en de conformiteit ervan met de vereisten van deze verordening.

(43) Producten met digitale elementen moeten als belangrijk worden beschouwd wanneer de negatieve gevolgen van het uitbuiten van potentiële kwetsbaarheden van het product ernstig kunnen zijn als gevolg van, onder meer, de aan cyberbeveiliging verbonden functionaliteit of een functie die een aanzienlijk risico op nadelige effecten inhoudt wat betreft de intensiteit ervan en het vermogen om een groot aantal andere producten of de gezondheid, beveiliging of veiligheid van gebruikers ervan te verstoren, controleren of beschadigen door directe manipulatie, zoals een centrale systeemfunctie, met inbegrip van netwerkbeheer, configuratiecontrole, virtualisering of verwerking van persoonsgegevens. Met name kunnen kwetsbaarheden in producten met digitale elementen met een aan cyberbeveiliging verbonden functionaliteit, zoals bootmanagers, leiden tot de verspreiding van veiligheidsproblemen

([19]) Verordening (EU) 2024/1781 van het Europees Parlement en de Raad van 13 juni 2024 betreffende de totstandbrenging van een kader voor het vaststellen van vereisten inzake ecologisch ontwerp voor duurzame producten, tot wijziging van Richtlijn (EU) 2020/1828 en Verordening (EU) 2023/1542, en tot intrekking van Richtlijn 2009/125/EG (PB L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

in de hele toeleveringsketen. De ernst van de gevolgen van een incident kan ook toenemen wanneer het product voornamelijk een centrale systeemfunctie uitvoert zoals netwerkbeheer, configuratiecontrole, virtualisering of verwerking van persoonsgegevens.

(44) Bepaalde categorieën producten met digitale elementen moeten aan strengere conformiteitsbeoordelingsprocedures worden onderworpen volgens een evenredige aanpak. Daartoe moeten belangrijke producten met digitale elementen in twee klassen worden ingedeeld, naargelang van het niveau van het cyberbeveiligingsrisico in verband met die productcategorieën. Een incident waarbij belangrijke producten met digitale elementen van klasse II betrokken zijn, kan grotere negatieve gevolgen hebben dan een incident met belangrijke producten met digitale elementen van klasse I, bijvoorbeeld vanwege de aard van hun aan cyberbeveiliging verbonden functie of omdat ze een andere functie vervullen die een aanzienlijk risico op nadelige effecten inhoudt. Als een indicatie van die grotere negatieve effecten kunnen producten met digitale elementen die onder klasse II vallen, ofwel een aan cyberbeveiliging verbonden functionaliteit vervullen of een andere functie vervullen die een aanzienlijk risico op nadelige effecten inhoudt dat hoger is dan die van klasse I, of aan beide voornoemde voorwaarden voldoen. Belangrijke producten met digitale elementen die onder klasse II vallen, moeten daarom worden onderworpen aan een strengere conformiteitsbeoordelingsprocedure.

(45) Belangrijke producten met digitale elementen als bedoeld in deze verordening moeten worden opgevat als producten die de kernfunctionaliteit hebben van een categorie belangrijke producten met digitale elementen die is opgenomen in deze verordening. In deze verordening worden bijvoorbeeld categorieën belangrijke producten met digitale elementen vastgesteld, die op basis van hun kernfunctionaliteit worden gedefinieerd als firewalls of inbraakdetectie- of inbraakpreventiesystemen van klasse II. Als gevolg daarvan zijn firewalls en inbraakdetectie- of inbraakpreventiesystemen onderworpen aan een verplichte conformiteitsbeoordeling door derden. Dat is niet het geval voor andere producten met digitale elementen die niet onder een categorie vallen van belangrijke producten met digitale elementen waarin firewalls of inbraakdetectie- of inbraakpreventiesystemen kunnen worden geïntegreerd. De Commissie moet een uitvoeringshandeling vaststellen tot nadere bepaling van de technische beschrijving van de categorieën belangrijke producten met digitale elementen die onder de in deze verordening beschreven klassen I en II vallen.

(46) De in deze verordening vastgestelde categorieën kritieke producten met digitale elementen hebben een aan cyberbeveiliging verbonden functionaliteit en vervullen een functie die een aanzienlijk risico op nadelige effecten inhoudt wat betreft de intensiteit ervan en het vermogen ervan om een groot aantal andere producten met digitale elementen te verstoren, te controleren of te beschadigen door directe manipulatie. Bovendien worden die categorieën producten met digitale elementen beschouwd als kritieke afhankelijkheden voor in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten. De categorieën kritieke producten met digitale elementen die in de bijlage bij deze verordening zijn opgenomen, maken vanwege hun kritieke karakter al op grote schaal gebruik van verschillende vormen van certificering en vallen ook onder de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) zoals beschreven in Uitvoeringsverordening (EU) 2024/482 van de Commissie ([20]). Om in de Unie te zorgen voor een gemeenschappelijke adequate bescherming van de cyberbeveiliging van kritieke producten met digitale elementen, kan het derhalve passend en evenredig zijn om dergelijke productcategorieën door middel van een gedelegeerde handeling te onderwerpen aan een verplichte Europese cyberbeveiligingscertificering, indien er reeds een relevante Europese cyberbeveiligingscertificeringsregeling voor die producten bestaat en de Commissie een beoordeling heeft verricht van de potentiële markteffecten van de beoogde verplichte certificering. Die beoordeling moet zowel de vraag- als de aanbodzijde in aanmerking nemen, en met name de vraag of zowel bij de lidstaten als bij de gebruikers voldoende vraag bestaat naar de betrokken producten met digitale elementen om een Europese cyberbeveiligingscertificering verplicht te stellen, alsook welke de doeleinden zijn waarvoor de producten met digitale elementen bestemd zijn om te worden gebruikt, met inbegrip van de kritieke afhankelijkheid van in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten ten aanzien van dergelijke producten. Ook moet bij de beoordeling een analyse worden gemaakt van de mogelijke gevolgen van de verplichte certificering voor de beschikbaarheid van die producten op de interne markt, alsook van de capaciteit en de bereidheid van de lidstaten om de relevante cyberbeveiligingscertificeringsregelingen uit te voeren.

(47) In gedelegeerde handelingen die een verplichte Europese cyberbeveiligingscertificering vereisen, moet worden bepaald welke producten met digitale elementen de kernfunctionaliteit hebben van een categorie kritieke producten met digitale elementen als beschreven in deze verordening die aan verplichte certificering moeten worden onderworpen, en moet het vereiste zekerheidsniveau worden vastgesteld, dat ten minste “substantieel” moet zijn. Het vereiste zekerheidsniveau moet in verhouding staan tot het niveau van het cyberbeveiligingsrisico dat aan het product met digitale elementen verbonden is. Wanneer het product met digitale elementen bijvoorbeeld de

([20]) Uitvoeringsverordening (EU) 2024/482 van de Commissie van 31 januari 2024 houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) (PB L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

kernfunctionaliteit heeft van een categorie kritieke producten met digitale elementen als beschreven in deze verordening, en bestemd is voor gebruik in een gevoelige of kritieke omgeving, zoals producten die bestemd zijn voor het gebruik door in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten, kan het hoogste zekerheidsniveau vereist worden.

(48) Om te zorgen voor een gemeenschappelijke adequate cyberbeveiliging in de Unie van producten met digitale elementen met de belangrijkste functionaliteit van een categorie kritieke producten met digitale elementen die is vastgesteld in deze verordening, moet de Commissie ook de bevoegdheid krijgen gedelegeerde handelingen vast te stellen om deze verordening te wijzigen, door categorieën kritieke producten met digitale elementen toe te voegen of te schrappen met betrekking waartoe van fabrikanten kan worden vereist dat zij een Europees cyberbeveiligingscertificaat verkrijgen in het kader van een Europese cyberbeveiligingscertificeringsregeling op grond van Verordening (EU) 2019/881 om aan te tonen dat zij aan deze verordening voldoen. Een nieuwe categorie kritieke producten met digitale elementen kan aan die categorieën worden toegevoegd als in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten er in kritieke mate van afhankelijk zijn, of als het gaat om een categorie producten waarvoor geldt dat, indien zij worden getroffen door incidenten of indien zij kwetsbaarheden bevatten die worden uitgebuit, dat kan leiden tot verstoringen van kritieke toeleveringsketens. Bij de beoordeling van de noodzaak om door middel van een gedelegeerde handeling categorieën kritieke producten met digitale elementen toe te voegen of te schrappen, moet de Commissie rekening kunnen houden met de vraag of de lidstaten op nationaal niveau producten met digitale elementen hebben geïdentificeerd die een cruciale rol spelen voor de veerkracht van in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten en die in toenemende mate getroffen worden door cyberaanvallen in de toeleveringsketen, met mogelijk ernstige verstorende effecten. Bovendien moet de Commissie rekening kunnen houden met de resultaten van de overeenkomstig artikel 22 van Richtlijn (EU) 2022/2555 verrichte op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.

(49) De Commissie dient ervoor te zorgen dat een breed scala aan relevante belanghebbenden regelmatig en op gestructureerde wijze wordt geraadpleegd bij de voorbereiding van maatregelen ter uitvoering van deze verordening. Dat dient met name het geval te zijn wanneer de Commissie beoordeelt of de lijsten van categorieën van belangrijke of kritieke producten met digitale elementen moeten worden bijgewerkt, waarbij relevante fabrikanten moeten worden geraadpleegd en hun standpunten in aanmerking moeten worden genomen om de cyberbeveiligingrisico's en de kosten-batenverhouding van het aanmerken van dergelijke categorieën producten als belangrijk of kritiek te analyseren.

(50) Deze verordening pakt cyberbeveiligingsrisico's op gerichte wijze aan. Producten met digitale elementen kunnen echter andere veiligheidsrisico's met zich meebrengen, die niet altijd verband houden met cyberbeveiliging maar een gevolg kunnen zijn van een inbreuk op de beveiliging. Die risico's moeten verder worden gereguleerd door andere relevante harmonisatiewetgeving van de Unie dan deze verordening. Indien geen andere harmonisatiewetgeving van de Unie dan deze verordening van toepassing is, moeten zij onder Verordening (EU) 2023/988 van het Europees Parlement en de Raad ([21]) 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 (EU) 2023/988, hoofdstuk III, deel 1, de hoofdstukken V en VII, en de hoofdstukken IX, X en XI van Verordening (EU) 2023/988 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 vereisten die zijn neergelegd in andere harmonisatiewetgeving van de Unie in de zin van artikel 3, punt 27, van Verordening (EU) 2023/988 dan deze verordening.

(51) Producten met digitale elementen die op grond van artikel 6 van Verordening (EU) 2024/1689 van het Europees Parlement en de Raad ([22]) als AI-systemen met een hoog risico worden aangemerkt en die binnen het toepassingsgebied van deze verordening vallen, moeten voldoen aan de essentiële cyberbeveiligingsvereisten van deze verordening. Wanneer die AI-systemen met een hoog risico aan de essentiële cyberbeveiligingsvereisten van deze verordening voldoen, moeten zij worden geacht in overeenstemming te zijn met de cyberbeveiligingsvereisten van artikel 15 van Verordening (EU) 2024/1689, voor zover die vereisten worden gedekt door de EU-conformiteitsverklaring, of delen daarvan, die uit hoofde van deze verordening is afgegeven. Daartoe moet bij de beoordeling van de cyberbeveiligingsrisico's in verband met een product met digitale elementen dat op grond van Verordening (EU) 2024/1689 als AI-systeem met een hoog risico wordt aangemerkt, waarmee rekening moet worden gehouden tijdens de plannings-, ontwerp-, ontwikkelings-, productie-, leverings- en onderhoudsfase van dat product, zoals vereist krachtens deze verordening, rekening worden gehouden met de risico's voor de cyberweerbaarheid van een AI-systeem ten gevolge van pogingen van onbevoegde derden om het gebruik, het gedrag of de prestaties van dat

([21]) Verordening (EU) 2023/988 van het Europees Parlement en de Raad van 10 mei 2023 inzake algemene productveiligheid, tot wijziging van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad en Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad, en tot intrekking van Richtlijn 2001/95/EG van het Europees Parlement en de Raad en Richtlijn 87/357/EEG van de Raad (PB L 135 van 23.5.2023, blz. 1).

([22]) Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

systeem te wijzigen, met inbegrip van AI-specifieke kwetsbaarheden zoals data poisoning of vijandige aanvallen, alsook, voor zover relevant, risico's voor de grondrechten, overeenkomstig Verordening (EU) 2024/1689. Wat betreft de conformiteitsbeoordelingsprocedures met betrekking tot de essentiële cyberbeveiligingsvereisten voor producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen en als een AI-systeem met een hoog risico worden aangemerkt, moet als regel artikel 43 van Verordening (EU) 2024/1689 worden toegepast in plaats van de relevante bepalingen van deze verordening. Die regel mag echter niet leiden tot een verlaging van het vereiste betrouwbaarheidsniveau voor belangrijke of kritieke producten met digitale elementen als bedoeld in deze verordening. Daarom moeten, in afwijking van die regel, AI-systemen met een hoog risico die binnen het toepassingsgebied van Verordening (EU) 2024/1689 vallen en die ook worden aangemerkt als belangrijke of kritieke producten met digitale elementen als bedoeld in deze verordening en waarop de conformiteitsbeoordelingsprocedure op basis van interne controle als bedoeld in bijlage VI bij Verordening (EU) 2024/1689 van toepassing is, onderworpen zijn aan de conformiteitsbeoordelingsprocedures die zijn voorzien in deze verordening wat de essentiële cyberbeveiligingsvereisten van deze verordening betreft. In een dergelijk geval moeten voor alle andere aspecten die onder Verordening (EU) 2024/1689 vallen, de relevante bepalingen inzake conformiteitsbeoordeling op basis van interne controle van bijlage VI bij die verordening van toepassing zijn.

(52) Om de beveiliging van producten met digitale elementen die op de interne markt worden gebracht, te verbeteren, is het noodzakelijk essentiële cyberbeveiligingsvereisten vast te stellen waaraan dergelijke producten moeten voldoen. Die essentiële cyberbeveiligingsvereisten mogen geen afbreuk doen aan de in artikel 22 van Richtlijn (EU) 2022/2555 bepaalde, op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens, waarbij rekening wordt gehouden met zowel technische als, voor zover relevant, niet-technische risicofactoren, zoals ongepaste beïnvloeding van leveranciers door een derde land. Voorts mogen ze geen afbreuk doen aan het prerogatief van de lidstaten om aanvullende vereisten 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 van de Commissie ([23]), in de gecoördineerde EU-risicobeoordeling van de cyberbeveiliging van 5G-netwerken en in het EU-instrumentarium voor 5G-cyberbeveiliging dat is overeengekomen door de op grond van artikel 14 van Richtlijn (EU) 2022/2555 opgerichte samenwerkingsgroep.

(53) Fabrikanten van producten die binnen het toepassingsgebied van Verordening (EU) 2023/1230 van het Europees Parlement en de Raad ([24]) vallen en die ook producten met digitale elementen zijn zoals gedefinieerd in deze verordening, moeten zowel aan de essentiële cyberbeveiligingsvereisten van deze verordening als aan de essentiële gezondheids- en veiligheidsvereisten van Verordening (EU) 2023/1230 voldoen. De essentiële cyberbeveiligingsvereisten van deze verordening en bepaalde essentiële vereisten van Verordening (EU) 2023/1230 kunnen wellicht betrekking hebben op soortgelijke cyberbeveiligingsrisico's. Daarom kan de naleving van de essentiële cyberbeveiligingsvereisten van deze verordening de naleving van de essentiële vereisten met betrekking tot bepaalde cyberbeveiligingsrisico's zoals vastgesteld in Verordening (EU) 2023/1230 vergemakkelijken, en met name de vereisten met betrekking tot de bescherming tegen corruptie en met betrekking tot de veiligheid en betrouwbaarheid van de besturingssystemen als beschreven in de punten 1.1.9 en 1.2.1 van bijlage III bij die verordening. Dergelijke synergieën moeten door de fabrikant worden aangetoond, bijvoorbeeld door na een risicobeoordeling van die cyberbeveiligingsrisico's, indien beschikbaar, geharmoniseerde normen of andere technische specificaties toe te passen die betrekking hebben op relevante essentiële cyberbeveiligingsvereisten. De fabrikant moet ook de in deze verordening en in Verordening (EU) 2023/1230 beschreven toepasselijke conformiteitsbeoordelingsprocedures volgen. De Commissie en de Europese normalisatieorganisaties moeten bij de voorbereidende werkzaamheden ter ondersteuning van de uitvoering van deze verordening en van Verordening (EU) 2023/1230 en de daarmee verband houdende normalisatieprocessen consistentie bevorderen in de wijze waarop de cyberbeveiligingsrisico's moeten worden beoordeeld en in de wijze waarop die risico's moeten worden afgedekt door geharmoniseerde normen met betrekking tot de relevante essentiële vereisten. De Commissie en de Europese normalisatieorganisaties moeten deze verordening met name in aanmerking nemen bij de voorbereiding en ontwikkeling van geharmoniseerde normen om de uitvoering van Verordening (EU) 2023/1230 te vergemakkelijken, met name wat betreft de cyberbeveiligingsaspecten die verband houden met de bescherming tegen corruptie en de veiligheid en betrouwbaarheid van de besturingssystemen als beschreven in de punten 1.1.9 en 1.2.1 van bijlage III bij die verordening. De Commissie moet richtsnoeren opstellen ter ondersteuning van fabrikanten die onder deze verordening vallen en die ook onder Verordening (EU) 2023/1230 vallen, met name om het aantonen van overeenstemming met de relevante essentiële vereisten van deze verordening en van Verordening (EU) 2023/1230 te vergemakkelijken.

(54) Om ervoor te zorgen dat producten met digitale elementen zowel bij het in de handel brengen als gedurende de tijd dat het product met digitale elementen naar verwachting in gebruik zal zijn, beveiligd zijn, moeten essentiële cyberbeveiligingsvereisten inzake de respons op kwetsbaarheden en essentiële cyberbeveiligingsvereisten met betrekking tot de kenmerken van producten met digitale elementen worden vastgesteld. Fabrikanten moeten voldoen

([23]) Aanbeveling (EU) 2019/534 van de Commissie van 26 maart 2019 — Cyberbeveiliging van 5G-netwerken (PB L 88 van 29.3.2019, blz. 42).

([24]) Verordening (EU) 2023/1230 van het Europees Parlement en de Raad van 14 juni 2023 betreffende machines en tot intrekking van Richtlijn 2006/42/EG van het Europees Parlement en de Raad en Richtlijn 73/361/EEG van de Raad (PB L 165 van 29.6.2023, blz. 1).

aan alle essentiële cyberbeveiligingsvereisten in verband met de respons op kwetsbaarheden tijdens de hele ondersteuningsperiode en moeten ook bepalen welke andere essentiële cyberbeveiligingsvereisten met betrekking tot de productkenmerken relevant zijn voor het betrokken type product met digitale elementen. Daartoe moeten fabrikanten de cyberbeveiligingsrisico's beoordelen die verbonden zijn aan een product met digitale elementen, om relevante risico's en relevante essentiële cyberbeveiligingsvereisten vast te stellen, opdat zij hun producten kunnen leveren zonder bekende uitbuitbare kwetsbaarheden die gevolgen kunnen hebben voor de beveiliging van die producten, en om op correcte wijze toepassing te geven aan passende geharmoniseerde normen, gemeenschappelijke specificaties of Europese of internationale normen.

(55) Indien bepaalde essentiële cyberbeveiligingsvereisten niet van toepassing zijn op een product met digitale elementen, moet de fabrikant een duidelijke motivering opnemen in de beoordeling van de cyberbeveiligingsrisico's die deel uitmaakt van de technische documentatie. Dat kan het geval zijn wanneer een essentiële cyberbeveiligingsvereiste onverenigbaar is met de aard van een product met digitale elementen. Zo kan het vanwege het beoogde doel van een product met digitale elementen noodzakelijk zijn dat de fabrikant algemeen erkende interoperabiliteitsnormen volgt, ook al worden de beveiligingskenmerken ervan niet langer als de stand van de techniek beschouwd. Ook kunnen fabrikanten op grond van ander Unierecht verplicht zijn om specifieke interoperabiliteitsvereisten toe te passen. Wanneer een essentiële cyberbeveiligingsvereiste niet van toepassing is op een product met digitale elementen, maar de fabrikant cyberbeveiligingsrisico's in verband met die essentiële cyberbeveiligingsvereiste heeft vastgesteld, moet hij maatregelen nemen om die risico's met andere middelen aan te pakken, bijvoorbeeld door het beoogde doel van het product te beperken tot betrouwbare omgevingen of door de gebruikers over die risico's te informeren.

(56) Een van de belangrijkste maatregelen die gebruikers moeten nemen om hun producten met digitale elementen tegen cyberaanvallen te beschermen, is het zo snel mogelijk installeren van de meest recente beveiligingsupdates. Fabrikanten moeten daarom hun producten op zodanige wijze ontwerpen dat producten met digitale elementen, en met name consumentenproducten, functies omvatten die het automatisch melden, verspreiden, downloaden en installeren van beveiligingsupdates mogelijk maken, en zij moeten daarvoor processen invoeren. Zij moeten ook de mogelijkheid bieden dat goedkeuring door de gebruiker als laatste stap nodig is om beveiligingsupdates te downloaden en te installeren. Gebruikers moeten de mogelijkheid blijven houden om automatische updates te deactiveren door middel van een duidelijk en gebruiksvriendelijk mechanisme, met duidelijke instructies over de manier waarop zij dat kunnen doen. De in een bijlage bij deze verordening vastgestelde vereisten met betrekking tot automatische updates zijn niet van toepassing op producten met digitale elementen die hoofdzakelijk bestemd zijn om als onderdeel in andere producten te worden geïntegreerd. Zij zijn evenmin van toepassing op producten met digitale elementen waarvan gebruikers redelijkerwijs geen automatische updates zouden verwachten, waaronder producten met digitale elementen die bedoeld zijn om te worden gebruikt in professionele ICT-netwerken, en met name in kritieke en industriële omgevingen waar een automatische update de activiteiten zou kunnen verstoren. Ongeacht of een product met digitale elementen is ontworpen om automatische updates te verkrijgen, moet de fabrikant gebruikers informeren over kwetsbaarheden en moet hij beveiligingsupdates onverwijld beschikbaar stellen. Wanneer een product met digitale elementen een gebruikersinterface of een soortgelijk technisch middel heeft dat directe interactie met zijn gebruikers mogelijk maakt, moet de fabrikant dergelijke functies gebruiken om, als het product met digitale elementen het einde van de ondersteuningsperiode heeft bereikt, gebruikers daarvan in kennis te stellen. Meldingen moeten beperkt blijven tot hetgeen nodig is om de doeltreffende ontvangst van die informatie te waarborgen en mogen geen negatieve gevolgen hebben voor de gebruikerservaring van het product met digitale elementen.

(57) Om de transparantie van de procedures inzake de respons op kwetsbaarheden te verbeteren en ervoor te zorgen dat gebruikers geen nieuwe functionaliteitsupdates hoeven te installeren met als enig doel de meest recente beveiligingsupdates te verkrijgen, moeten fabrikanten ervoor zorgen dat, indien technisch haalbaar, nieuwe beveiligingsupdates los van de functionaliteitsupdates worden aangeboden.

(58) In de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 20 juni 2023 betreffende een "Strategie voor economische veiligheid van de EU" wordt gesteld dat de Unie de voordelen van haar economische openheid moet maximaliseren en tegelijkertijd de risico's van economische afhankelijkheid van leveranciers met een hoog risico tot een minimum moet beperken door middel van een gemeenschappelijk strategisch kader voor de economische veiligheid van de Unie. Afhankelijkheid van leveranciers van producten met digitale elementen met een hoog risico kan een strategisch risico vormen dat op het niveau van de Unie moet worden aangepakt, met name wanneer de producten met digitale elementen bestemd zijn voor gebruik door in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten. Dergelijke risico's kunnen verband houden met, onder meer, de jurisdictie waaronder de fabrikant valt, de kenmerken van de bedrijfseigendom en de uitoefening van zeggenschap door de overheid van het derde land waar de fabrikant gevestigd is, met name wanneer een derde land zich bezighoudt met economische spionage of onverantwoordelijke overheidsgedragingen in de cyberruimte en de wetgeving van het land willekeurige toegang biedt tot alle soorten bedrijfsactiviteiten of -gegevens, waaronder commercieel gevoelige gegevens, en verplichtingen kan opleggen voor inlichtingendoeleinden zonder democratische checks-and-balances, toezichtmechanismen, eerlijke rechtsgang of het recht om beroep in te stellen bij een onafhankelijke rechterlijke instantie. Bij het bepalen van de significantie van een cyberbeveiligingsrisico in de zin van deze verordening moeten de Commissie en de markttoezichtautoriteiten, overeenkomstig hun verantwoordelijkheden zoals vastgelegd in deze verordening, ook niet-technische risicofactoren

in aanmerking nemen, met name die welke zijn vastgesteld als gevolg van overeenkomstig artikel 22 van Richtlijn (EU) 2022/2555 uitgevoerde op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.

(59) Met het oog op het waarborgen van de beveiliging van producten met digitale elementen nadat zij in de handel zijn gebracht, moeten fabrikanten de ondersteuningsperiode vaststellen, die de tijd moet weerspiegelen dat het product met digitale elementen naar verwachting in gebruik zal zijn. Bij het bepalen van een ondersteuningsperiode moet een fabrikant met name rekening houden met redelijke verwachtingen van gebruikers, de aard van het product en het relevante Unierecht dat de levensduur van producten met digitale elementen bepaalt. Fabrikanten moeten ook rekening kunnen houden met andere relevante factoren. Criteria moeten zodanig worden toegepast dat de evenredigheid bij de vaststelling van de ondersteuningsperiode wordt gewaarborgd. Fabrikanten moeten de markttoezichtautoriteiten op verzoek de informatie verstrekken die in aanmerking is genomen om de ondersteuningsperiode van een product met digitale elementen te bepalen.

(60) De ondersteuningsperiode gedurende welke de fabrikant de doeltreffende respons op kwetsbaarheden waarborgt, mag niet korter zijn dan vijf jaar, tenzij de levensduur van het product met digitale elementen korter dan vijf jaar is, in welk geval de fabrikant de respons op kwetsbaarheden gedurende die levensduur moet waarborgen. Wanneer redelijkerwijs kan worden verwacht dat het product met digitale elementen langer dan vijf jaar zal worden gebruikt, zoals vaak het geval is bij hardwarecomponenten zoals moederborden of microprocessors, netwerkapparatuur zoals routers, modems of netwerkswitches, alsook software zoals besturingssystemen of video-editingprogramma's, moeten fabrikanten zorgen voor langere ondersteuningsperioden die daarbij aansluiten. Met name producten met digitale elementen die bestemd zijn voor gebruik in industriële omgevingen, zoals industriële besturingssystemen, worden vaak gedurende aanzienlijk langere tijd gebruikt. Het moet fabrikanten alleen worden toegestaan een ondersteuningsperiode van korter dan vijf jaar vast te stellen indien de aard van het product met digitale elementen dat rechtvaardigt en indien dat product naar verwachting korter dan vijf jaar zal worden gebruikt, in welk geval de ondersteuningsperiode moet overeenstemmen met de verwachte gebruikstijd. Zo kan de ondersteuningsperiode van een contacttraceringsapplicatie die bedoeld is om tijdens een pandemie te worden gebruikt, worden beperkt tot de duur van de pandemie. Bovendien kunnen bepaalde softwaretoepassingen door hun aard alleen op basis van een abonnementsmodel beschikbaar worden gesteld, met name wanneer de applicatie, zodra het abonnement verstrijkt, niet meer beschikbaar is voor de gebruiker en bijgevolg niet meer wordt gebruikt.

(61) Fabrikanten moeten overwegen om na afloop van de ondersteuningsperiode van producten met digitale elementen de broncode van die producten vrij te geven aan het publiek of aan andere ondernemingen die zich ertoe verbinden de dienstverlening in verband met de respons op kwetsbaarheden op zich te nemen, om ervoor te zorgen dat kwetsbaarheden na afloop van de ondersteuningsperiode kunnen worden verholpen. Wanneer fabrikanten de broncode vrijgeven aan andere ondernemingen, moeten zij de eigendomsrechten van het product met digitale elementen kunnen beschermen en moeten zij kunnen voorkomen dat de broncode wordt vrijgegeven aan het publiek, bijvoorbeeld door dat contractueel vast te leggen.

(62) Om te waarborgen dat fabrikanten in de hele Unie voor vergelijkbare producten met digitale elementen soortgelijke ondersteuningsperioden vaststellen, moet de ADCO statistieken publiceren over de gemiddelde ondersteuningsperioden die fabrikanten hebben vastgesteld voor categorieën producten met digitale elementen, en moet de ADCO richtsnoeren verstrekken voor de vaststelling van passende ondersteuningsperioden voor de verschillende categorieën. Om een geharmoniseerde aanpak in de hele interne markt te waarborgen, moet de Commissie voorts gedelegeerde handelingen kunnen vaststellen ter vaststelling van minimumondersteuningsperioden voor specifieke productcategorieën, als uit de door markttoezichtautoriteiten verstrekte gegevens blijkt dat fabrikanten systematisch ondersteuningsperioden vaststellen die niet in overeenstemming zijn met de in deze verordening vastgestelde criteria voor het vaststellen van ondersteuningsperioden of dat fabrikanten in verschillende lidstaten op ongerechtvaardigde wijze uiteenlopende ondersteuningsperioden vaststellen.

(63) Fabrikanten moeten een centraal contactpunt opzetten dat gebruikers in staat stelt gemakkelijk met hen te communiceren, onder meer om melding te doen van kwetsbaarheden van producten met digitale elementen of om informatie over kwetsbaarheden van producten met digitale elementen te verkrijgen. Fabrikanten moeten ervoor zorgen dat het centrale contactpunt gemakkelijk toegankelijk is voor gebruikers, moeten het centrale contactpunt onder de aandacht brengen en moeten ervoor zorgen dat informatie ter zake actueel is. Als fabrikanten ervoor kiezen geautomatiseerde hulpmiddelen, zoals een chatbox, beschikbaar te stellen, moeten zij ook een telefoonnummer of een andere digitale contactmogelijkheid bieden, zoals een e-mailadres of een contactformulier. Het centrale contactpunt mag niet uitsluitend gebruikmaken van geautomatiseerde hulpmiddelen.

(64) Fabrikanten moeten hun producten met digitale elementen op de markt aanbieden met een standaard beveiligde configuratie en moeten gebruikers kosteloos beveiligingsupdates verstrekken. Fabrikanten mogen alleen van de essentiële cyberbeveiligingsvereisten afwijken in geval van producten op maat die voor een bepaalde zakelijke gebruiker en een bepaald doel zijn gemaakt, en waarbij zowel de fabrikant als de gebruiker uitdrukkelijk heeft ingestemd met andere contractuele voorwaarden.

(65) Fabrikanten moeten, via het centrale meldingsplatform, tegelijkertijd aan het als coördinator aangewezen computer security incident response team (CSIRT) en aan Enisa melding doen van actief uitgebuite kwetsbaarheden in producten met digitale elementen en ernstige incidenten die gevolgen hebben voor de beveiliging van die producten. De meldingen moeten worden gedaan via het elektronisch endpoint voor melding van een als coördinator aangewezen CSIRT en moeten tegelijkertijd toegankelijk zijn voor Enisa.

(66) Fabrikanten moeten melding doen van actief uitgebuite kwetsbaarheden om ervoor te zorgen dat de als coördinatoren aangewezen CSIRT's en Enisa een goed overzicht hebben van dergelijke kwetsbaarheden en de informatie krijgen die zij nodig hebben om hun taken uit hoofde van Richtlijn (EU) 2022/2555 te vervullen en het algemene niveau van cyberbeveiliging van in artikel 3 van die richtlijn bedoelde essentiële en belangrijke entiteiten te verhogen, alsook om de doeltreffende werking van markttoezichtautoriteiten te waarborgen. Aangezien de meeste producten met digitale elementen op de hele interne markt in de handel worden gebracht, moet elke uitgebuite kwetsbaarheid in een product met digitale elementen worden beschouwd als een bedreiging voor de werking van de interne markt. Enisa moet, na overleg met de fabrikant, verholpen kwetsbaarheden openbaar maken in de Europese kwetsbaarheidsdatabase die is opgezet op grond van artikel 12, lid 2, van Richtlijn (EU) 2022/2555. De Europese kwetsbaarheidsdatabase zal fabrikanten helpen bekende uitbuitbare kwetsbaarheden in hun producten op te sporen, om ervoor te zorgen dat de producten die op de markt worden aangeboden, veilig zijn.

(67) Fabrikanten moeten eveneens aan het als coördinator aangewezen CSIRT en aan Enisa melding doen van elk ernstig incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen. Om ervoor te zorgen dat gebruikers snel kunnen reageren op ernstige 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 cyberbeveiligingsrisico's dat rechtvaardigen, door rechtstreeks contact met de gebruikers op te nemen.

(68) Bij actief uitgebuite kwetsbaarheden gaat het om gevallen waarin een fabrikant vaststelt dat een inbreuk op de beveiliging met gevolgen voor gebruikers of andere natuurlijke of rechtspersonen het gevolg is van gebruikmaking door een kwaadwillige actor van een tekortkoming in een van de producten met digitale elementen die door de fabrikant op de markt worden aangeboden. Voorbeelden van dergelijke kwetsbaarheden zijn tekortkomingen in de identificatie- of de authenticatiefunctie van een product. Voor kwetsbaarheden die worden ontdekt zonder kwaadwillige bedoelingen, met het oog op het te goeder trouw testen, onderzoeken, corrigeren of bekendmaken ervan, met de bedoeling om de beveiliging of veiligheid van de eigenaar van het systeem en de gebruikers ervan te waarborgen, mag niet de verplichting gelden dat daarvan melding moet worden gedaan. Bij ernstige incidenten die gevolgen hebben voor de beveiliging van het product met digitale elementen gaat het om situaties waarin een cyberbeveiligingsincident zodanige gevolgen heeft voor het ontwikkelings-, productie- of onderhoudsproces van de fabrikant dat er een verhoogd cyberbeveiligingsrisico voor gebruikers of andere personen kan ontstaan. Bij een dergelijk ernstig incident kan het gaan om een situatie waarin een aanvaller met succes een kwaadwillige code heeft ingevoerd in het kanaal dat de fabrikant gebruikt om beveiligingsupdates aan gebruikers te verstrekken.

(69) Om ervoor te zorgen dat meldingen snel onder alle relevante als coördinatoren aangewezen CSIRT's kunnen worden verspreid en om fabrikanten in staat te stellen in elke fase van het meldingsproces één enkele melding in te dienen, moet Enisa een centraal meldingsplatform met nationale elektronische endpoints voor melding oprichten. De dagelijkse werkzaamheden van het centrale meldingsplatform moeten worden beheerd en uitgevoerd door Enisa. De als coördinatoren aangewezen CSIRT's moeten hun respectieve markttoezichtautoriteiten informeren over kwetsbaarheden of incidenten waarvan melding is gedaan. Het centrale meldingsplatform moet zodanig van opzet zijn dat de vertrouwelijkheid van meldingen wordt gewaarborgd, met name als die meldingen betrekking hebben op kwetsbaarheden waarvoor nog geen beveiligingsupdate beschikbaar is. Daarnaast moet Enisa procedures invoeren om te waarborgen dat informatie op een veilige en vertrouwelijke manier wordt behandeld. 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 dat verslag voorleggen aan de op grond van artikel 14 van Richtlijn (EU) 2022/2555 opgerichte samenwerkingsgroep.

(70) In uitzonderlijke omstandigheden, en met name op verzoek van de fabrikant, moet het als coördinator aangewezen CSIRT dat als eerste een melding ontvangt, kunnen besluiten de verspreiding ervan aan de andere relevante als coördinatoren aangewezen CSIRT's via het centrale meldingsplatform uit te stellen indien dat gerechtvaardigd is om redenen in verband met cyberbeveiliging en slechts zolang dat strikt noodzakelijk is. Het als coördinator aangewezen CSIRT moet Enisa onmiddellijk in kennis stellen van het besluit om de verspreiding uit te stellen, onder vermelding van de redenen daarvoor, en tevens aangeven wanneer het voornemens is de melding verder te verspreiden. De Commissie moet door middel van een gedelegeerde handeling specificeren wat de voorwaarden zijn waaronder die cyberbeveiligingsgerelateerde redenen een rechtvaardiging vormen voor uitstel en moet bij het opstellen van het ontwerp van gedelegeerde handeling samenwerken met het op grond van artikel 15 van Richtlijn (EU) 2022/2555 opgerichte CSIRT-netwerk en met Enisa. Voorbeelden van cyberbeveiligingsgerelateerde redenen zijn onder meer een lopende procedure voor gecoördineerde bekendmaking van kwetsbaarheden of situaties waarin een fabrikant naar verwachting op korte termijn een risicobeperkende maatregel zal nemen en de cyberbeveiligingsrisico's van onmiddellijke verspreiding via het centrale meldingsplatform zwaarder wegen dan de voordelen ervan. Op verzoek

van het als coördinator aangewezen CSIRT moet Enisa dat CSIRT kunnen ondersteunen bij de toepassing van cyberbeveiligingsgerelateerde redenen voor het uitstel van de verspreiding van de melding, op basis van de informatie die Enisa van dat CSIRT heeft ontvangen over het besluit om de melding om die cyberbeveiligingsgerelateerde redenen niet verder te verspreiden. Daarnaast moet vastgelegd worden dat Enisa in zeer uitzonderlijke omstandigheden niet alle details van een melding van een actief uitgebuite kwetsbaarheid gelijktijdig mag ontvangen. Dat is het geval wanneer de fabrikant in zijn melding vermeldt dat de kwetsbaarheid waarvan melding wordt gedaan actief is uitgebuit door een kwaadwillige actor en dat de kwetsbaarheid, volgens de beschikbare informatie, in geen enkele andere lidstaat is uitgebuit dan de lidstaat van het als coördinator aangewezen CSIRT waaraan de fabrikant de kwetsbaarheid heeft gemeld, wanneer onmiddellijke verdere verspreiding van de melding van de kwetsbaarheid naar verwachting zou leiden tot verstrekking van informatie waarvan de openbaarmaking in strijd zou zijn met de wezenlijke belangen van die lidstaat, of wanneer verdere verspreiding van de melding een hoog cyberbeveiligingsrisico inhoudt. In dergelijke gevallen krijgt Enisa alleen gelijktijdig toegang tot de informatie dat de fabrikant een melding heeft gedaan, algemene informatie over het betrokken product met digitale elementen, de informatie over de algemene aard van de uitbuiting en de informatie dat er door de fabrikant beveiligingsgerelateerde redenen zijn aangevoerd en dat de volledige inhoud van de melding derhalve nog niet wordt gedeeld. De volledige melding moet vervolgens ter beschikking worden gesteld van Enisa en andere relevante als coördinatoren aangewezen CSIRT's wanneer het als coördinator aangewezen CSIRT die de melding als eerste ontvangt, vaststelt dat die beveiligingsgerelateerde redenen waarom er sprake was van zeer uitzonderlijke omstandigheden zoals vastgelegd in deze verordening, niet meer bestaan. Indien Enisa op basis van de beschikbare informatie van oordeel is dat er een systeemrisico bestaat met gevolgen voor de veiligheid op de interne markt, moet Enisa het ontvangende CSIRT aanbevelen de volledige melding onder de andere als coördinatoren aangewezen CSIRT's en Enisa zelf te verspreiden.

(71) Wanneer fabrikanten melding doen van een actief uitgebuite kwetsbaarheid of een ernstig incident met gevolgen voor de beveiliging van het product met digitale elementen, moeten zij aangeven hoe gevoelig de informatie waarvan zij melding doen volgens hen is. Het als coördinator aangewezen CSIRT dat de melding als eerste ontvangt, moet die informatie in aanmerking nemen bij de beoordeling van de vraag of er in verband met de melding sprake is van uitzonderlijke omstandigheden die uitstel van de verspreiding van de melding onder de andere relevante als coördinatoren aangewezen CSIRT's om cyberbeveiligingsgerelateerde redenen rechtvaardigen. Zij moet die informatie ook in aanmerking nemen bij de beoordeling van de vraag of er in verband met de melding van een actief uitgebuite kwetsbaarheid sprake is van zeer uitzonderlijke omstandigheden die rechtvaardigen dat de volledige melding niet gelijktijdig aan Enisa ter beschikking wordt gesteld. Tot slot moeten de als coördinatoren aangewezen CSIRT's die informatie in aanmerking kunnen nemen bij het vaststellen van passende maatregelen om de risico's die voortvloeien uit dergelijke kwetsbaarheden en incidenten, te beperken.

(72) Om de verstrekking van de krachtens deze verordening vereiste informatie te vereenvoudigen, in het licht van andere rapportageverplichtingen die zijn vastgelegd in het Unierecht, zoals Verordening (EU) 2016/679, Verordening (EU) 2022/2554 van het Europees Parlement en de Raad ([25]), Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([26]) en Richtlijn (EU) 2022/2555, en om de administratieve lasten voor entiteiten te verminderen, worden de lidstaten aangespoord te overwegen op nationaal niveau te voorzien in centrale contactpunten voor dergelijke rapportageverplichtingen. Het gebruik van dergelijke centrale contactpunten voor de melding van beveiligingsincidenten krachtens Verordening (EU) 2016/679 en Richtlijn 2002/58/EG mag geen afbreuk doen aan de toepassing van de bepalingen van Verordening (EU) 2016/679 en Richtlijn 2002/58/EG, en met name de bepalingen met betrekking tot de onafhankelijkheid van de daarin bedoelde autoriteiten. Bij de oprichting van het in deze verordening bedoelde centrale meldingsplatform moet Enisa rekening houden met de mogelijkheid dat de in deze verordening bedoelde nationale elektronische endpoints voor melding worden geïntegreerd in nationale centrale contactpunten die ook gebruikt kunnen worden voor andere uit hoofde van het Unierecht vereiste meldingen.

(73) Bij de oprichting van het in deze verordening bedoelde centrale meldingsplatform moet Enisa overleg plegen met andere instellingen of agentschappen van de Unie die platforms of databanken beheren waarvoor strenge beveiligingverseisten gelden, zoals het Agentschap van de Europese Unie voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA), om van de ervaringen die zij reeds hebben opgedaan te kunnen profiteren. Enisa moet ook mogelijke complementariteiten met de Europese kwetsbaarheidsdatabase die is opgezet op grond van artikel 12, lid 2, van Richtlijn (EU) 2022/2555, analyseren.

(74) Fabrikanten en andere natuurlijke en rechtspersonen moeten aan een als coördinator aangewezen CSIRT of aan Enisa op vrijwillige basis melding kunnen doen van kwetsbaarheden in een product met digitale elementen,

([25]) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).

([26]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (PB L 201 van 31.7.2002, blz. 37).

cyberdreigingen die van invloed kunnen zijn op het risicoprofiel van een product met digitale elementen, incidenten die gevolgen hebben voor de beveiliging van het product met digitale elementen en bijna-incidenten die tot een dergelijk incident hadden kunnen leiden.

(75) De lidstaten moeten ernaar streven zo veel mogelijk de problemen weg te nemen waar onderzoekers van kwetsbaarheden mee worden geconfronteerd, waaronder hun mogelijke blootstelling aan strafrechtelijke aansprakelijkheid, overeenkomstig het nationale recht. Aangezien natuurlijke en rechtspersonen die onderzoek doen naar kwetsbaarheden in sommige lidstaten strafrechtelijk en civielrechtelijk aansprakelijk kunnen worden gesteld, worden de lidstaten aangespoord richtsnoeren vast te stellen met betrekking tot niet-vervolging van onderzoekers op het gebied van informatiebeveiliging en vrijstelling van civielrechtelijke aansprakelijkheid voor hun activiteiten.

(76) Fabrikanten van producten met digitale elementen moeten een gecoördineerd beleid inzake openbaarmaking van kwetsbaarheden invoeren ter vergemakkelijking van de melding van kwetsbaarheden door personen of entiteiten, hetzij direct aan de fabrikant, hetzij indirect, en op verzoek anoniem, via CSIRT's die zijn aangewezen als coördinatoren ten behoeve van de gecoördineerde bekendmaking van kwetsbaarheden overeenkomstig artikel 12, lid 1, van Richtlijn (EU) 2022/2555. In het beleid van fabrikanten 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 die 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. Bovendien moeten fabrikanten ook overwegen hun beveiligingsbeleid in een machineleesbaar formaat te publiceren. Aangezien informatie over uitbuitbare kwetsbaarheden 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. Daarmee worden zogeheten "bug bounty"-programma's bedoeld.

(77) 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 cyberbeveiligingsrisico's op te sporen. Het is bijzonder belangrijk dat fabrikanten ervoor zorgen dat hun producten met digitale elementen geen kwetsbare componenten bevatten die door derden zijn ontwikkeld. Fabrikanten mogen niet worden verplicht de softwarestuklijst openbaar te maken.

(78) In het kader van de nieuwe complexe bedrijfsmodellen die verband houden met onlineverkopen kan een bedrijf dat online actief is een verscheidenheid aan diensten aanbieden. Afhankelijk van de aard van de diensten die met betrekking tot een bepaald product met digitale elementen worden verleend, kan dezelfde entiteit onder verschillende categorieën bedrijfsmodellen of marktdeelnemers vallen. Wanneer een entiteit voor een bepaald product met digitale elementen alleen onlinetussenhandelsdiensten aanbiedt en slechts een aanbieder van een onlinemarktplaats is zoals gedefinieerd in artikel 3, punt 14), van Verordening (EU) 2023/988, wordt zij niet aangemerkt als een van de in deze verordening gedefinieerde soorten marktdeelnemers. Wanneer dezelfde entiteit een aanbieder van een onlinemarktplaats is en ook optreedt als marktdeelnemer zoals gedefinieerd in deze verordening voor de verkoop van bepaalde producten met digitale elementen, moet zij onderworpen zijn aan de in deze verordening vastgestelde verplichtingen voor dat type marktdeelnemer. Als de aanbieder van een onlinemarktplaats bijvoorbeeld ook een product met digitale elementen distribueert, dan zou die aanbieder wat betreft de verkoop van dat product als distributeur worden beschouwd. Op dezelfde wijze geldt dat als de betrokken entiteit haar eigen merkproducten met digitale elementen verkoopt, die entiteit aangemerkt wordt als fabrikant en dus moet voldoen aan de toepasselijke vereisten voor fabrikanten. Ook kunnen sommige entiteiten worden aangemerkt als fulfilmentdienstverleners zoals gedefinieerd in artikel 3, punt 11), van Verordening (EU) 2019/1020 van het Europees Parlement en de Raad ([27]) indien zij dergelijke diensten aanbieden. Dergelijke gevallen moeten per geval worden beoordeeld. Gezien de belangrijke rol die onlinemarktplaatsen spelen bij het mogelijk maken van elektronische handel, moeten zij ernaar streven samen te werken met de markttoezichtautoriteiten van de lidstaten om ervoor te zorgen dat producten met digitale elementen die via onlinemarktplaatsen worden gekocht, voldoen aan de cyberbeveiligingsvereisten van deze verordening.

(79) 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 cyberbeveiligingsvereisten van deze verordening omzetten in gedetailleerde technische specificaties, en die zijn vastgesteld overeenkomstig Verordening (EU) nr. 1025/2012

([27]) 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).

van het Europees Parlement en de Raad ([28]). Die verordening voorziet in een procedure voor bezwaren tegen geharmoniseerde normen die niet volledig aan de vereisten van deze verordening voldoen. Het normalisatieproces moet een evenwichtige vertegenwoordiging van belangen en doeltreffende participatie van belanghebbenden uit het maatschappelijk middenveld, met inbegrip van consumentenorganisaties, waarborgen. Ook internationale normen die in overeenstemming zijn met het niveau van cyberbeveiliging dat met de essentiële cyberbeveiligingsvereisten van deze verordening wordt beoogd, moeten in aanmerking worden genomen, teneinde de ontwikkeling van geharmoniseerde normen en de uitvoering van deze verordening te vergemakkelijken en de naleving door ondernemingen, met name micro-ondernemingen en kleine en middelgrote ondernemingen en ondernemingen die wereldwijd actief zijn, te vergemakkelijken.

(80) Met het oog op de doeltreffende uitvoering van deze verordening is het met name belangrijk dat tijdens de overgangsperiode voor de toepassing van deze verordening tijdig geharmoniseerde normen worden ontwikkeld en dat die beschikbaar zijn vóór de datum van toepassing van deze verordening. Dat geldt met name voor belangrijke producten met digitale elementen die vallen onder klasse I. De beschikbaarheid van geharmoniseerde normen zal fabrikanten van dergelijke producten in staat stellen om de conformiteitsbeoordelingen uit te voeren via de procedure voor interne controle, waardoor knelpunten en vertragingen in de activiteiten van conformiteitsbeoordelingsinstanties kunnen worden voorkomen.

(81) Bij Verordening (EU) 2019/881 is een vrijwillig Europees kader voor cyberbeveiligingscertificering voor ICT-producten, -processen en -diensten vastgesteld. Europese cyberbeveiligingscertificeringsregelingen bieden gebruikers een gemeenschappelijk vertrouwenskader voor het gebruik van producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen. Deze verordening moet bijgevolg synergieën tot stand brengen met Verordening (EU) 2019/881. Om de beoordeling van de conformiteit met de vereisten van deze verordening te vergemakkelijken, worden producten met digitale elementen die zijn gecertificeerd of waarvoor een conformiteitsverklaring is afgegeven in het kader van een Europese cyberbeveiligingscertificeringsregeling op grond van Verordening (EU) 2019/881 die door de Commissie bij uitvoeringshandeling is vastgesteld, geacht in overeenstemming te zijn met de essentiële cyberbeveiligingsvereisten van deze verordening, voor zover het cyberbeveiligingscertificaat of de conformiteitsverklaring of delen daarvan die vereisten dekken. De behoefte aan nieuwe Europese cyberbeveiligingscertificeringsregelingen voor producten met digitale elementen moet in het licht van deze verordening worden beoordeeld, onder meer in het kader van de voorbereiding van het voortschrijdend werkprogramma van de Unie overeenkomstig Verordening (EU) 2019/881. Indien er behoefte is aan een nieuwe regeling voor producten met digitale elementen, onder meer om de naleving van deze verordening te vergemakkelijken, kan de Commissie overeenkomstig artikel 48 van Verordening (EU) 2019/881 Enisa verzoeken een potentiële regeling op te stellen. Dergelijke toekomstige Europese cyberbeveiligingscertificeringsregelingen voor producten met digitale elementen moeten rekening houden met de essentiële cyberbeveiligingsvereisten en conformiteitsbeoordelingsprocedures als vastgelegd in deze verordening en de naleving van deze verordening vergemakkelijken. Het kan zijn dat het nodig is om met betrekking tot Europese cyberbeveiligingscertificeringsregelingen die vóór de inwerkingtreding van deze verordening in werking treden, gedetailleerde aspecten inzake de toepassing van een vermoeden van conformiteit nader te specificeren. De Commissie moet de bevoegdheid krijgen om door middel van gedelegeerde handelingen te specificeren onder welke voorwaarden de Europese cyberbeveiligingscertificeringsregelingen kunnen worden gebruikt om de conformiteit met de essentiële cyberbeveiligingsvereisten van deze verordening aan te tonen. Voorts mogen, om onnodige administratieve lasten te vermijden, fabrikanten niet worden verplicht een conformiteitsbeoordeling door derden als voorzien in deze verordening te laten verrichten voor de overeenkomstige vereisten, als uit hoofde van dergelijke Europese cyberbeveiligingscertificeringsregelingen een Europees cyberbeveiligingscertificaat is afgegeven op ten minste zekerheidsniveau “substantieel”.

(82) Bij de inwerkingtreding van Uitvoeringsverordening (EU) 2024/482, die betrekking heeft op producten die binnen het toepassingsgebied van deze verordening vallen, zoals hardwarebeveiligingsmodules en microprocessoren, moet de Commissie door middel van een gedelegeerde handeling kunnen bepalen hoe de EUCC een vermoeden van conformiteit met de essentiële cyberbeveiligingsvereisten van deze verordening of delen daarvan vestigt. Voorts kan in een dergelijke gedelegeerde handeling 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 op grond van deze verordening voor overeenkomstige vereisten.

(83) Het huidige Europese kader voor normalisatie, dat gebaseerd is op de beginselen van de nieuwe aanpak die zijn uiteengezet in de resolutie van de Raad van 7 mei 1985 betreffende een nieuwe aanpak op het gebied van de technische harmonisatie en normalisatie en op Verordening (EU) nr. 1025/2012, vormt het standaardkader voor het opstellen van normen die voorzien in een vermoeden van conformiteit met de relevante essentiële cyberbeveiligingsvereisten van deze verordening. De Europese normen moeten marktgestuurd zijn, rekening houden met het algemeen belang en met de beleidsdoelstellingen die duidelijk zijn vermeld in het verzoek van de Commissie aan één of meer Europese normalisatieorganisaties om geharmoniseerde normen op te stellen binnen een vastgestelde termijn, en moeten stoelen op consensus. Bij gebrek aan relevante referenties van geharmoniseerde normen moet de

([28]) 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).

Commissie echter uitvoeringshandelingen kunnen vaststellen met het oog op het opstellen van gemeenschappelijke technische specificaties voor de essentiële cyberbeveiligingsvereisten van deze verordening, op voorwaarde dat zij daarbij de rol en de functies van Europese normalisatieorganisaties naar behoren eerbiedigt, bij wijze van uitzonderlijke terugvaloplossing om de fabrikant te helpen voldoen aan zijn verplichting die essentiële cyberbeveiligingsvereisten na te leven, als het normalisatieproces stilligt of als de vaststelling van passende geharmoniseerde normen vertraging oploopt. Indien dergelijke vertraging te wijten is aan de technische complexiteit van de betrokken norm, moet de Commissie daar rekening mee houden alvorens de vaststelling van gemeenschappelijke specificaties te overwegen.

(84) Om zo efficiënt mogelijk gemeenschappelijke specificaties voor de essentiële cyberbeveiligingsvereisten van deze verordening vast te stellen, moet de Commissie de relevante belanghebbenden bij dat proces betrekken.

(85) Een redelijke termijn voor de bekendmaking van een referentie van geharmoniseerde normen in het *Publicatieblad van de Europese Unie* overeenkomstig Verordening (EU) nr. 1025/2012, moet een periode zijn waarin de bekendmaking van de referentie van de norm of de rectificatie of wijziging daarvan in het *Publicatieblad van de Europese Unie* wordt verwacht, en die niet langer mag zijn dan één jaar na de overeenkomstig Verordening (EU) nr. 1025/2012 vastgestelde termijn voor het opstellen van een Europese norm.

(86) Om de beoordeling van de conformiteit met de essentiële cyberbeveiligingsvereisten 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 op grond van deze verordening heeft vastgesteld om gedetailleerde technische specificaties van die vereisten aan te geven.

(87) De toepassing van geharmoniseerde normen, gemeenschappelijke specificaties of op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregelingen die voorzien in een vermoeden van conformiteit met betrekking tot de essentiële cyberbeveiligingsvereisten die van toepassing zijn op producten met digitale elementen, zal de beoordeling van de conformiteit door de fabrikanten vergemakkelijken. Indien de fabrikant ervoor kiest om dergelijke middelen met betrekking tot bepaalde vereisten niet toe te passen, moet hij in zijn technische documentatie aangeven op welke andere wijze de conformiteit wordt gewaarborgd. Bovendien vergemakkelijkt de toepassing, door fabrikanten, van geharmoniseerde normen, gemeenschappelijke specificaties of op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregelingen die een vermoeden van conformiteit vestigen, de controle van de conformiteit van producten met digitale elementen door markttoezichtautoriteiten. Daarom worden fabrikanten van producten met digitale elementen aangespoord om dergelijke geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen toe te passen.

(88) 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 cyberbeveiligingsvereisten van deze verordening en, indien van toepassing, van de andere relevante harmonisatiewetgeving van de Unie waaronder het product met digitale elementen valt. Fabrikanten kunnen ook op grond van andere rechtshandelingen 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 relevante afzonderlijke conformiteitsverklaringen.

(89) 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 ([29]). 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 vereisten van deze verordening.

(90) Om marktdeelnemers in staat te stellen de conformiteit met de essentiële cyberbeveiligingsvereisten 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 die vereisten voldoen, moet worden voorzien in conformiteitsbeoordelingsprocedures. Bij Besluit nr. 768/2008/EG van het Europees Parlement en de Raad ([30]) zijn

([29]) 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).

([30]) 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).

modules voor conformiteitsbeoordelingsprocedures vastgesteld die in verhouding staan tot het betrokken risiconiveau en het vereiste beveiligingsniveau. Om voor coherentie tussen de sectoren te zorgen en ad-hocvarianten te voorkomen, moeten de conformiteitsbeoordelingsprocedures die geschikt zijn om de conformiteit van producten met digitale elementen met de essentiële cyberbeveiligingsvereisten van deze verordening te controleren, op die modules worden gebaseerd. De conformiteitsbeoordelingsprocedures moeten zowel product- als procesgerelateerde vereisten 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 met digitale elementen.

(91) De conformiteitsbeoordeling van producten met digitale elementen die in deze verordening niet zijn aangemerkt als belangrijke of kritieke producten met digitale elementen, kan door de fabrikant onder eigen verantwoordelijkheid worden uitgevoerd volgens de procedure voor interne controle op basis van module A van Besluit nr. 768/2008/EG overeenkomstig deze verordening. Dat geldt ook voor gevallen waarin een fabrikant ervoor kiest een toepasselijke geharmoniseerde norm, gemeenschappelijke specificatie of Europese cyberbeveiligingscertificeringsregeling geheel of gedeeltelijk niet toe te passen. De fabrikant blijft over de flexibiliteit beschikken om te kiezen voor een strengere conformiteitsbeoordelingsprocedure waarbij een derde partij betrokken is. In het kader van de conformiteitsbeoordelingsprocedure op basis van interne controle garandeert en verklaart de fabrikant op eigen verantwoordelijkheid dat het product met digitale elementen en de processen van de fabrikant aan de toepasselijke essentiële cyberbeveiligingsvereisten van deze verordening voldoen. Indien een belangrijk product met digitale elementen onder klasse I valt, is aanvullende zekerheid vereist om aan te tonen dat het product aan de essentiële cyberbeveiligingsvereisten van deze verordening voldoet. De fabrikant moet geharmoniseerde normen, gemeenschappelijke specificaties of op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregelingen, die door de Commissie bij uitvoeringshandeling zijn vastgesteld, toepassen, indien hij de conformiteitsbeoordeling onder zijn eigen verantwoordelijkheid wil uitvoeren (module A). Als de fabrikant dergelijke geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen niet toepast, moet de fabrikant een conformiteitsbeoordeling ondergaan waarbij een derde partij betrokken is (op basis van de modules B en C of module H). 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 de modules B en C of module H van Besluit nr. 768/2008/EG gekozen als de meest geschikte voor een evenredige en doeltreffende beoordeling van de conformiteit van belangrijke 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 belangrijke producten met digitale elementen die vallen onder klasse II, moet bij de conformiteitsbeoordeling in dat geval altijd een derde partij betrokken zijn, zelfs wanneer het product geheel of gedeeltelijk voldoet aan geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen. Fabrikanten van belangrijke producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt, moeten de procedure voor interne controle op basis van module A kunnen volgen, op voorwaarde dat zij de technische documentatie openbaar maken.

(92) De vervaardiging van materiële producten met digitale elementen vereist doorgaans dat fabrikanten aanzienlijke inspanningen leveren tijdens de ontwerp-, ontwikkelings- en productiefase, maar de vervaardiging van producten met digitale elementen in de vorm van software is bijna uitsluitend gericht op ontwerp en ontwikkeling, waarbij 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. Die 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 cyberbeveiligingsvereisten van deze verordening voldoet.

(93) Om evenredigheid te waarborgen is het passend dat met betrekking tot micro-ondernemingen en kleine ondernemingen de administratieve kosten worden verlicht, zonder dat afbreuk wordt gedaan aan het niveau van cyberbeveiliging met betrekking tot producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen en zonder dat het gelijke speelveld tussen fabrikanten wordt aangetast. Het is daarom passend dat de Commissie een vereenvoudigd formulier voor technische documentatie vaststelt dat is afgestemd op de behoeften van micro-ondernemingen en kleine ondernemingen. Het door de Commissie vast te stellen vereenvoudigde formulier voor technische documentatie moet alle in deze verordening vastgestelde toepasselijke elementen in verband met technische documentatie omvatten, en nader bepalen hoe een micro-onderneming of een kleine onderneming de gevraagde elementen, zoals de beschrijving van het ontwerp, de ontwikkeling en de productie van het product met digitale elementen, op beknopte wijze kan verstrekken. Op die manier draagt het formulier ertoe bij dat de administratieve lasten in verband met de naleving worden verlicht doordat de betrokken ondernemingen rechtszekerheid wordt geboden over de omvang en de gedetailleerdheid van de te verstrekken informatie. Micro-ondernemingen en kleine ondernemingen moeten ervoor kunnen kiezen de toepasselijke elementen in verband met de technische documentatie in uitgebreide vorm te verstrekken en geen gebruik te maken van het vereenvoudigde technische formulier waarvan zij gebruik mogen maken.

(94) Met het oog op de bevordering en bescherming van innovatie is het belangrijk dat in het bijzonder rekening wordt gehouden met de belangen van fabrikanten die micro-ondernemingen of kleine of middelgrote ondernemingen zijn, in het bijzonder micro-ondernemingen en kleine ondernemingen, met inbegrip van start-ups. Daartoe kunnen de lidstaten initiatieven ontwikkelen ten behoeve van fabrikanten die micro- of kleine ondernemingen zijn, waaronder initiatieven op het gebied van opleiding, bewustmaking, gegevensverstrekking, testactiviteiten en conformiteitsbeoordeling door derden en het opzetten van testomgevingen. Vertaalkosten in verband met de op grond van deze verordening te verstrekken documentatie, zoals de technische documentatie en de informatie en instructies voor de gebruiker, en communicatie met de autoriteiten, kunnen voor fabrikanten, met name voor kleinere fabrikanten, een aanzienlijke financiële last vormen. Daarom moeten de lidstaten kunnen bepalen dat een van de door hen vastgestelde en aanvaarde talen voor de relevante documentatie van fabrikanten en voor de communicatie met fabrikanten een taal is die beheerst wordt door een zo groot mogelijk aantal gebruikers.

(95) Om een soepele toepassing van deze verordening te waarborgen, moeten de lidstaten ernaar streven ervoor te zorgen dat er vóór de datum van toepassing van deze verordening een voldoende aantal aangemelde instanties is om conformiteitsbeoordelingen door derden uit te voeren. De Commissie moet zich inspannen om de lidstaten en andere relevante partijen daarbij te ondersteunen, om knelpunten en belemmeringen voor de markttoegang van fabrikanten te voorkomen. Gerichte opleidingsactiviteiten onder leiding van de lidstaten, indien passend met steun van de Commissie, kunnen bijdragen tot de beschikbaarheid van gekwalificeerde professionals, onder meer ter ondersteuning van de activiteiten van aangemelde instanties uit hoofde van deze verordening. Gelet op de kosten die gepaard kunnen gaan met conformiteitsbeoordeling door derden, moeten voorts financieringsinitiatieven op Unie- en nationaal niveau ter verlichting van dergelijke kosten voor micro-ondernemingen en kleine ondernemingen in overweging worden genomen.

(96) Om evenredigheid te waarborgen, moeten conformiteitsbeoordelingsinstanties bij het vaststellen van de vergoedingen voor conformiteitsbeoordelingsprocedures rekening houden met de specifieke belangen en behoeften van micro-ondernemingen en kleine en middelgrote ondernemingen, met inbegrip van start-ups. Met name dienen conformiteitsbeoordelingsinstanties de relevante onderzoeksprocedure en tests waarin deze verordening voorziet, uitsluitend toe te passen indien dat passend is en dienen zij een risicogebaseerde aanpak te hanteren.

(97) De testomgevingen voor regelgeving moeten ten doel hebben innovatie en concurrentievermogen bij bedrijven te bevorderen, door te voorzien in gecontroleerde omgevingen voor het uitvoeren van tests voordat de producten met digitale elementen in de handel worden gebracht. Testomgevingen voor regelgeving moeten de rechtszekerheid vergroten voor alle actoren die binnen het toepassingsgebied van deze verordening vallen en moeten de toegang van producten met digitale elementen tot de markt van de Unie vergemakkelijken en versnellen, met name als zij geleverd worden door micro-ondernemingen en kleine ondernemingen, met inbegrip van start-ups.

(98) 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.

(99) Om een consistent kwaliteitsniveau bij de uitvoering van een conformiteitsbeoordeling van producten met digitale elementen te waarborgen, moeten ook vereisten 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.

(100) Conformiteitsbeoordelingsinstanties die zijn geaccrediteerd en aangemeld uit hoofde van het Unierecht waarin vereisten zijn vastgesteld die vergelijkbaar zijn met die van deze verordening, zoals een conformiteitsbeoordelingsinstantie die is aangemeld voor een Europese cyberbeveiligingscertificeringsregeling die is vastgesteld op grond van Verordening (EU) 2019/881 of is aangemeld uit hoofde van Gedelegeerde Verordening (EU) 2022/30, moeten tevens worden beoordeeld en aangemeld uit hoofde van deze verordening. Om onnodige financiële en administratieve lasten te voorkomen en om een soepel en vlot verlopend aanmeldingsproces te waarborgen, kunnen de relevante autoriteiten echter synergieën vaststellen met betrekking tot overlappende vereisten.

(101) 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 evaluatie 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.

(102) 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 een product met digitale elementen dat in de handel wordt gebracht, is het essentieel dat de betrokken onderaannemers en dochterondernemingen voor de uitvoering van conformiteitsbeoordelingstaken aan dezelfde vereisten voldoen als de aangemelde instanties.

(103) 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. Het Nando-informatiesysteem is het door de Commissie ontwikkelde en beheerde elektronische aanmeldingsinstrument dat een lijst van alle aangemelde instanties bevat.

(104) 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 instanties gaan functioneren.

(105) 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. Dat kan het best worden bereikt door passende coördinatie en samenwerking tussen aangemelde instanties.

(106) Markttoezicht is een essentieel instrument om de correcte en uniforme toepassing van het Unierecht te waarborgen. Daarom moet een rechtskader tot stand worden gebracht waarbinnen passend markttoezicht kan worden uitgeoefend. De in Verordening (EU) 2019/1020 vastgestelde voorschriften inzake markttoezicht in de Unie en controle van producten die de markt van de Unie binnenkomen, zijn van toepassing op producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen.

(107) Overeenkomstig Verordening (EU) 2019/1020 voert een markttoezichtautoriteit markttoezicht uit op het grondgebied van de lidstaat die haar aanwijst. Deze verordening mag de lidstaten niet beletten te kiezen welke autoriteiten voor de uitvoering van markttoezichttaken bevoegd zijn. Elke lidstaat moet een of meer markttoezichtautoriteiten op zijn grondgebied aanwijzen. De lidstaten moeten ervoor kunnen kiezen een bestaande of nieuwe autoriteit aan te wijzen als markttoezichtautoriteit, met inbegrip van bevoegde autoriteiten die zijn aangewezen of opgericht op grond van artikel 8 van Richtlijn (EU) 2022/2555, nationale cyberbeveiligingscertificeringsautoriteiten die zijn aangewezen op grond van artikel 58 van Verordening (EU) 2019/881 of markttoezichtautoriteiten die zijn aangewezen voor de toepassing van Richtlijn 2014/53/EU. 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 markttoezichttaken in verband met deze verordening. Op grond van 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.

(108) Voor de uniforme toepassing van deze verordening moet op grond van artikel 30, lid 2, van Verordening (EU) 2019/1020 een speciale ADCO voor de cyberweerbaarheid van producten met digitale elementen worden opgericht. De 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 die verordening 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 Unienetwerk voor productconformiteit, zijn subgroepen en de ADCO. Zij moet de ADCO ook bijstaan door middel van een uitvoerend secretariaat dat technische en logistieke ondersteuning biedt. De ADCO kan ook onafhankelijke deskundigen uitnodigen om deel te nemen en contacten onderhouden met andere ADCO's, zoals die welke is opgericht krachtens Richtlijn 2014/53/EU.

(109) Markttoezichtautoriteiten moeten via de krachtens deze verordening opgerichte ADCO nauw samenwerken en richtsnoeren kunnen ontwikkelen om de markttoezichtactiviteiten op nationaal niveau te faciliteren, bijvoorbeeld door beste praktijken en indicatoren te ontwikkelen om effectief te controleren of producten met digitale elementen aan deze verordening voldoen.

(110) 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. Dat moet de markttoezichtautoriteiten ook in staat 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, hoeft er geen verdere betrokkenheid van de Commissie vereist te zijn, behalve wanneer de niet-conformiteit kan worden toegeschreven aan tekortkomingen van een geharmoniseerde norm.

(111) 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 nationale recht ter bescherming van de grondrechten, voor de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van diensten die via een elektronisch informatiesysteem worden aangeboden door in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten, 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 om 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 met digitale elementen op die manier beperkt of verbiedt, moet de lidstaat aan de Commissie en aan de andere lidstaten onverwijld melding doen van de voorlopige maatregelen, met opgave van de redenen en motivering van het besluit. Wanneer een markttoezichtautoriteit dergelijke maatregelen neemt tegen producten met digitale elementen die een risico vormen, moet de Commissie onverwijld in overleg treden met de lidstaten en de betrokken marktdeelnemer en de nationale maatregel evalueren. Aan de hand van die evaluatie moet de Commissie besluiten of de maatregel al dan niet gerechtvaardigd is. De Commissie moet haar besluit aan alle lidstaten richten en dat onmiddellijk aan hen en aan de betrokken marktdeelnemers kenbaar maken. Indien de maatregel gerechtvaardigd wordt geacht, moet de Commissie ook overwegen voorstellen tot herziening van het desbetreffende Unierecht vast te stellen.

(112) 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, voor de naleving van verplichtingen uit hoofde van Unierecht of nationaal recht ter bescherming van de grondrechten, of voor de beschikbaarheid, de authenticiteit, de integriteit of de vertrouwelijkheid van diensten die via een elektronisch informatiesysteem worden aangeboden door in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten, moet de Commissie Enisa kunnen verzoeken een evaluatie te verrichten. Op basis van die evaluatie moet de Commissie door middel van uitvoeringshandelingen corrigerende of beperkende maatregelen op Unieniveau kunnen vaststellen, onder meer door te gelasten de betrokken producten met digitale elementen binnen een redelijke termijn in verhouding tot de aard van het risico uit de handel te nemen of terug te roepen. De Commissie moet een dergelijke maatregel alleen kunnen toepassen in uitzonderlijke omstandigheden die een onmiddellijk optreden rechtvaardigen om de goede werking van de interne markt te beschermen, en alleen wanneer de markttoezichtautoriteiten geen doeltreffende maatregelen hebben genomen om de situatie te verhelpen. Dergelijke uitzonderlijke omstandigheden kunnen noodsituaties zijn waarin bijvoorbeeld een niet-conform product met digitale elementen door de fabrikant in verschillende lidstaten op grote schaal wordt aangeboden, ook in belangrijke sectoren wordt gebruikt door entiteiten die binnen het toepassingsgebied van Richtlijn (EU) 2022/2555 vallen, en bekende kwetsbaarheden bevat die door kwaadwillige actoren worden uitgebuit en waarvoor de fabrikant geen patches verstrekt. De Commissie moet in dergelijke noodsituaties alleen kunnen 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.

(113) Indien 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.

(114) 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 categorieën producten met digitale elementen vaak cyberbeveiligingsrisico's blijken te vormen. Bovendien moeten de markttoezichtautoriteiten bij het bepalen van de productcategorieën die aan bezemacties moeten worden onderworpen, ook rekening houden met omstandigheden in verband met niet-technische risicofactoren. Daartoe moeten de markttoezichtautoriteiten rekening kunnen houden met de resultaten van de overeenkomstig artikel 22 van Richtlijn (EU) 2022/2555 verrichte, op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens, met inbegrip van omstandigheden in verband met niet-technische risicofactoren. Enisa moet bij de markttoezichtautoriteiten voorstellen indienen voor categorieën producten met digitale elementen waarvoor bezemacties kunnen worden georganiseerd, onder meer op basis van de meldingen van kwetsbaarheden van producten en incidenten die het ontvangt.

(115) Enisa moet, in het licht van zijn deskundigheid en zijn mandaat, het proces voor de uitvoering van deze verordening kunnen ondersteunen. Enisa 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 bezemacties 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.

(116) Bij deze verordening worden bepaalde taken aan Enisa toegewezen waarvoor passende middelen qua deskundigheid en personeel nodig zijn om Enisa in staat te stellen die taken doeltreffend uit te voeren. Bij de opstelling van het ontwerp van algemene begroting van de Unie zal de Commissie volgens de procedure van artikel 29 van Verordening (EU) 2019/881 de nodige begrotingsmiddelen voor de personeelsformatie van Enisa voorstellen. Daarbij zal de Commissie de totale middelen van Enisa in overweging nemen om het in staat te stellen zijn taken te vervullen, met inbegrip van de taken die op grond van deze verordening aan Enisa zijn toegewezen.

(117) Teneinde ervoor te zorgen dat het regelgevingskader waar nodig kan worden aangepast, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 van het Verdrag betreffende de werking van de Europese Unie (VWEU) handelingen vast te stellen ten aanzien van het actualiseren van een bijlage bij deze verordening met de lijst van belangrijke producten met digitale elementen. Aan de Commissie moet de bevoegdheid worden overgedragen 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 in het kader van een Europese cyberbeveiligingscertificeringsregeling van de kritieke producten met digitale elementen die in een bijlage bij deze verordening zijn opgenomen, alsook voor het actualiseren van de lijst van kritieke producten met digitale elementen op basis van in deze verordening vastgestelde criteria omtrent hun kritieke karakter, en voor het specificeren van de op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregelingen die kunnen worden gebruikt om de conformiteit met de in een bijlage bij deze verordening opgenomen essentiële cyberbeveiligingsvereisten of delen daarvan aan te tonen. Ook moet aan de Commissie de bevoegdheid worden overgedragen om gedelegeerde handelingen vast te stellen om de minimale ondersteuningsperiode voor specifieke productcategorieën te specificeren wanneer uit de markttoezichtgegevens blijkt dat de ondersteuningsperioden ontoereikend zijn, alsook om de voorwaarden te specificeren voor de toepassing van de cyberbeveiligingsgerelateerde redenen voor het uitstellen van de verspreiding van meldingen van actief uitgebuite kwetsbaarheden. Voorts moet aan de Commissie de bevoegdheid worden overgedragen om gedelegeerde handelingen vast te stellen om vrijwillige beveiligingsattestatieprogramma's op te zetten om te beoordelen of producten met digitale elementen die als vrije en opensourcesoftware kunnen worden aangemerkt, aan alle of bepaalde essentiële cyberbeveiligingsvereisten of andere verplichtingen van deze verordening voldoen, alsook om de minimuminhoud van de EU-conformiteitsverklaring te specificeren en om de elementen die in de technische documentatie moeten worden opgenomen, aan te vullen. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen gebeuren in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven ([31]). 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. De bevoegdheid om op grond van deze verordening gedelegeerde handelingen vast te stellen, moet aan de Commissie worden toegekend voor een periode van vijf jaar vanaf 10 december 2024. De Commissie moet uiterlijk negen maanden voor het einde van de termijn van vijf jaar een verslag opstellen over de bevoegdheidsdelegatie. De bevoegdheidsdelegatie moet stilzwijgend met termijnen van dezelfde duur worden verlengd, tenzij het Europees Parlement of de Raad zich uiterlijk drie maanden voor het einde van elke termijn tegen die verlenging verzet.

(118) Om eenvormige voorwaarden te waarborgen voor de uitvoering van deze verordening, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend om de technische beschrijving van de in een bijlage bij deze verordening opgenomen categorieën belangrijke producten met digitale elementen te specificeren, om de vorm en de procedure van de door fabrikanten ingediende meldingen van actief uitgebuite kwetsbaarheden en ernstige incidenten met gevolgen voor de beveiliging van producten met digitale elementen nader te specificeren, om gemeenschappelijke specificaties vast te stellen inzake technische vereisten die een middel bieden om te voldoen aan de in een bijlage bij deze verordening opgenomen essentiële cyberbeveiligingsvereisten, om technische specificaties vast te stellen voor etiketten, pictogrammen of andere merktekens in verband met de beveiliging van producten met digitale elementen, de ondersteuningsperiode ervan en mechanismen om het gebruik ervan te bevorderen en het publiek beter bewust te maken van de beveiliging van producten met digitale elementen, om het op de behoeften van micro-ondernemingen en kleine ondernemingen afgestemde vereenvoudigde documentatieformulier te specificeren, en om besluiten te nemen over corrigerende of beperkende maatregelen op het niveau van de Unie in uitzonderlijke

([31]) PB L 123 van 12.5.2016, blz. 1.

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 ([32]).

(119) Om een op vertrouwen gebaseerde 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.

(120) 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 daarvan te vragen. Daarom moeten maximumniveaus worden vastgesteld voor administratieve geldboeten waarin het nationale 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 de fabrikant een micro-, kleine of middelgrote onderneming, met inbegrip van een start-up, is en of dezelfde of andere markttoezichtautoriteiten reeds administratieve geldboeten hebben opgelegd aan dezelfde marktdeelnemer voor een soortgelijke inbreuk. 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 in overweging wordt genomen, 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. Aangezien administratieve geldboeten niet van toepassing zijn op micro-ondernemingen of kleine ondernemingen bij niet-naleving van de termijn van 24 uur voor de vroegtijdige waarschuwing over actief uitgebuite kwetsbaarheden of ernstige incidenten die gevolgen hebben voor de beveiliging van het product met digitale elementen, noch op opensourcesoftwarestewards bij inbreuken op deze verordening, en met inachtneming van het beginsel dat sancties doeltreffend, evenredig en afschrikkend moeten zijn, mogen de lidstaten die entiteiten geen andere soorten geldelijke sancties opleggen.

(121) Wanneer administratieve geldboeten worden opgelegd aan een persoon die geen onderneming is, 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.

(122) De lidstaten moeten, rekening houdend met de nationale omstandigheden, de mogelijkheid onderzoeken om de inkomsten uit de sancties waarin deze verordening voorziet, of het financiële equivalent daarvan, te gebruiken om cyberbeveiligingsbeleid te ondersteunen en het cyberbeveiligingsniveau in de Unie te verhogen, door onder meer het aantal gekwalificeerde cyberbeveiligingsprofessionals te vergroten, de capaciteitsopbouw voor micro-ondernemingen en kleine en middelgrote ondernemingen te versterken en het publiek beter bewust te maken van cyberdreigingen.

(123) In haar betrekkingen met derde landen streeft de Unie 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. Die 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 met verschillende derde landen. Die overeenkomsten inzake wederzijdse erkenning worden gesloten in een aantal specifieke sectoren, die van derde land tot derde 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 derde partnerlanden is ook belangrijk om de cyberweerbaarheid wereldwijd te versterken, aangezien dat op lange termijn zal bijdragen tot een versterkt cyberbeveiligingskader, zowel binnen als buiten de Unie.

([32]) 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) Consumenten moeten hun rechten met betrekking tot de verplichtingen die uit hoofde van deze verordening aan marktdeelnemers worden opgelegd, kunnen afdwingen door middel van representatieve vorderingen op grond van Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad ([33]). Daartoe moet in deze verordening worden bepaald dat Richtlijn (EU) 2020/1828 van toepassing is op de representatieve vorderingen met betrekking tot inbreuken op deze verordening die de collectieve belangen van consumenten schaden of kunnen schaden. Bijlage I bij die richtlijn moet daarom dienovereenkomstig worden gewijzigd. Het is aan de lidstaten om ervoor te zorgen dat die wijzigingen worden weergegeven in de op grond van die richtlijn vastgestelde omzettingsmaatregelen, hoewel de vaststelling van nationale omzettingsmaatregelen in dat verband geen voorwaarde is voor de toepasselijkheid van die richtlijn op die representatieve vorderingen. Die richtlijn moet vanaf 11 december 2027 van toepassing zijn op representatieve vorderingen die worden ingesteld wegens inbreuken op bepalingen van deze verordening door marktdeelnemers die de collectieve belangen van consumenten schaden of zouden kunnen schaden.

(125) De Commissie moet deze verordening in overleg met relevante belanghebbenden op gezette tijden evalueren en toetsen, met name om na te gaan of zij in het licht van de veranderende maatschappelijke, politieke, technologische of marktomstandigheden moet worden gewijzigd. Deze verordening zal het voor entiteiten die onder het toepassingsgebied van Verordening (EU) 2022/2554 en Richtlijn (EU) 2022/2555 vallen en die producten met digitale elementen gebruiken, gemakkelijker maken om hun verplichtingen inzake de beveiliging van de toeleveringsketen na te leven. De Commissie moet in het kader van die periodieke toetsing de gecombineerde effecten van het cyberbeveiligingskader van de Unie evalueren.

(126) De marktdeelnemers moeten voldoende tijd krijgen om zich aan de vereisten van deze verordening aan te passen. Deze verordening moet vanaf 11 december 2027 van toepassing zijn, met uitzondering van de meldingsplicht met betrekking tot actief uitgebuite kwetsbaarheden en ernstige incidenten die gevolgen hebben voor de beveiliging van producten met digitale elementen, die vanaf 11 september 2026 van toepassing moet zijn, en van de bepalingen betreffende de aanmelding van conformiteitsbeoordelingsinstanties, die vanaf 11 juni 2026 van toepassing moeten zijn.

(127) Het is belangrijk om micro-ondernemingen en kleine en middelgrote ondernemingen, met inbegrip van start-ups, te ondersteunen bij de uitvoering van deze verordening en de risico's voor de uitvoering als gevolg van een gebrek aan kennis en deskundigheid op de markt tot een minimum te beperken, alsook om het voor fabrikanten gemakkelijker te maken hun verplichtingen uit hoofde van deze verordening na te leven. Het programma Digitaal Europa en andere relevante programma's van de Unie bieden financiële en technische ondersteuning die die ondernemingen in staat stelt bij te dragen tot de groei van de economie van de Unie en de versterking van het gemeenschappelijke cyberbeveiligingsniveau in de Unie. Ook het Europees Kenniscentrum voor cyberbeveiliging, de nationale coördinatiecentra en de Europese digitale-innovatiehubs die door de Commissie en de lidstaten op Unie- of nationaal niveau zijn opgericht, kunnen ondernemingen en overheidsorganisaties ondersteunen en bijdragen tot de uitvoering van deze verordening. Binnen hun respectieve taken en bevoegdheidsgebieden zouden zij micro-ondernemingen en kleine en middelgrote ondernemingen technische en wetenschappelijke ondersteuning kunnen bieden, bijvoorbeeld voor testactiviteiten en conformiteitsbeoordelingen door derden. Ook zouden zij de uitrol van instrumenten om de uitvoering van deze verordening te vergemakkelijken, kunnen bevorderen.

(128) Voorts moeten de lidstaten overwegen aanvullende maatregelen te nemen om micro-ondernemingen en kleine en middelgrote ondernemingen begeleiding en ondersteuning te bieden, bijvoorbeeld door testomgevingen voor regelgeving en speciale communicatiekanalen op te zetten. Om het cyberbeveiligingsniveau in de Unie te verhogen, kunnen de lidstaten ook overwegen steun te verlenen voor het ontwikkelen van capaciteit en vaardigheden op het gebied van cyberbeveiliging van producten met digitale elementen, het verbeteren van de cyberveerkracht van marktdeelnemers, in het bijzonder micro-ondernemingen en kleine en middelgrote ondernemingen, en bewustmaking van het publiek over de cyberbeveiliging van producten met digitale elementen.

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

(130) Overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([34]) is de Europese Toezichthouder voor gegevensbescherming geraadpleegd, en op 9 november 2022 heeft hij een advies ([35]) uitgebracht,

([33]) Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad van 25 november 2020 betreffende representatieve vorderingen ter bescherming van de collectieve belangen van consumenten en tot intrekking van Richtlijn 2009/22/EG (PB L 409 van 4.12.2020, blz. 1).

([34]) 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).

([35]) PB C 452 van 29.11.2022, blz. 23.

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

Bij deze verordening worden vastgesteld:

a) regels voor het op de markt aanbieden van producten met digitale elementen om de cyberbeveiliging van dergelijke producten te waarborgen;

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

c) essentiële cyberbeveiligingsvereisten voor de procedures inzake de respons op kwetsbaarheden die fabrikanten hebben ingesteld om de cyberbeveiliging van producten met digitale elementen te waarborgen gedurende de tijd dat de producten naar verwachting in gebruik zullen zijn, en verplichtingen voor marktdeelnemers met betrekking tot die procedures;

d) voorschriften inzake markttoezicht, met inbegrip van monitoring, en handhaving van de in dit artikel bedoelde regels en vereisten.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op op de markt aangeboden producten met digitale elementen waarvan het beoogde doel of het 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 rechtshandelingen 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. Deze verordening is niet van toepassing op uitrusting die binnen het toepassingsgebied van Richtlijn 2014/90/EU van het Europees Parlement en de Raad ([36]) valt.

5. De toepassing van deze verordening op producten met digitale elementen die vallen onder andere voorschriften van de Unie tot vaststelling van vereisten die betrekking hebben op alle of een deel van de risico's die door de essentiële cyberbeveiligingsvereisten 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 of een hoger beschermingsniveau bieden als deze verordening.

De Commissie is bevoegd om overeenkomstig artikel 61 gedelegeerde handelingen vast te stellen om deze verordening aan te vullen door nader te bepalen of een dergelijke beperking of uitsluiting noodzakelijk is, welke producten en regels daarbij betrokken zijn en, voor zover relevant, wat het toepassingsgebied van de beperking is.

([36]) Richtlijn 2014/90/EU van het Europees Parlement en de Raad van 23 juli 2014 inzake uitrusting van zeeschepen en tot intrekking van Richtlijn 96/98/EG van de Raad (PB L 257 van 28.8.2014, blz. 146).

6. Deze verordening is niet van toepassing op reserveonderdelen die op de markt worden aangeboden ter vervanging van identieke componenten in producten door digitale elementen en die zijn vervaardigd volgens dezelfde specificaties als de componenten die zij beogen te vervangen.

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

8. De in deze verordening vastgelegde verplichtingen omvatten niet de verstrekking van informatie waarvan de bekendmaking strijdig zou zijn met de wezenlijke belangen van de lidstaten inzake nationale veiligheid, openbare veiligheid of defensie.

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

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

2) "gegevensverwerking op afstand": gegevensverwerking vanop een 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) "cyberbeveiliging": cyberbeveiliging zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2019/881;

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

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

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

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

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

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

10) "indirecte verbinding": een verbinding met een apparaat of netwerk die niet direct plaatsvindt, maar eerder als onderdeel van een groter systeem dat een directe verbinding kan maken met dat apparaat of netwerk;

11) "endpoint": een apparaat dat op een netwerk is aangesloten en als toegangspunt tot dat netwerk fungeert;

12) "marktdeelnemer": de fabrikant, de gemachtigde vertegenwoordiger, de importeur, de distributeur of een andere natuurlijke of rechtspersoon op wie overeenkomstig deze verordening verplichtingen van toepassing zijn ten aanzien van de vervaardiging van producten met digitale elementen of het op de markt aanbieden van producten met digitale elementen;

13) "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 merk tegen betaling, met een verdienmodel of gratis in de handel brengt;

14) "opensourcesoftwaresteward": een rechtspersoon die geen fabrikant is en die als oogmerk of doelstelling heeft om systematisch en duurzaam ondersteuning te verlenen voor de ontwikkeling van specifieke producten met digitale elementen die als vrije en opensourcesoftware kunnen worden aangemerkt en voor handelsactiviteiten bestemd zijn, en die de levensvatbaarheid van die producten waarborgt;

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

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

17) “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 daarvan te beïnvloeden;

18) “consument”: een natuurlijke persoon die handelt met doeleinden die geen verband houden met de handels-, bedrijfs-, ambachts- of beroepsactiviteit van die persoon;

19) “micro-ondernemingen”, “kleine ondernemingen” en “middelgrote ondernemingen”: respectievelijk micro-ondernemingen, kleine ondernemingen en middelgrote ondernemingen zoals gedefinieerd in de bijlage bij Aanbeveling 2003/361/EG;

20) “ondersteuningsperiode”: de periode gedurende welke een fabrikant ervoor moet zorgen dat kwetsbaarheden van een product met digitale elementen doeltreffend en in overeenstemming met de essentiële cyberbeveiligingsvereisten van deel II van bijlage I worden aangepakt;

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

22) “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;

23) “beoogde 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;

24) “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;

25) “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;

26) “aanmeldende autoriteit”: de nationale autoriteit die verantwoordelijk is voor het opzetten en uitvoeren van de noodzakelijke procedures voor de beoordeling, aanwijzing en aanmelding van de conformiteitsbeoordelingsinstanties en de monitoring daarvan;

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

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

29) “aangemelde instantie”: een conformiteitsbeoordelingsinstantie die overeenkomstig artikel 43 en andere relevante harmonisatiewetgeving van de Unie is aangewezen;

30) “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 cyberbeveiligingsvereisten van deel I van bijlage I of leidt tot een wijziging van het beoogde doel waarvoor het product met digitale elementen is beoordeeld;

31) “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 cyberbeveiligingsvereisten van bijlage I en andere toepasselijke harmonisatiewetgeving van de Unie die in het aanbrengen ervan voorziet;

32) “harmonisatiewetgeving van de Unie”: harmonisatiewetgeving van de Unie die is opgenomen in bijlage I bij Verordening (EU) 2019/1020 en alle andere Uniewetgeving tot harmonisering van de voorwaarden voor het verhandelen van producten waarop die verordening van toepassing is;

33) “markttoezichtautoriteit”: een markttoezichtautoriteit zoals gedefinieerd in artikel 3, punt 4, van Verordening (EU) 2019/1020;

34) “internationale norm”: een internationale norm zoals gedefinieerd in artikel 2, punt 1, a), van Verordening (EU) nr. 1025/2012;

35) “Europese norm”: een Europese norm zoals gedefinieerd in artikel 2, punt 1, b), van Verordening (EU) nr. 1025/2012;

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

37) “cyberbeveiligingsrisico”: de mogelijkheid van verlies of verstoring als gevolg van een incident; dat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat het incident zich voordoet;

38) “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;

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

40) “kwetsbaarheid”: een zwakheid, vatbaarheid of gebrek van een product met digitale elementen die/dat door een cyberdreiging kan worden uitgebuit;

41) “uitbuitbare kwetsbaarheid”: een kwetsbaarheid die onder praktische operationele omstandigheden effectief door een tegenstander zou kunnen worden gebruikt;

42) “actief uitgebuite kwetsbaarheid”: een kwetsbaarheid waarvoor betrouwbare bewijzen bestaan dat een kwaadwillige actor die heeft uitgebuit in een systeem zonder toestemming van de systeemeigenaar;

43) “incident”: een incident zoals gedefinieerd in artikel 6, punt 6, van Richtlijn (EU) 2022/2555;

44) “incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen”: een incident dat negatieve gevolgen heeft of kan hebben voor het vermogen van een product met digitale elementen om de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of functies te beschermen;

45) “bijna-incident”: een bijna-incident zoals gedefinieerd in artikel 6, punt 5, van Richtlijn (EU) 2022/2555;

46) “cyberdreiging”: een cyberdreiging zoals gedefinieerd in artikel 2, punt 8, van Verordening (EU) 2019/881;

47) “persoonsgegevens”: persoonsgegevens zoals gedefinieerd in artikel 4, punt 1, van Verordening (EU) 2016/679;

48) “vrije en opensourcesoftware”: software waarvan de broncode openlijk wordt gedeeld en die beschikbaar wordt gesteld onder een vrije en opensourcelicentie die voorziet in alle rechten om die vrij toegankelijk, bruikbaar, wijzigbaar en herdistrueerbaar te maken;

49) “terugroepen”: terugroepen zoals gedefinieerd in artikel 3, punt 22, van Verordening (EU) 2019/1020;

50) “uit de handel nemen”: uit de handel nemen zoals gedefinieerd in artikel 3, punt 23, van Verordening (EU) 2019/1020;

51) “als coördinator aangewezen CSIRT”: een CSIRT dat op grond van artikel 12, lid 1, van Richtlijn (EU) 2022/2555 als coördinator is aangewezen.

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, demonstraties of soortgelijke evenementen een product met digitale elementen wordt gepresenteerd of gebruikt dat niet aan deze verordening voldoet, met inbegrip van prototypes daarvan, mits het product wordt gepresenteerd met een zichtbaar teken dat duidelijk aangeeft dat het niet aan deze verordening voldoet en dat het pas op de markt mag worden aangeboden zodra het dat wel doet.

3. De lidstaten beletten niet dat onafgewerkte software die niet aan deze verordening voldoet, op de markt 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 dat deze niet voor andere doeleinden dan tests op de markt zal worden aangeboden.

4. Lid 3 is niet van toepassing op veiligheidscomponenten als bedoeld in andere harmonisatiewetgeving van de Unie dan deze verordening.

Artikel 5

Aankoop of gebruik van producten met digitale elementen

1. Deze verordening belet de lidstaten niet om producten met digitale elementen te onderwerpen aan aanvullende cyberbeveiligingsvereisten voor de aankoop of het gebruik van die producten voor specifieke doeleinden, ook wanneer die producten worden aangekocht of gebruikt voor doeleinden van nationale veiligheid of voor defensiedoeleinden, mits die vereisten stroken met de verplichtingen van de lidstaten uit hoofde van het Unierecht en noodzakelijk en evenredig zijn voor de verwezenlijking van die doeleinden.

2. Onverminderd de Richtlijnen 2014/24/EU en 2014/25/EU zorgen de lidstaten ervoor dat wanneer producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen, worden aangekocht, in het aankoopproces rekening wordt gehouden met de naleving van de essentiële cyberbeveiligingsvereisten van bijlage I bij deze verordening, met inbegrip van het vermogen van fabrikanten om kwetsbaarheden doeltreffend aan te pakken.

Artikel 6

Vereisten voor producten met digitale elementen

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

a) zij voldoen aan de essentiële cyberbeveiligingsvereisten van deel I van bijlage I, mits zij op passende wijze worden geïnstalleerd, onderhouden, gebruikt voor hun beoogde doel of in redelijkerwijs voorzienbare omstandigheden en, indien van toepassing, mits de nodige beveiligingsupdates zijn geïnstalleerd, en

b) de door de fabrikant ingestelde processen voldoen aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I.

Artikel 7

Belangrijke producten met digitale elementen

1. Producten met digitale elementen met de belangrijkste functionaliteit van een categorie als vermeld in bijlage III worden geacht belangrijke producten met digitale elementen te zijn en worden onderworpen aan de in artikel 32, leden 2 en 3, bedoelde conformiteitsbeoordelingsprocedures. De integratie van een product met digitale elementen met de belangrijkste functionaliteit van een categorie als vermeld in bijlage III betekent op zich niet dat het product waarin het wordt geïntegreerd, wordt onderworpen aan de in artikel 32, leden 2 en 3, bedoelde conformiteitsbeoordelingsprocedures.

2. De in lid 1 van dit artikel bedoelde categorieën producten met digitale elementen, onderverdeeld in de klassen I en II als vermeld in bijlage III, voldoen aan ten minste een van de volgende criteria:

a) het product met digitale elementen vervult voornamelijk functies die van kritiek belang zijn voor de cyberbeveiliging van andere producten, netwerken of diensten, waaronder het beveiligen van authenticatie en toegang, het voorkomen en opsporen van binnendringing, endpointbeveiliging of netwerkbeveiliging;

b) het product met digitale elementen vervult een functie die een aanzienlijk risico op nadelige effecten inhoudt wat betreft de intensiteit ervan en het vermogen ervan om een groot aantal andere producten of de gezondheid, beveiliging of veiligheid van gebruikers ervan te verstoren, te controleren of te beschadigen door directe manipulatie, zoals een centrale systeemfunctie, waaronder netwerkbeheer, configuratiecontrole, virtualisering of verwerking van persoonsgegevens.

3. De Commissie is bevoegd om overeenkomstig artikel 61 gedelegeerde handelingen vast te stellen om bijlage III te wijzigen door in de lijst een nieuwe categorie op te nemen binnen elke klasse van de categorieën producten met digitale elementen en de definitie daarvan te specificeren, een categorie producten van de ene naar de andere klasse over te hevelen 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 de cyberbeveiligingsgerelateerde functionaliteiten of de functie en het niveau van het cyberbeveiligingsrisico dat de producten met digitale elementen inhouden overeenkomstig de in lid 2 van dit artikel bedoelde criteria.

De in de eerste alinea van dit lid bedoelde gedelegeerde handelingen voorzien zo nodig in een minimale overgangsperiode van twaalf maanden, met name wanneer een nieuwe categorie belangrijke producten met digitale elementen wordt toegevoegd aan klasse I of II of wordt overgeheveld van klasse I naar klasse II als vermeld in bijlage III, voordat de desbetreffende conformiteitsbeoordelingsprocedures als bedoeld in artikel 32, leden 2 en 3, van toepassing worden, tenzij een kortere overgangsperiode om dwingende redenen van urgentie gerechtvaardigd is.

4. Uiterlijk op 11 december 2025 stelt de Commissie een uitvoeringshandeling vast met de technische beschrijving van de categorieën producten met digitale elementen van de klassen I en II als vermeld in bijlage III en de technische beschrijving van de categorieën producten met digitale elementen als vermeld in bijlage IV. Die uitvoeringshandeling wordt volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 8

Kritieke producten met digitale elementen

1. De Commissie is bevoegd om overeenkomstig artikel 61 gedelegeerde handelingen ter aanvulling van deze verordening vast te stellen om te bepalen voor welke producten met digitale elementen met de belangrijkste functionaliteit van een productcategorie die is vermeld in bijlage IV bij deze verordening een Europees cyberbeveiligingscertificaat op ten minste het zekerheidsniveau "substantieel" in het kader van een op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregeling moet worden verkregen om de conformiteit met de essentiële cyberbeveiligingsvereisten van bijlage I bij deze verordening of delen daarvan aan te tonen, mits er op grond van Verordening (EU) 2019/881 een Europese cyberbeveiligingscertificeringsregeling voor die categorieën producten met digitale elementen is vastgesteld en beschikbaar is voor de fabrikanten. In die gedelegeerde handelingen wordt het vereiste zekerheidsniveau gespecificeerd, dat in verhouding staat tot het niveau van het cyberbeveiligingsrisico dat aan de producten met digitale elementen verbonden is en rekening houdt met het beoogde doel ervan, met inbegrip van de kritieke afhankelijkheid van in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten ten aanzien van dergelijke producten.

Alvorens dergelijke gedelegeerde handelingen vast te stellen, verricht de Commissie een beoordeling van het potentiële markteffect van de beoogde maatregelen en raadpleegt zij relevante belanghebbenden, waaronder de uit hoofde van Verordening (EU) 2019/881 opgerichte Europese Groep voor cyberbeveiligingscertificering. Bij de beoordeling wordt rekening gehouden met de mate waarin de lidstaten gereed zijn en over de capaciteit beschikken om de desbetreffende Europese cyberbeveiligingscertificeringsregeling toe te passen. Indien er geen gedelegeerde handelingen als bedoeld in de eerste alinea van dit lid zijn vastgesteld, worden producten met digitale elementen met de belangrijkste functionaliteit van een productcategorie als vermeld in bijlage IV onderworpen aan de in artikel 32, lid 3, bedoelde conformiteitsbeoordelingsprocedures.

De in de eerste alinea bedoelde gedelegeerde handelingen voorzien in een minimale overgangsperiode van zes maanden, tenzij een kortere overgangsperiode om dwingende redenen van urgentie gerechtvaardigd is.

2. De Commissie is bevoegd om overeenkomstig artikel 61 gedelegeerde handelingen vast te stellen om bijlage IV te wijzigen door categorieën producten met digitale elementen toe te voegen of te schrappen. Bij het bepalen van dergelijke categorieën kritieke producten met digitale elementen en het vereiste zekerheidsniveau, overeenkomstig lid 1 van dit artikel, houdt de Commissie rekening met de in artikel 7, lid 2, bedoelde criteria en zorgt ze ervoor dat de categorieën producten met digitale elementen ten minste aan een van de volgende criteria voldoen:

a) er is een kritieke afhankelijkheid van in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten ten aanzien van de categorie producten met digitale elementen;

b) incidenten en uitgebuite kwetsbaarheden met betrekking tot de categorie producten met digitale elementen zouden tot ernstige verstoringen van kritieke toeleveringsketens in de hele interne markt kunnen leiden.

Alvorens dergelijke gedelegeerde handelingen vast te stellen, verricht de Commissie een beoordeling van het type als bedoeld in lid 1.

De in de eerste alinea bedoelde gedelegeerde handelingen voorzien in een minimale overgangsperiode van zes maanden, tenzij een kortere overgangsperiode om dwingende redenen van urgentie gerechtvaardigd is.

Artikel 9

Raadpleging van belanghebbenden

1. Bij de voorbereiding van maatregelen ter uitvoering van deze verordening raadpleegt de Commissie relevante belanghebbenden, zoals relevante autoriteiten van de lidstaten, ondernemingen uit de particuliere sector, met inbegrip van micro-ondernemingen en kleine en middelgrote ondernemingen, de opensourcesoftwaregemeenschap, consumentenorganisaties, de academische wereld en relevante agentschappen en organen van de Unie, alsook op het niveau van de Unie opgerichte deskundigengroepen, en houdt zij rekening met hun standpunten. In het bijzonder raadpleegt de Commissie, waar passend, die belanghebbenden op gestructureerde wijze en vraagt zij hun mening wanneer zij:

a) de in artikel 26 bedoelde richtsnoeren opstelt;

b) overeenkomstig artikel 7, lid 4, de technische beschrijvingen van de productcategorieën in bijlage III opstelt, overeenkomstig artikel 7, lid 3, en artikel 8, lid 2, beoordeelt of mogelijke actualiseringen van de lijst van productcategorieën nodig zijn, of de in artikel 8, lid 1, bedoelde beoordeling van het potentiële markteffect verricht, onverminderd artikel 61;

c) voorbereidende werkzaamheden voor de evaluatie en toetsing van deze verordening verricht.

2. De Commissie organiseert regelmatig en ten minste eenmaal per jaar raadplegings- en informatiebijeenkomsten om de standpunten van de in lid 1 bedoelde belanghebbenden over de uitvoering van deze verordening te verzamelen.

Artikel 10

Verbetering van vaardigheden in een cyberveerkrachtige digitale omgeving

Voor de toepassing van deze verordening en om tegemoet te komen aan de behoeften van professionals ter ondersteuning van de uitvoering van deze verordening, bevorderen de lidstaten, waar passend met steun van de Commissie, het Europees kenniscentrum voor cyberbeveiliging en Enisa, en met volledige inachtneming van de verantwoordelijkheid van de lidstaten op onderwijsgebied, maatregelen en strategieën die beogen:

a) vaardigheden op het gebied van cyberbeveiliging te ontwikkelen en organisatorische en technologische instrumenten te creëren om ervoor te zorgen dat er voldoende gekwalificeerde professionals beschikbaar zijn om de activiteiten van de markttoezichtautoriteiten en conformiteitsbeoordelingsinstanties te ondersteunen;

b) te zorgen voor meer samenwerking tussen de particuliere sector, marktdeelnemers — onder meer door om- of bijscholing voor werknemers van fabrikanten —, consumenten, aanbieders van opleidingen en overheidsdiensten, zodat jongeren meer mogelijkheden krijgen om een baan in de cyberbeveiligingssector te vinden.

Artikel 11

Algemene productveiligheid

In afwijking van artikel 2, lid 1, derde alinea, punt b), van Verordening (EU) 2023/988 zijn hoofdstuk III, punt 1, de hoofdstukken V en VII, en de hoofdstukken IX, X en XI van die verordening van toepassing op producten met digitale elementen met betrekking tot aspecten en risico's of risicocategorieën die niet onder deze verordening vallen indien voor die producten geen specifieke veiligheidsvereisten gelden die zijn vastgesteld in andere "harmonisatiewetgeving van de Unie" zoals gedefinieerd in artikel 3, punt 27, van Verordening (EU) 2023/988.

Artikel 12

AI-systemen met een hoog risico

1. Onverminderd de in artikel 15 van Verordening (EU) 2024/1689 vastgestelde vereisten inzake nauwkeurigheid en robuustheid worden producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen en die op grond van artikel 6 van die verordening als AI-systemen met een hoog risico worden aangemerkt, geacht in overeenstemming te zijn met de in artikel 15 van die verordening vastgestelde cyberbeveiligingsvereisten indien:

a) die producten voldoen aan de essentiële cyberbeveiligingsvereisten van deel I van bijlage I;

b) de door de fabrikant ingestelde processen voldoen aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I, en

c) in de krachtens deze verordening afgegeven EU-conformiteitsverklaring wordt aangetoond dat het krachtens artikel 15 van Verordening (EU) 2024/1689 vereiste niveau van bescherming van de cyberbeveiliging wordt bereikt.

2. Op de in lid 1 van dit artikel bedoelde producten met digitale elementen en cyberbeveiligingsvereisten is de relevante conformiteitsbeoordelingsprocedure als voorgeschreven in artikel 43 van Verordening (EU) 2024/1689 van toepassing. Ten behoeve van die beoordeling zijn aangemelde instanties die uit hoofde van Verordening (EU) 2024/1689 bevoegd zijn om de conformiteit van de AI-systemen met een hoog risico te controleren, ook bevoegd om de conformiteit van AI-systemen met een hoog risico die binnen het toepassingsgebied van deze verordening vallen met de vereisten van bijlage I bij deze verordening te controleren, mits de naleving door die aangemelde instanties van de vereisten van artikel 39 van deze verordening in het kader van de aanmeldingsprocedure uit hoofde van Verordening (EU) 2024/1689 is beoordeeld.

3. In afwijking van lid 2 van dit artikel zijn belangrijke producten met digitale elementen die zijn opgenomen in bijlage III bij deze verordening, die worden onderworpen aan de in artikel 32, lid 2, punten a) en b), en lid 3, van deze verordening bedoelde conformiteitsbeoordelingsprocedures en kritieke producten met digitale elementen die zijn opgenomen in bijlage IV bij deze verordening waarvoor een Europees cyberbeveiligingscertificaat op grond van artikel 8, lid 1, van deze verordening moet worden verkregen, of, bij gebreke daarvan, die worden onderworpen aan de in artikel 32, lid 3, van deze verordening bedoelde conformiteitsbeoordelingsprocedures, en die ook worden aangemerkt als AI-systemen met een hoog risico op grond van artikel 6 van Verordening (EU) 2024/1689, en waarop de in bijlage VI bij Verordening (EU) 2024/1689 bedoelde conformiteitsbeoordelingsprocedure op basis van interne controle van toepassing is, onderworpen aan de conformiteitsbeoordelingsprocedures waarin deze verordening voorziet voor zover het de essentiële cyberbeveiligingsvereisten van deze verordening betreft.

4. Fabrikanten van in lid 1 van dit artikel bedoelde producten met digitale elementen kunnen deelnemen aan de in artikel 57 van Verordening (EU) 2024/1689 bedoelde AI-testomgeving voor regelgeving.

HOOFDSTUK II

VERPLICHTINGEN VAN MARKTDEELNEMERS EN BEPALINGEN IN VERBAND MET VRIJE EN OPENSOURCESOFTware

Artikel 13

Verplichtingen van fabrikanten

1. Wanneer fabrikanten een product met digitale elementen in de handel brengen, zorgen zij ervoor dat dat product is ontworpen, ontwikkeld en geproduceerd overeenkomstig de essentiële cyberbeveiligingsvereisten van deel I 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, incidenten te voorkomen en de gevolgen daarvan tot een minimum te beperken, onder meer met betrekking tot de gezondheid en veiligheid van gebruikers.

3. De beoordeling van de cyberbeveiligingsrisico's wordt gedocumenteerd en zo nodig bijgewerkt tijdens een overeenkomstig lid 8 van dit artikel vast te stellen ondersteuningsperiode. Die beoordeling van de cyberbeveiligingsrisico's omvat ten minste een analyse van cyberbeveiligingsrisico's op basis van het beoogde doel en het redelijkerwijs voorzienbaar gebruik, alsook de voorwaarden van het gebruik, van het product met digitale elementen, zoals de operationele omgeving of de te beschermen activa, waarbij rekening wordt gehouden met de verwachte gebruiksduur van het product. In de beoordeling van de cyberbeveiligingsrisico's wordt vermeld of, en zo ja op welke wijze, de beveiligingsvereisten van deel I, punt 2, van bijlage I, van toepassing zijn op het desbetreffende product met digitale elementen en op welke wijze die vereisten worden uitgevoerd op basis van de beoordeling van de cyberbeveiligingsrisico's. Daarin wordt ook aangegeven hoe de fabrikant deel I, punt 1, van bijlage I, en de in deel II van bijlage I, vastgestelde vereisten inzake de respons op kwetsbaarheden toepast.

4. Wanneer de fabrikant een product met digitale elementen in de handel brengt, neemt hij een beoordeling van de in lid 3 van dit artikel bedoelde cyberbeveiligingsrisico's op in de technische documentatie als vereist op grond van artikel 31 en bijlage VII. Voor producten met digitale elementen als bedoeld in artikel 12, die ook onder andere rechtshandelingen van de Unie vallen, kan de beoordeling van de cyberbeveiligingsrisico's deel uitmaken van de risicobeoordeling die op grond van die respectieve rechtshandelingen van de Unie vereist is. Indien bepaalde essentiële cyberbeveiligingsvereisten niet van toepassing zijn op het product met digitale elementen, neemt de fabrikant in die technische documentatie daarvoor een duidelijke motivering op.

5. Met het oog op de naleving van lid 1 betrachten fabrikanten de passende zorgvuldigheid bij de integratie van van derden afkomstige componenten in producten met digitale elementen, zodat die componenten de cyberbeveiliging van het product met digitale elementen niet in gevaar brengen, ook bij integratie van componenten van vrije en opensourcesoftware die niet in het kader van een handelsactiviteit op de markt worden aangeboden.

6. 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 vervaardigt of onderhoudt, en pakken onverwijld de kwetsbaarheid aan en verhelpen die in overeenstemming met de vereisten inzake de respons op kwetsbaarheden van deel II van bijlage I. Wanneer fabrikanten een wijziging van software of hardware hebben ontwikkeld om de kwetsbaarheid van die component aan te pakken, delen zij de desbetreffende code of documentatie met de persoon of entiteit die de component vervaardigt of onderhoudt, indien passend in een machineleesbaar formaat.

7. De fabrikanten documenteren systematisch, op een wijze die in verhouding staat tot de aard en de cyberbeveiligingsrisico's, relevante cyberbeveiligingsaspecten met betrekking tot de producten met digitale elementen, met inbegrip van kwetsbaarheden waarvan zij kennisnemen en alle relevante informatie die door derden wordt verstrekt, en werken, indien van toepassing, de beoordeling van de cyberbeveiligingsrisico's van de producten bij.

8. Fabrikanten zorgen ervoor, wanneer zij een product met digitale elementen in de handel brengen en gedurende de ondersteuningsperiode, dat de kwetsbaarheden van dat product, met inbegrip van de componenten daarvan, doeltreffend en in overeenstemming met de essentiële cyberbeveiligingsvereisten van deel II van bijlage I worden aangepakt.

Fabrikanten bepalen de ondersteuningsperiode op zodanige wijze dat die de verwachte gebruiksduur van het product weerspiegelt, waarbij met name rekening wordt gehouden met redelijke verwachtingen van de gebruikers, de aard van het product, met inbegrip van het beoogde doel van het product, en het relevante Unierecht dat de levensduur van producten met digitale elementen bepaalt. Bij het bepalen van de ondersteuningsperiode kunnen fabrikanten ook rekening houden met de ondersteuningsperioden voor producten met digitale elementen met een soortgelijke functionaliteit die door andere fabrikanten in de handel worden gebracht, de beschikbaarheid van de operationele omgeving, de ondersteuningsperioden voor geïntegreerde componenten die kernfuncties leveren en afkomstig zijn van derden, alsook relevante richtsnoeren van de op grond van artikel 52, lid 15, opgerichte speciale administratievesamenwerkingsgroep (ADCO) en de Commissie. De aangelegenheden waarmee rekening moet worden gehouden om de ondersteuningsperiode te bepalen, worden op zodanige wijze in aanmerking genomen dat de evenredigheid wordt gewaarborgd.

Onverminderd de tweede alinea bedraagt de ondersteuningsperiode ten minste vijf jaar. Wanneer het product met digitale elementen naar verwachting minder dan vijf jaar in gebruik zal zijn, stemt de ondersteuningsperiode overeen met de verwachte gebruiksduur.

Rekening houdend met de ADCO-aanbevelingen als bedoeld in artikel 52, lid 16, kan de Commissie overeenkomstig artikel 61 gedelegeerde handelingen vaststellen ter aanvulling van deze verordening door de minimale ondersteuningsperiode voor specifieke productcategorieën te specificeren wanneer uit de markttoezichtgegevens blijkt dat de ondersteuningsperioden ontoereikend zijn.

Fabrikanten nemen de informatie die in aanmerking is genomen om de ondersteuningsperiode van een product met digitale elementen te bepalen, op in de in bijlage VII beschreven technische documentatie.

Fabrikanten beschikken over passende beleidslijnen en procedures, met inbegrip van een gecoördineerd beleid inzake openbaarmaking van kwetsbaarheden, als bedoeld in deel II, 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.

9. Fabrikanten zorgen ervoor dat elke beveiligingsupdate, als bedoeld in deel II, punt 8, van bijlage I, die tijdens de ondersteuningsperiode ter beschikking van de gebruikers is gesteld, na afgifte ten minste gedurende tien jaar beschikbaar blijft, of gedurende de rest van de ondersteuningsperiode, indien die langer is.

10. Wanneer een fabrikant opeenvolgende ingrijpend gewijzigde versies van een softwareproduct in de handel heeft gebracht, mag die fabrikant ervoor zorgen dat alleen voor de laatst in de handel gebrachte versie aan het essentiële cyberbeveiligingsvereiste van deel II, punt 2, van bijlage I wordt voldaan, mits de gebruikers van de eerder in de handel gebrachte versies kosteloos toegang hebben tot de laatst in de handel gebrachte versie en geen extra kosten hoeven te maken voor de aanpassing van de hardware- en softwareomgeving waarin zij de oorspronkelijke versie van dat product gebruiken.

11. Fabrikanten kunnen openbare softwarearchieven bijhouden om de toegang van gebruikers tot historische versies te verbeteren. In die gevallen worden gebruikers duidelijk en op gemakkelijk toegankelijke wijze geïnformeerd over de risico's in verband met het gebruik van niet-ondersteunde software.

12. Alvorens een product met digitale elementen in de handel te brengen, stellen fabrikanten de in artikel 31 bedoelde technische documentatie op.

Zij voeren de in artikel 32 bedoelde gekozen conformiteitsbeoordelingsprocedures uit of laten die uitvoeren.

Wanneer met die conformiteitsbeoordelingsprocedure is aangetoond dat het product met digitale elementen voldoet aan de essentiële cyberbeveiligingsvereisten van deel I van bijlage I en dat de door de fabrikant ingestelde processen voldoen aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I, stellen de fabrikanten de EU-conformiteitsverklaring op overeenkomstig artikel 28 en brengen zij de CE-markering aan overeenkomstig artikel 30.

13. Fabrikanten houden de technische documentatie en de EU-conformiteitsverklaring gedurende ten minste tien jaar nadat het product met digitale elementen in de handel is gebracht of gedurende de ondersteuningsperiode indien die langer is, ter beschikking van de markttoezichtautoriteiten.

14. Fabrikanten voeren procedures in om de conformiteit met deze verordening te waarborgen van producten met digitale elementen die deel uitmaken van een productiereeks. Fabrikanten houden 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 in artikel 27 bedoelde geharmoniseerde normen, Europese cyberbeveiligingscertificeringsregelingen of 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.

15. Fabrikanten zorgen ervoor dat op hun producten met digitale elementen een type-, partij- of serienummer, dan wel een ander identificatiemiddel is aangebracht, of wanneer dat niet mogelijk is, dat die informatie op de verpakking ervan of in een bij het product met digitale elementen gevoegd document is vermeld.

16. Fabrikanten vermelden de naam, de geregistreerde handelsnaam of het geregistreerde merk van de fabrikant en het postadres, het e-mailadres of andere digitale contactgegevens, alsook, in voorkomend geval, de website waarop contact met de fabrikant kan worden opgenomen, op het product met digitale elementen, op de verpakking ervan of in een bij het product met digitale elementen gevoegd document. Die informatie wordt ook opgenomen in de in bijlage II vermelde informatie en instructies voor de gebruiker. De contactgegevens worden gesteld in een taal die de gebruikers en de markttoezichtautoriteiten gemakkelijk kunnen begrijpen.

17. Voor de toepassing van deze verordening wijzen fabrikanten een centraal contactpunt aan om gebruikers in staat te stellen rechtstreeks en snel met hen te communiceren, onder meer om de melding van kwetsbaarheden van het product met digitale elementen te vergemakkelijken.

Fabrikanten zorgen ervoor dat het centraal contactpunt gemakkelijk te identificeren is voor de gebruikers. Zij nemen het centrale contactpunt ook op in de in bijlage II vermelde informatie en instructies voor de gebruiker.

Het centrale contactpunt biedt gebruikers de mogelijkheid om de communicatiemiddelen van hun voorkeur te kiezen en beperkt die middelen niet tot geautomatiseerde hulpmiddelen.

18. Fabrikanten zorgen ervoor dat producten met digitale elementen vergezeld gaan van de in bijlage II vermelde informatie en instructies voor de gebruiker, op papier of in elektronische vorm. Die informatie en instructies worden verstrekt in een taal die de gebruikers en markttoezichtautoriteiten gemakkelijk kunnen begrijpen. Zij zijn duidelijk, begrijpelijk en leesbaar. Zij maken de veilige installatie, de veilige werking en het veilig gebruik van producten met digitale elementen mogelijk. Fabrikanten houden de in bijlage II vermelde informatie en instructies voor de gebruiker gedurende ten minste tien jaar nadat het product met digitale elementen in de handel is gebracht of gedurende de ondersteuningsperiode indien die langer is, ter beschikking van de gebruikers en de markttoezichtautoriteiten. Wanneer die informatie en instructies online worden verstrekt, zorgen de fabrikanten ervoor dat ze toegankelijk, gebruiksvriendelijk en online beschikbaar zijn gedurende ten minste tien jaar nadat het product met digitale elementen in de handel is gebracht of gedurende de ondersteuningsperiode indien die langer is.

19. Fabrikanten zorgen ervoor dat de einddatum van de in lid 8 bedoelde ondersteuningsperiode, met inbegrip van ten minste de maand en het jaar, op het moment van aankoop op gemakkelijk toegankelijke wijze duidelijk en begrijpelijk wordt gespecificeerd en, in voorkomend geval, op het product met digitale elementen, op de verpakking ervan of met digitale middelen.

Indien dat in verband met de aard van het product met digitale elementen technisch haalbaar is, stellen fabrikanten gebruikers door de weergave van een notificatie ervan op de hoogte dat hun product met digitale elementen het einde van de ondersteuningsperiode heeft bereikt.

20. Fabrikanten verstrekken een kopie van de EU-conformiteitsverklaring of een vereenvoudigde EU-conformiteitsverklaring bij het product met digitale elementen. Wanneer een vereenvoudigde EU-conformiteitsverklaring wordt verstrekt, bevat die het juiste internetadres waarop de volledige EU-conformiteitsverklaring kan worden geraadpleegd.

21. Vanaf het in de handel brengen en gedurende de ondersteuningsperiode 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 cyberbeveiligingsvereisten van bijlage I, onmiddellijk de nodige corrigerende maatregelen om dat 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.

22. Fabrikanten verstrekken op een met redenen omkleed verzoek van een markttoezichtautoriteit aan die autoriteit, in een taal die die autoriteit 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 cyberbeveiligingsvereisten van bijlage I aan te tonen. Fabrikanten 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.

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

24. De Commissie kan door middel van uitvoeringshandelingen, rekening houdend met Europese of internationale normen en beste praktijken, het formaat en de elementen van de in deel II, punt 1, van bijlage I bedoelde softwarestuklijst specificeren. Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

25. Om te beoordelen of de lidstaten en de Unie als geheel afhankelijk zijn van softwarecomponenten en met name van componenten die als vrije en opensourcesoftware kunnen worden aangemerkt, kan de ADCO besluiten een EU-brede afhankelijkheidsbeoordeling uit te voeren voor specifieke categorieën producten met digitale elementen. Daartoe kunnen markttoezichtautoriteiten fabrikanten van dergelijke categorieën producten met digitale elementen verzoeken de desbetreffende softwarestuklijsten als bedoeld in deel II, punt 1, van bijlage I te verstrekken. Op basis van die informatie kunnen de markttoezichtautoriteiten aan de ADCO geanonimiseerde en geaggregeerde informatie over softwareafhankelijkheden verstrekken. De ADCO dient een verslag over de resultaten van de afhankelijkheidsbeoordeling in bij de op grond van artikel 14 van Richtlijn (EU) 2022/2555 opgerichte samenwerkingsgroep.

Artikel 14

Rapportageverplichtingen van fabrikanten

1. Een fabrikant doet tegelijkertijd aan het overeenkomstig lid 7 van dit artikel als coördinator aangewezen CSIRT en aan Enisa melding van elke actief uitgebuite kwetsbaarheid in het product met digitale elementen waarvan hij kennis krijgt. De fabrikant doet van die actief uitgebuite kwetsbaarheid melding via het op grond van artikel 16 opgerichte centrale meldingsplatform.

2. Ten behoeve van de in lid 1 bedoelde melding dient de fabrikant het volgende in:

a) een vroegtijdige waarschuwing over een actief uitgebuite kwetsbaarheid, zonder onnodige vertraging en in elk geval binnen 24 uur nadat de fabrikant er kennis van heeft gekregen, met vermelding, in voorkomend geval, van de lidstaten op het grondgebied waarvan de fabrikant ervan op de hoogte is dat zijn product met digitale elementen beschikbaar is gesteld;

b) tenzij de relevante informatie reeds is verstrekt, een kwetsbaarheidsmelding, zonder onnodige vertraging en in elk geval binnen 72 uur nadat de fabrikant kennis heeft gekregen van de actief uitgebuite kwetsbaarheid, waarin algemene informatie wordt verstrekt, voor zover beschikbaar, over het desbetreffende product met digitale elementen, de algemene aard van de uitbuiting en van de betroffen kwetsbaarheid, alsook alle genomen corrigerende of risicobeperkende maatregelen, en corrigerende of risicobeperkende maatregelen die gebruikers kunnen nemen, en waarin in voorkomend geval ook wordt aangegeven hoe gevoelig de fabrikant de gemelde informatie acht;

c) tenzij de relevante informatie reeds is verstrekt, een eindverslag, uiterlijk 14 dagen nadat een corrigerende of risicobeperkende maatregel beschikbaar is, waarin ten minste het volgende is opgenomen:

   i) een beschrijving van de kwetsbaarheid, inclusief de ernst en de gevolgen ervan;

   ii) indien beschikbaar, informatie over elke kwaadwillige actor die de kwetsbaarheid heeft uitgebuit of die de kwetsbaarheid aan het uitbuiten is;

   iii) details over de beveiligingsupdate of andere corrigerende maatregelen die beschikbaar zijn gesteld om de kwetsbaarheid te verhelpen.

3. Een fabrikant doet tegelijkertijd aan het overeenkomstig lid 7 van dit artikel als coördinator aangewezen CSIRT en aan Enisa melding van elk ernstig incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen waarvan hij kennis krijgt. De fabrikant doet van dat incident melding via het op grond van artikel 16 opgerichte centrale meldingsplatform.

4. Ten behoeve van de in lid 3 bedoelde melding dient de fabrikant het volgende in:

a) een vroegtijdige waarschuwing over een ernstig incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen, zonder onnodige vertraging en in elk geval binnen 24 uur nadat de fabrikant er kennis van heeft gekregen, waarin ten minste wordt vermeld of het incident vermoedelijk door onwettige of kwaadwillige handelingen is veroorzaakt, en waarin, in voorkomend geval, ook de lidstaten worden vermeld op het grondgebied waarvan de fabrikant ervan op de hoogte is dat zijn product met digitale elementen beschikbaar is gesteld;

b) tenzij de relevante informatie reeds is verstrekt, een incidentmelding, zonder onnodige vertraging en in elk geval binnen 72 uur nadat de fabrikant kennis heeft gekregen van het incident, waarin algemene informatie wordt verstrekt, voor zover beschikbaar, over de aard van het incident, een eerste beoordeling van het incident, alsook alle genomen corrigerende of risicobeperkende maatregelen, en corrigerende of risicobeperkende maatregelen die gebruikers kunnen nemen, en waarin in voorkomend geval ook wordt aangegeven hoe gevoelig de fabrikant de gemelde informatie acht;

c) tenzij de relevante informatie reeds is verstrekt, binnen één maand na de indiening van de incidentmelding uit hoofde van punt b), een eindverslag waarin ten minste het volgende is opgenomen:

   i) een gedetailleerde beschrijving van het incident, inclusief de ernst en de gevolgen ervan;

   ii) het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;

   iii) toegepaste en lopende beperkende maatregelen.

5. Voor de toepassing van lid 3 wordt een incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen als ernstig beschouwd wanneer:

a) het negatieve gevolgen heeft of negatieve gevolgen kan hebben voor het vermogen van een product met digitale elementen om de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gevoelige of belangrijke gegevens of functies te beschermen, of

b) het heeft geleid of kan leiden tot de invoering of uitvoering van kwaadwillige code in een product met digitale elementen of in de netwerk- en informatiesystemen van een gebruiker van het product met digitale elementen.

6. Indien nodig kan het als coördinator aangewezen CSIRT dat als eerste de melding ontvangt, fabrikanten verzoeken een tussentijds verslag te verstrekken over relevante updates van de status van de actief uitgebuite kwetsbaarheid of het ernstige incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen.

7. De in de leden 1 en 3 van dit artikel bedoelde meldingen worden ingediend via het in artikel 16 bedoelde centrale meldingsplatform met gebruikmaking van een van de in artikel 16, lid 1, bedoelde elektronische endpoints voor melding. De melding wordt ingediend met gebruikmaking van het elektronische endpoint voor melding van het als coördinator aangewezen CSIRT van de lidstaat waar de fabrikanten hun hoofdvestiging in de Unie hebben, en is tegelijkertijd toegankelijk voor Enisa.

Voor de toepassing van deze verordening wordt een fabrikant geacht zijn hoofdvestiging in de Unie te hebben in de lidstaat waar de besluiten met betrekking tot de cyberbeveiliging van zijn product met digitale elementen hoofdzakelijk worden genomen. Indien niet kan worden bepaald welke lidstaat dat is, wordt de hoofdvestiging geacht zich te bevinden in de lidstaat waar de betrokken fabrikant de vestiging met het grootste aantal werknemers in de Unie heeft.

Indien een fabrikant geen hoofdvestiging in de Unie heeft, dient hij de in de leden 1 en 3 bedoelde meldingen in met gebruikmaking van het elektronische endpoint voor melding van het als coördinator aangewezen CSIRT in de lidstaat die bepaald is op grond van onderstaande volgorde en op basis van de informatie waarover de fabrikant beschikt:

a) de lidstaat waar de gemachtigde vertegenwoordiger die namens de fabrikant optreedt voor het grootste aantal producten met digitale elementen van die fabrikant, is gevestigd;

b) de lidstaat waar de importeur is gevestigd die het grootste aantal producten met digitale elementen van die fabrikant in de handel brengt;

c) de lidstaat waar de distributeur is gevestigd die het grootste aantal producten met digitale elementen van die fabrikant op de markt aanbiedt;

d) de lidstaat waar het grootste aantal gebruikers van producten met digitale elementen van die fabrikant is gevestigd.

Met betrekking tot de derde alinea, punt d), kan een fabrikant bij hetzelfde als coördinator aangewezen CSIRT waaraan hij de eerste melding heeft gedaan, meldingen indienen in verband met elke volgende actief uitgebuite kwetsbaarheid of ernstig incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen.

8. Nadat de fabrikant kennis heeft gekregen van een actief uitgebuite kwetsbaarheid of een ernstig incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen, stelt hij de getroffen gebruikers van het product met digitale elementen en indien passend alle gebruikers, op de hoogte van die kwetsbaarheid of van dat incident en, indien nodig, van risicobeperking en corrigerende maatregelen die de gebruikers kunnen nemen om de gevolgen van die kwetsbaarheid of dat incident te beperken, indien passend in een gestructureerd, machineleesbaar formaat dat gemakkelijk automatisch verwerkbaar is. Indien de fabrikant de gebruikers van het product met digitale elementen niet tijdig op de hoogte brengt, kunnen de als coördinatoren aangewezen CSIRT's dergelijke informatie verstrekken aan de gebruikers wanneer dat evenredig en noodzakelijk wordt geacht om de gevolgen van die kwetsbaarheid of dat incident te voorkomen of te beperken.

9. Uiterlijk op 11 december 2025 stelt de Commissie overeenkomstig artikel 61 van deze verordening gedelegeerde handelingen vast teneinde deze verordening aan te vullen door de voorwaarden te specificeren voor de toepassing van de cyberbeveiligingsgerelateerde redenen voor het uitstellen van de verspreiding van meldingen als bedoeld in artikel 16, lid 2 van deze verordening. De Commissie werkt samen met het op grond van artikel 15 van Richtlijn (EU) 2022/2555 opgerichte CSIRT-netwerk en Enisa bij het opstellen van de ontwerpen van gedelegeerde handelingen.

10. De Commissie kan door middel van uitvoeringshandelingen het formaat en de procedures van de in dit artikel en in de artikelen 15 en 16 bedoelde meldingen nader specificeren. Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld. De Commissie werkt samen met het CSIRT-netwerk en Enisa bij het opstellen van die ontwerpuitvoeringshandelingen.

Artikel 15

Vrijwillige melding

1. Fabrikanten en andere natuurlijke of rechtspersonen kunnen op vrijwillige basis van elke kwetsbaarheid in een product met digitale elementen alsook van cyberdreigingen die van invloed kunnen zijn op het risicoprofiel van een product met digitale elementen, melding doen aan een als coördinator aangewezen CSIRT of aan Enisa.

2. Fabrikanten en andere natuurlijke of rechtspersonen kunnen op vrijwillige basis van elk incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen en van bijna-incidenten die tot een dergelijk incident hadden kunnen leiden, melding doen aan een als coördinator aangewezen CSIRT of aan Enisa.

3. Het als coördinator aangewezen CSIRT of Enisa verwerkt de in de leden 1 en 2 van dit artikel bedoelde meldingen volgens de in artikel 16 vastgestelde procedure.

Het als coördinator aangewezen CSIRT kan voorrang geven aan de verwerking van verplichte meldingen boven vrijwillige meldingen.

4. Wanneer een andere natuurlijke of rechtspersoon dan de fabrikant melding doet van een actief uitgebuite kwetsbaarheid of een ernstig incident dat gevolgen heeft voor de beveiliging van een product met digitale elementen overeenkomstig lid 1 of lid 2, stelt het als coördinator aangewezen CSIRT de fabrikant daarvan zonder onnodige vertraging op de hoogte.

5. De als coördinatoren aangewezen CSIRT's en Enisa waarborgen de vertrouwelijkheid en passende bescherming van de door de meldende natuurlijke of rechtspersoon verstrekte informatie. Onverminderd de voorkoming van, het onderzoek naar en de opsporing en de vervolging van strafbare feiten, mag vrijwillige melding er niet toe leiden dat een meldende natuurlijke of rechtspersoon bijkomende verplichtingen worden opgelegd waaraan zij niet onderworpen zou zijn geweest indien zij geen melding had gedaan.

Artikel 16

Oprichting van een centraal meldingsplatform

1. Ten behoeve van de meldingen bedoeld in artikel 14, leden 1 en 3, en artikel 15, leden 1 en 2, en om de rapportageverplichtingen van fabrikanten te vereenvoudigen, richt Enisa een centraal meldingsplatform op. De dagelijkse werkzaamheden van dat centrale meldingsplatform worden beheerd en uitgevoerd door Enisa. De architectuur van het centrale meldingsplatform stelt de lidstaten en Enisa in staat hun eigen elektronische endpoints voor melding op te zetten.

2. Na ontvangst van een melding verspreidt het als coördinator aangewezen CSIRT die de melding als eerste ontvangt, de melding onverwijld via het centrale meldingsplatform onder de CSIRT's die zijn aangewezen als coördinatoren op het grondgebied waarvan de fabrikant heeft aangegeven dat het product met digitale elementen beschikbaar is gesteld.

In uitzonderlijke omstandigheden, en met name op verzoek van de fabrikant en in het licht van het gevoeligheidsniveau van de gemelde informatie zoals aangegeven door de fabrikant krachtens artikel 14, lid 2, punt a), van deze verordening, kan de verspreiding van de melding op basis van gegronde cyberbeveiligingsgerelateerde redenen worden uitgesteld gedurende een periode die niet langer dan strikt noodzakelijk is, ook wanneer een kwetsbaarheid onderworpen is aan een procedure voor gecoördineerde bekendmaking van kwetsbaarheden als bedoeld in artikel 12, lid 1, van Richtlijn (EU) 2022/2555. Wanneer een CSIRT besluit een melding achter te houden, stelt het CSIRT Enisa onmiddellijk in kennis van het besluit en verstrekt het zowel een motivering voor het achterhouden van de melding als een indicatie van wanneer het de melding zal verspreiden overeenkomstig de in dit lid vastgestelde verspreidingsprocedure. Enisa kan het CSIRT ondersteunen bij de toepassing van cyberbeveiligingsgerelateerde redenen met betrekking tot het uitstellen van de verspreiding van de melding.

In zeer uitzonderlijke omstandigheden, wanneer de fabrikant in de in artikel 14, lid 2, punt b), bedoelde melding aangeeft:

a) dat de gemelde kwetsbaarheid actief wordt uitgebuit door een kwaadwillige actor en, volgens de beschikbare informatie, wordt uitgebuit in geen enkele andere lidstaat dan die van het als coördinator aangewezen CSIRT waaraan de fabrikant de kwetsbaarheid heeft gemeld;

b) dat elke onmiddellijke verdere verspreiding van de gemelde kwetsbaarheid waarschijnlijk zou leiden tot de verstrekking van informatie waarvan de bekendmaking strijdig zou zijn met de wezenlijke belangen van die lidstaat, of

c) dat de gemelde kwetsbaarheid een dreigend hoog cyberbeveiligingsrisico vormt als gevolg van de verdere verspreiding;

zullen uitsluitend de informatie dat de fabrikant een melding heeft gedaan, de algemene informatie over het product, de informatie over de algemene aard van de uitbuiting en de informatie dat er beveiligingsgerelateerde redenen zijn aangevoerd, tegelijkertijd aan Enisa ter beschikking worden gesteld totdat de volledige melding wordt verspreid onder de betrokken CSIRT's en Enisa. Indien Enisa op basis van die informatie van oordeel is dat er een systeemrisico bestaat dat gevolgen heeft voor de veiligheid op de interne markt, beveelt Enisa het ontvangende CSIRT aan de volledige melding onder de andere als coördinatoren aangewezen CSIRT's en Enisa zelf te verspreiden.

3. Na ontvangst van een melding van een actief uitgebuite kwetsbaarheid in een product met digitale elementen of van een ernstig incident dat gevolgen heeft voor de beveiliging van een product met digitale elementen, verstrekken de als coördinatoren aangewezen CSIRT's de markttoezichtautoriteiten van hun respectieve lidstaten de gemelde informatie die de markttoezichtautoriteiten nodig hebben om hun verplichtingen uit hoofde van deze verordening na te komen.

4. Enisa neemt passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van het centrale meldingsplatform en de informatie die via het centrale meldingsplatform wordt ingediend of verspreid, te beheren. Zij doet zonder onnodige vertraging melding aan het CSIRT-netwerk en aan de Commissie van elk beveiligingsincident dat gevolgen heeft voor het centrale meldingsplatform.

5. Enisa verstrekt en voert, in samenwerking met het CSIRT-netwerk, specificaties uit voor de technische, operationele en organisatorische maatregelen met betrekking tot de oprichting, het onderhoud en de veilige werking van het in lid 1 bedoelde centrale meldingsplatform, waaronder ten minste de beveiligingsregelingen in verband met de oprichting, de werking en het onderhoud van het centrale meldingsplatform, alsook de elektronische endpoints voor melding die zijn opgezet door de CSIRT's die zijn aangewezen als coördinatoren op nationaal niveau en door Enisa op Unieniveau, met inbegrip van procedurele aspecten om ervoor te zorgen dat, wanneer voor een gemelde kwetsbaarheid geen corrigerende of risicobeperkende maatregelen beschikbaar zijn, informatie over die kwetsbaarheid wordt gedeeld in overeenstemming met strikte beveiligingsprotocollen en alleen voor zover dat noodzakelijk is.

6. Wanneer een als coördinator aangewezen CSIRT op de hoogte is gebracht van een actief uitgebuite kwetsbaarheid in het kader van een procedure voor gecoördineerde bekendmaking van kwetsbaarheden als bedoeld in artikel 12, lid 1, van Richtlijn (EU) 2022/2555, kan het als coördinator aangewezen CSIRT dat de melding als eerste ontvangt, de verspreiding van de desbetreffende melding via het centrale meldingsplatform op basis van gegronde cyberbeveiligingsgerelateerde redenen uitstellen gedurende een periode die niet langer dan strikt noodzakelijk is en totdat de bij de gecoördineerde bekendmaking van kwetsbaarheden betrokken partijen hun toestemming voor bekendmaking hebben gegeven. Dat vereiste belet fabrikanten niet om op vrijwillige basis een dergelijke kwetsbaarheid in overeenstemming met de procedure van dit artikel te melden.

Artikel 17

Andere bepalingen in verband met melding

1. Enisa kan aan het uit hoofde van artikel 16 van Richtlijn (EU) 2022/2555 opgerichte Europese netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) informatie verstrekken waarvan melding is gedaan op grond van artikel 14, leden 1 en 3, en artikel 15, leden 1 en 2, van deze verordening, indien die informatie relevant is voor het gecoördineerde beheer van grootschalige incidenten en crises op het gebied van cyberbeveiliging op operationeel niveau. Om die relevantie te bepalen, kan Enisa, indien beschikbaar, technische analyses die door het CSIRT-netwerk worden uitgevoerd, in aanmerking nemen.

2. Indien bewustmaking van het publiek noodzakelijk is om een ernstig incident met gevolgen voor de beveiliging van het product met digitale elementen te voorkomen of te beperken of om een lopend incident af te handelen, of indien de bekendmaking van het incident anderszins in het algemeen belang is, kan het als coördinator aangewezen CSIRT van de betrokken lidstaat, na raadpleging van de betrokken fabrikant en, indien passend, in samenwerking met Enisa, het publiek over het incident informeren of de fabrikant verplichten dat te doen.

3. Enisa stelt, op basis van de op grond van artikel 14, leden 1 en 3, en artikel 15, leden 1 en 2, van deze verordening ontvangen meldingen, om de 24 maanden een technisch verslag op over opkomende trends met betrekking tot cyberbeveiligingsrisico's in producten met digitale elementen en dient dat in bij de samenwerkingsgroep die is opgericht op grond van artikel 14 van Richtlijn (EU) 2022/2555. Het eerste verslag wordt ingediend binnen 24 maanden nadat de in artikel 14, leden 1 en 3, van deze verordening vastgestelde verplichtingen van toepassing worden. Enisa neemt relevante informatie uit zijn technische verslagen op in zijn verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie op grond van artikel 18 van Richtlijn (EU) 2022/2555.

4. De loutere handeling van melding overeenkomstig artikel 14, leden 1 en 3, of artikel 15, leden 1 en 2, brengt voor de meldende natuurlijke of rechtspersoon geen verhoogde aansprakelijkheid met zich mee.

5. Nadat een beveiligingsupdate of een andere vorm van corrigerende of risicobeperkende maatregel beschikbaar is, voegt Enisa, in overleg met de fabrikant van het product met digitale elementen, de openbaar bekende kwetsbaarheid waarvan op grond van artikel 14, lid 1, of artikel 15, lid 1, van deze verordening melding is gedaan, toe aan de op grond van artikel 12, lid 2, van Richtlijn (EU) 2022/2555 opgerichte Europese kwetsbaarheidsdatabase.

6. De als coördinatoren aangewezen CSIRT's verlenen helpdeskondersteuning aan fabrikanten met betrekking tot de rapportageverplichtingen op grond van artikel 14, en met name aan fabrikanten die als micro-onderneming of als kleine of middelgrote onderneming kunnen worden aangemerkt.

Artikel 18

Gemachtigde vertegenwoordigers

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

2. De verplichtingen uit hoofde van artikel 13, leden 1 tot en met 11, artikel 13, lid 12, eerste alinea, en artikel 13, lid 14, 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. De gemachtigde vertegenwoordiger legt op verzoek een kopie van het mandaat over aan de markttoezichtautoriteiten. Het mandaat stelt de gemachtigde vertegenwoordiger in staat ten minste het volgende te doen:

a) hij houdt de EU-conformiteitsverklaring als bedoeld in artikel 28 en de technische documentatie als bedoeld in artikel 31 gedurende een periode van ten minste tien jaar nadat het product met digitale elementen in de handel is gebracht of gedurende de ondersteuningsperiode indien die langer is, 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 19

Verplichtingen van importeurs

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

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

a) de fabrikant de juiste in artikel 32 bedoelde conformiteitsbeoordelingsprocedures heeft uitgevoerd;

b) de fabrikant de technische documentatie heeft opgesteld;

c) het product met digitale elementen is voorzien van de in artikel 30 bedoelde CE-markering en vergezeld gaat van de in artikel 13, lid 20, bedoelde EU-conformiteitsverklaring en de in bijlage II vastgestelde informatie en instructies voor de gebruiker, in een taal die gebruikers en markttoezichtautoriteiten gemakkelijk kunnen begrijpen;

d) de fabrikant aan de vereisten van artikel 13, leden 15, 16 en 19, heeft voldaan.

Voor de toepassing van dit lid moeten importeurs de nodige documenten kunnen verstrekken waaruit blijkt dat aan de vereisten van dit artikel is voldaan.

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 deze verordening, brengt de importeur het product niet in de handel voordat dat product of de door de fabrikant ingestelde processen in overeenstemming zijn gebracht met deze verordening. Bovendien brengt de importeur, indien het product met digitale elementen een significant cyberbeveiligingsrisico inhoudt, de fabrikant en de markttoezichtautoriteiten daarvan op de hoogte.

Wanneer een importeur redenen heeft om aan te nemen dat een product met digitale elementen in het licht van niet-technische risicofactoren een significant cyberbeveiligingsrisico kan inhouden, stelt de importeur de markttoezichtautoriteiten daarvan op de hoogte. Na ontvangst van die informatie volgen de markttoezichtautoriteiten de in artikel 54, lid 2, bedoelde procedures.

4. Importeurs vermelden hun naam, geregistreerde handelsnaam of geregistreerde merk, het postadres, het e-mailadres of een ander digitaal communicatiemiddel, alsook, in voorkomend geval, de website waarop met hen contact kan worden opgenomen, op het product met digitale elementen, op de verpakking ervan 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 die weten of redenen hebben om aan te nemen dat een door hen in de handel gebracht product met digitale elementen niet in overeenstemming is met deze verordening, nemen onmiddellijk de nodige corrigerende maatregelen om ervoor te zorgen dat het product met digitale elementen in overeenstemming wordt gebracht met deze verordening, of om het product zo nodig uit de handel te nemen of terug te roepen.

Wanneer importeurs kennis krijgen van een kwetsbaarheid in het product met digitale elementen, stellen zij de fabrikant zonder onnodige vertraging 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, daarvan onmiddellijk op de hoogte, waarbij zij in het bijzonder de non-conformiteit en alle genomen corrigerende maatregelen uitvoerig beschrijven.

6. Importeurs houden gedurende ten minste tien jaar nadat het product met digitale elementen in de handel is gebracht of gedurende de ondersteuningsperiode indien die langer is, 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.

7. Importeurs verstrekken op een met redenen omkleed verzoek van een markttoezichtautoriteit aan die autoriteit alle benodigde informatie en documentatie, schriftelijk of in elektronische vorm, om de conformiteit van het product met digitale elementen met de essentiële cyberbeveiligingsvereisten van deel I van bijlage I, en van de processen die de fabrikant heeft ingesteld met de essentiële cyberbeveiligingsvereisten van deel II 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.

8. 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 die 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 20

Verplichtingen van distributeurs

1. Distributeurs die een product met digitale elementen op de markt aanbieden, betrachten de nodige zorgvuldigheid in verband met de vereisten 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 artikel 13, leden 15, 16, 18, 19 en 20, en artikel 19, lid 4, en alle nodige documenten hebben verstrekt aan de distributeur.

3. Wanneer een distributeur, op grond van informatie in zijn bezit, 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 cyberbeveiligingsvereisten van 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 met deze verordening. Bovendien brengt de distributeur, indien het product met digitale elementen een significant cyberbeveiligingsrisico inhoudt, de fabrikant en de markttoezichtautoriteiten daarvan zonder onnodige vertraging op de hoogte.

4. Distributeurs die, op grond van informatie in hun bezit, 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 deze verordening, 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 kennis krijgen van een kwetsbaarheid in het product met digitale elementen, stellen zij de fabrikant zonder onnodige vertraging 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 daarvan 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 die 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 deze verordening 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, op grond van informatie in zijn bezit, 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 zonder onnodige vertraging in kennis van die 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 21

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 artikelen 13 en 14 voldoen wanneer die importeur of distributeur een product met digitale elementen onder zijn naam of merk in de handel brengt of een ingrijpende wijziging uitvoert aan een reeds in de handel gebrachte product met digitale elementen.

Artikel 22

Andere gevallen waarin de verplichtingen van fabrikanten van toepassing zijn

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

2. De in lid 1 van dit artikel bedoelde persoon moet aan de in de artikelen 13 en 14, vermelde verplichtingen voldoen voor het deel van het product met digitale elementen 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 23

Identificatie van marktdeelnemers

1. Marktdeelnemers verstrekken de markttoezichtautoriteiten op verzoek de volgende informatie:

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

b) indien beschikbaar, 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 aan hen is geleverd, en tot tien jaar nadat zij het product met digitale elementen hebben geleverd.

Artikel 24

Verplichtingen van opensourcesoftwarestewards

1. Opensourcesoftwarestewards voeren een cyberbeveiligingsbeleid in en documenteren dat op een verifieerbare manier om de ontwikkeling van een veilig product met digitale elementen en een effectieve aanpak van kwetsbaarheden door de ontwikkelaars van dat product te bevorderen. Dat beleid bevordert ook de vrijwillige melding van kwetsbaarheden zoals bepaald in artikel 15 door de ontwikkelaars van dat product en houdt rekening met de specifieke aard van de opensourcesoftwaresteward en de juridische en organisatorische regelingen waaraan die is onderworpen. Dat beleid omvat met name aspecten die verband houden met het documenteren, aanpakken en verhelpen van kwetsbaarheden en bevordert de uitwisseling van informatie over ontdekte kwetsbaarheden binnen de opensourcegemeenschap.

2. Opensourcesoftwarestewards werken op verzoek van markttoezichtautoriteiten met hen samen om de cyberbeveiligingsrisico's van producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt, te beperken.

Op een met redenen omkleed verzoek van een markttoezichtautoriteit verstrekken opensourcesoftwarestewards die autoriteit, in een taal die die autoriteit gemakkelijk kan begrijpen, de in lid 1 bedoelde documentatie op papier of in elektronische vorm.

3. De verplichtingen van artikel 14, lid 1, zijn van toepassing op opensourcesoftwarestewards voor zover zij betrokken zijn bij de ontwikkeling van de producten met digitale elementen. De verplichtingen van artikel 14, leden 3 en 8, zijn van toepassing op opensourcesoftwarestewards voor zover ernstige incidenten die gevolgen hebben voor de beveiliging van producten met digitale elementen van invloed zijn op de netwerk- en informatiesystemen die door de opensourcesoftwarestewards voor de ontwikkeling van dergelijke producten worden geleverd.

Artikel 25

Beveiligingsattestatie van vrije en opensourcesoftware

Om de naleving van de in artikel 13, lid 5, vastgestelde passendezorgvuldigheidsverplichting te vergemakkelijken, met name ten aanzien van fabrikanten die vrije en opensourcesoftwarecomponenten in hun producten met digitale elementen integreren, is de Commissie bevoegd om overeenkomstig artikel 61 gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen door vrijwillige beveiligingsattestatieprogramma's vast te stellen die ontwikkelaars of gebruikers van producten met digitale elementen die als vrije en opensourcesoftware aangemerkt worden, alsook andere derden in staat stellen de conformiteit van dergelijke producten met alle of bepaalde essentiële cyberbeveiligingsvereisten of andere in deze verordening vastgestelde verplichtingen te beoordelen.

Artikel 26

Richtsnoeren

1. Om de uitvoering te vergemakkelijken en de consistentie van die uitvoering te waarborgen, publiceert de Commissie richtsnoeren om de marktdeelnemers te helpen bij de toepassing van deze verordening, met bijzondere aandacht voor de wijze waarop de naleving door kleine, middelgrote en micro-ondernemingen kan worden vergemakkelijkt.

2. Wanneer de Commissie voornemens is de in lid 1 bedoelde richtsnoeren te verstrekken, gaat zij ten minste in op de volgende aspecten:

a) het toepassingsgebied van deze verordening, met bijzondere aandacht voor oplossingen voor gegevensverwerking op afstand en vrije en opensourcesoftware;

b) de toepassing van ondersteuningsperioden met betrekking tot bepaalde categorieën producten met digitale elementen;

c) richtsnoeren voor fabrikanten die onder deze verordening vallen en die ook onderworpen zijn aan andere harmonisatiewetgeving van de Unie dan deze verordening of andere daarmee verband houdende rechtshandelingen van de Unie;

d) het begrip "ingrijpende wijziging".

De Commissie houdt ook een gemakkelijk toegankelijke lijst bij van de gedelegeerde handelingen en uitvoeringshandelingen die op grond van deze verordening zijn vastgesteld.

3. Bij het opstellen van de richtsnoeren op grond van dit artikel raadpleegt de Commissie de relevante belanghebbenden.

HOOFDSTUK III

CONFORMITEIT VAN HET PRODUCT MET DIGITALE ELEMENTEN

Artikel 27

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 cyberbeveiligingsvereisten van bijlage I die door die normen of delen daarvan worden bestreken.

De Commissie verzoekt overeenkomstig artikel 10, lid 1, van Verordening (EU) nr. 1025/2012 een of meer Europese normalisatieorganisaties om geharmoniseerde normen op te stellen voor de essentiële cyberbeveiligingsvereisten van bijlage I bij deze verordening. Bij het opstellen van normalisatieverzoeken voor deze verordening streeft de Commissie ernaar rekening te houden met bestaande Europese en internationale normen voor cyberbeveiliging die van kracht of in ontwikkeling zijn, teneinde de ontwikkeling van geharmoniseerde normen te vereenvoudigen, overeenkomstig Verordening (EU) nr. 1025/2012.

2. De Commissie kan uitvoeringshandelingen vaststellen met gemeenschappelijke specificaties inzake technische vereisten die een middel bieden om te voldoen aan de essentiële cyberbeveiligingsvereisten van bijlage I voor binnen het toepassingsgebied van deze verordening vallende producten met digitale elementen.

Die uitvoeringshandelingen worden alleen vastgesteld indien aan de volgende voorwaarden is voldaan:

a) de Commissie heeft, op grond van artikel 10, lid 1, van Verordening (EU) nr. 1025/2012, één of meer Europese normalisatieorganisaties verzocht geharmoniseerde normen voor de essentiële cyberbeveiligingsvereisten van bijlage I op te stellen en:

   i) het verzoek is niet aanvaard;

   ii) de geharmoniseerde normen waarop dat verzoek betrekking heeft, worden niet binnen de overeenkomstig artikel 10, lid 1, van Verordening (EU) nr. 1025/2012 vastgestelde termijn geleverd, of

   iii) de geharmoniseerde normen voldoen niet aan het verzoek, en

b) er is geen referentie van geharmoniseerde normen overeenkomstig Verordening (EU) nr. 1025/2012 bekendgemaakt in het *Publicatieblad van de Europese Unie* voor de desbetreffende essentiële cyberbeveiligingsvereisten van bijlage I bij deze verordening, en een dergelijke referentie zal naar verwachting niet binnen een redelijke termijn worden bekendgemaakt.

Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

3. Alvorens de in lid 2 van dit artikel bedoelde ontwerpuitvoeringshandeling op te stellen, stelt de Commissie het in artikel 22 van Verordening (EU) nr. 1025/2012 bedoelde comité ervan in kennis dat zij van oordeel is dat aan de voorwaarden van lid 2 van dit artikel is voldaan.

4. Bij het opstellen van de in lid 2 bedoelde ontwerpuitvoeringshandeling houdt de Commissie rekening met de standpunten van de relevante instanties en raadpleegt zij naar behoren alle relevante belanghebbenden.

5. Producten met digitale elementen en processen die door de fabrikant zijn ingesteld en in overeenstemming zijn met de gemeenschappelijke specificaties die zijn vastgesteld bij de in lid 2 van dit artikel bedoelde uitvoeringshandelingen, of delen daarvan, worden geacht in overeenstemming te zijn met de essentiële cyberbeveiligingsvereisten van bijlage I die door die gemeenschappelijke specificaties of delen daarvan worden bestreken.

6. Wanneer een geharmoniseerde norm door een Europese normalisatieorganisatie wordt vastgesteld en aan de Commissie wordt voorgesteld met het oog op de bekendmaking van de referentie ervan in het *Publicatieblad van de Europese Unie*, beoordeelt de Commissie de geharmoniseerde norm overeenkomstig Verordening (EU) nr. 1025/2012. Wanneer een referentie van een geharmoniseerde norm in het *Publicatieblad van de Europese Unie* wordt bekendgemaakt, trekt de Commissie de in lid 2 van dit artikel bedoelde uitvoeringshandelingen of delen daarvan die dezelfde essentiële cyberbeveiligingsvereisten bestrijken als die geharmoniseerde norm, in.

7. Indien een lidstaat van oordeel is dat een gemeenschappelijke specificatie niet volledig aan de essentiële cyberbeveiligingsvereisten van bijlage I voldoet, stelt die lidstaat de Commissie daarvan in kennis door middel van een gedetailleerde toelichting. De Commissie beoordeelt die gedetailleerde toelichting en kan de uitvoeringshandeling tot vaststelling van de gemeenschappelijke specificatie in kwestie indien nodig wijzigen.

8. 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 op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregeling, worden geacht in overeenstemming te zijn met de essentiële cyberbeveiligingsvereisten van bijlage I, voor zover die vereisten door de EU-conformiteitsverklaring of het Europese cyberbeveiligingscertificaat, of delen daarvan, worden bestreken.

9. De Commissie is bevoegd om overeenkomstig artikel 61 van deze verordening gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen door de op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregelingen te specificeren die kunnen worden gebruikt om de conformiteit van producten met digitale elementen met de essentiële cyberbeveiligingsvereisten, of delen daarvan, van bijlage I bij deze verordening aan te tonen. Bovendien ontslaat de afgifte van een in het kader van dergelijke regelingen afgegeven Europees cyberbeveiligings-certificaat, op ten minste zekerheidsniveau "substantieel", de fabrikant van de verplichting om een conformiteitsbeoordeling door derden te laten verrichten voor de overeenkomstige vereisten, zoals uiteengezet in artikel 32, lid 2, punten a) en b), en lid 3, punten a) en b), van deze verordening.

Artikel 28

EU-conformiteitsverklaring

1. De EU-conformiteitsverklaring wordt door fabrikanten opgesteld overeenkomstig artikel 13, lid 12, en vermeldt dat is aangetoond dat aan de toepasselijke essentiële cyberbeveiligingsvereisten van bijlage I is voldaan.

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

De in artikel 13, lid 20, bedoelde vereenvoudigde EU-conformiteitsverklaring komt qua structuur overeen met het model in bijlage VI. Zij wordt beschikbaar gesteld in de talen die zijn 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 rechtshandeling van de Unie een EU-conformiteitsverklaring vereist is, wordt één EU-conformiteitsverklaring met betrekking tot al dergelijke rechtshandelingen van de Unie opgesteld. In die verklaring wordt aangegeven om welke rechtshandelingen van de Unie het gaat, met vermelding van de publicatiegegevens ervan.

4. Door de EU-conformiteitsverklaring op te stellen, neemt de fabrikant de verantwoordelijkheid voor de conformiteit van het product met digitale elementen op zich.

5. De Commissie is bevoegd om overeenkomstig artikel 61 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 V om rekening te houden met technologische ontwikkelingen.

Artikel 29

Algemene beginselen van de CE-markering

De CE-markering is onderworpen aan de algemene beginselen die zijn vastgesteld in artikel 30 van Verordening (EG) nr. 765/2008.

Artikel 30

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 dat 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 28 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 28 bedoelde EU-conformiteitsverklaring, hetzij op de website die bij het softwareproduct hoort. In het laatste geval is het relevante gedeelte van de website eenvoudig en rechtstreeks toegankelijk voor consumenten.

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. Zij kan worden gevolgd door een pictogram of een ander merkteken dat wijst op een bijzonder cyberbeveiligingsrisico 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 in artikel 32 bedoelde conformiteitsbeoordelingsprocedure op basis van volledige kwaliteitsborging (op basis van module H).

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

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 harmonisatiewetgeving van de Unie dan deze verordening, die ook voorziet in het aanbrengen van de CE-markering, geeft de CE-markering aan dat het product ook aan de vereisten van dergelijke andere harmonisatiewetgeving van de Unie voldoet.

6. De Commissie kan door middel van uitvoeringshandelingen technische specificaties vaststellen voor etiketten, pictogrammen of andere merktekens die verband houden met de beveiliging van producten met digitale elementen, de ondersteuningsperioden ervan alsook mechanismen om het gebruik ervan te bevorderen en het publieke bewustzijn omtrent de veiligheid van producten met digitale elementen te vergroten. Bij het opstellen van de ontwerpuitvoeringshandelingen raadpleegt de Commissie de relevante belanghebbenden en, indien die reeds is opgericht op grond van artikel 52, lid 15, de ADCO. Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 31

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 cyberbeveiligingsvereisten van bijlage I voldoen. De technische documentatie bevat ten minste de in bijlage VII vermelde elementen.

2. De technische documentatie wordt opgesteld voordat het product met digitale elementen in de handel wordt gebracht en wordt indien passend voortdurend bijgewerkt, in ieder geval tijdens de ondersteuningsperiode.

3. Voor producten met digitale elementen als bedoeld in artikel 12, die ook onder andere rechtshandelingen van de Unie vallen die in technische documentatie voorzien, wordt één set van technische documentatie opgesteld die de in bijlage VII bedoelde informatie en de bij die rechtshandelingen 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 om overeenkomstig artikel 61 gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen door elementen toe te voegen die moeten worden opgenomen in de in bijlage VII vermelde technische documentatie, teneinde rekening te houden met technologische ontwikkelingen en ontwikkelingen die zich tijdens het uitvoeringsproces van deze verordening voordoen. Daartoe streeft de Commissie ernaar ervoor te zorgen dat de administratieve lasten voor micro-ondernemingen en kleine en middelgrote ondernemingen evenredig zijn.

Artikel 32

Conformiteitsbeoordelingsprocedures voor producten 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 cyberbeveiligingsvereisten van bijlage I is voldaan. De fabrikant toont de conformiteit met de essentiële cyberbeveiligingsvereisten aan de hand van een van de volgende procedures aan:

a) de procedure voor interne controle (op basis van module A) zoals beschreven in bijlage VIII;

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

c) een conformiteitsbeoordeling op basis van volledige kwaliteitsborging (op basis van module H) zoals beschreven in bijlage VIII, of

d) indien beschikbaar en van toepassing, een Europese cyberbeveiligingscertificeringsregeling op grond van artikel 27, lid 9.

2. Wanneer de fabrikant bij de beoordeling van de conformiteit van een belangrijk product met digitale elementen dat valt onder klasse I zoals vastgesteld in bijlage III en van de door de fabrikant ingestelde processen met de essentiële cyberbeveiligingsvereisten van bijlage I, geen geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen op ten minste zekerheidsniveau “substantieel” als bedoeld in artikel 27 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 cyberbeveiligingsvereisten aan een van de volgende procedures onderworpen:

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

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

3. Indien het product een belangrijk product met digitale elementen is dat valt onder klasse II zoals beschreven in bijlage III, toont de fabrikant de conformiteit met de essentiële cyberbeveiligingsvereisten van bijlage I aan door middel van een van de volgende procedures:

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

b) een conformiteitsbeoordeling op basis van volledige kwaliteitsborging (op basis van module H) zoals beschreven in bijlage VIII, of

c) indien beschikbaar en van toepassing, een Europese cyberbeveiligingscertificeringsregeling op grond van artikel 27, lid 9, van deze verordening op ten minste zekerheidsniveau "substantieel" op grond van Verordening (EU) 2019/881.

4. Voor kritieke producten met digitale elementen die zijn opgenomen in bijlage IV, wordt de conformiteit met de essentiële cyberbeveiligingsvereisten van bijlage I aangetoond door middel van een van de volgende procedures:

a) een Europese cyberbeveiligingscertificeringsregeling overeenkomstig artikel 8, lid 1, of

b) indien niet aan de voorwaarden van artikel 8, lid 1, is voldaan, een van de in lid 3 van dit artikel bedoelde procedures.

5. Fabrikanten van producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt en die onder de categorieën van bijlage III vallen, kunnen aantonen dat zij aan de essentiële cyberbeveiligingsvereisten van bijlage I voldoen door middel van een van de in lid 1 van dit artikel bedoelde procedures, op voorwaarde dat de in artikel 31 bedoelde technische documentatie ter beschikking van het publiek wordt gesteld op het moment dat die producten in de handel worden gebracht.

6. Bij het vaststellen van de vergoedingen voor conformiteitsbeoordelingsprocedures wordt rekening gehouden met de specifieke belangen en behoeften van micro-ondernemingen en kleine en middelgrote ondernemingen, met inbegrip van start-ups, en die vergoedingen worden verlaagd in verhouding tot hun specifieke belangen en behoeften.

Artikel 33

Steunmaatregelen voor micro-ondernemingen en kleine en middelgrote ondernemingen, met inbegrip van start-ups

1. De lidstaten ondernemen, waar passend, de volgende acties die zijn afgestemd op de behoeften van micro-ondernemingen en kleine ondernemingen:

a) specifieke bewustmakings- en opleidingsactiviteiten over de toepassing van deze verordening organiseren;

b) een specifiek kanaal opzetten voor communicatie met micro-ondernemingen en kleine ondernemingen en, voor zover passend, lokale overheden om advies te verstrekken en vragen over de uitvoering van deze verordening te beantwoorden;

c) ondersteunen van test- en conformiteitsbeoordelingsactiviteiten, voor zover relevant onder meer met de steun van het Europees kenniscentrum voor cyberbeveiliging.

2. De lidstaten kunnen, indien passend, testomgevingen voor regelgeving inzake cyberweerbaarheid opzetten. Dergelijke testomgevingen voor regelgeving voorzien in gecontroleerde testomgevingen voor innovatieve producten met digitale elementen om de ontwikkeling, het ontwerp, de validering en het testen ervan te vergemakkelijken met het oog op de naleving van deze verordening gedurende een beperkte periode voordat zij in de handel worden gebracht. De Commissie en, voor zover passend, Enisa kunnen technische ondersteuning, advies en instrumenten verlenen voor de oprichting en werking van testomgevingen voor regelgeving. De testomgevingen voor regelgeving worden opgezet onder direct toezicht en met directe begeleiding en ondersteuning van de markttoezichtautoriteiten. De lidstaten stellen de Commissie en de andere markttoezichtautoriteiten via de ADCO in kennis van de oprichting van een testomgeving voor regelgeving. De testomgevingen voor regelgeving laten de toezichthoudende en corrigerende bevoegdheden van de bevoegde autoriteiten onverlet. De lidstaten zorgen voor open, eerlijke en transparante toegang tot testomgevingen voor regelgeving, en vergemakkelijken met name de toegang voor micro-ondernemingen en kleine ondernemingen, met inbegrip van start-ups.

3. Overeenkomstig artikel 26 verstrekt de Commissie richtsnoeren voor micro-ondernemingen en kleine en middelgrote ondernemingen met betrekking tot de uitvoering van deze verordening.

4. De Commissie maakt de beschikbare financiële steun in het regelgevingskader van bestaande programma's van de Unie bekend, met name om de financiële lasten voor micro-ondernemingen en kleine ondernemingen te verlichten.

5. Micro-ondernemingen en kleine ondernemingen kunnen alle elementen van de in bijlage VII gespecificeerde technische documentatie in vereenvoudigde vorm verstrekken. Daartoe specificeert de Commissie door middel van uitvoeringshandelingen het vereenvoudigde formulier voor technische documentatie dat gericht is op de behoeften van micro-ondernemingen en kleine ondernemingen, met inbegrip van de wijze waarop de in bijlage VII vermelde elementen moeten worden verstrekt. Wanneer een micro-onderneming of kleine onderneming ervoor kiest de in bijlage VII vermelde informatie op vereenvoudigde wijze te verstrekken, gebruikt zij het in dit lid bedoelde formulier. Aangemelde instanties aanvaarden dat formulier ten behoeve van de conformiteitsbeoordeling.

Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 34

Overeenkomsten inzake wederzijdse erkenning

Rekening houdend met het niveau van technische ontwikkeling en de aanpak van de conformiteitsbeoordeling van een derde land, kan de Unie overeenkomstig artikel 218 VWEU overeenkomsten inzake wederzijdse erkenning met derde landen sluiten om de internationale handel te bevorderen en te vergemakkelijken.

HOOFDSTUK IV

AANMELDING VAN CONFORMITEITSBEOORDELINGSINSTANTIES

Artikel 35

Aanmelding

1. De lidstaten doen aan de Commissie en aan de andere lidstaten melding van de instanties die bevoegd zijn om conformiteitsbeoordelingen overeenkomstig deze verordening te verrichten.

2. De lidstaten streven ernaar ervoor te zorgen dat er uiterlijk op 11 december 2026 een voldoende aantal aangemelde instanties in de Unie is om conformiteitsbeoordelingen uit te voeren, teneinde knelpunten en belemmeringen voor toegang tot de markt te voorkomen.

Artikel 36

Aanmeldende autoriteiten

1. Elke lidstaat wijst een aanmeldende autoriteit aan die verantwoordelijk is voor de opstelling en uitvoering van de nodige procedures voor de beoordeling, aanwijzing en aanmelding van conformiteitsbeoordelingsinstanties en de monitoring daarvan, met inbegrip van de naleving van artikel 41.

2. De lidstaten kunnen de beoordeling en de monitoring als bedoeld in lid 1 laten uitvoeren door een nationale accreditatie-instantie in de zin van en overeenkomstig Verordening (EG) nr. 765/2008.

3. Indien de aanmeldende autoriteit de beoordeling, de aanmelding of de monitoring zoals bedoeld in lid 1 van dit artikel delegeert of op een andere wijze toevertrouwt aan een instantie die geen overheidsinstantie is, is die instantie een rechtspersoon en voldoet zij mutatis mutandis aan artikel 37. Bovendien treft die instantie regelingen om de aansprakelijkheid voor haar activiteiten te dekken.

4. De aanmeldende autoriteit is volledig aansprakelijk voor de taken die de in lid 3 vermelde instantie verricht.

Artikel 37

Vereisten met betrekking tot aanmeldende autoriteiten

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

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

3. Een aanmeldende autoriteit is zodanig georganiseerd dat elk besluit in verband met de aanmelding van een conformiteitsbeoordelingsinstantie wordt genomen door bekwame personen die niet de beoordeling hebben verricht.

4. Een aanmeldende autoriteit verricht geen activiteiten die worden uitgevoerd door conformiteitsbeoordelingsinstanties en verleent geen adviesdiensten op commerciële of concurrende 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 38

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 de monitoring van aangemelde instanties, en van alle wijzigingen daarin.

2. De Commissie maakt de in lid 1 bedoelde informatie openbaar.

Artikel 39

Vereisten met betrekking tot aangemelde instanties

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

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

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

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 derde partij worden beschouwd, op voorwaarde dat haar onafhankelijkheid en de afwezigheid van belangenconflicten worden aangetoond.

4. Een conformiteitsbeoordelingsinstantie, haar hoogste leidinggevenden en het personeel dat de conformiteitsbeoordelingstaken verricht, zijn niet de ontwerper, ontwikkelaar, fabrikant, leverancier, importeur, distributeur, installateur, koper, eigenaar, gebruiker of onderhouder van de door hen beoordeelde producten met digitale elementen, noch de gemachtigde vertegenwoordiger van één van die partijen. Dat vormt echter geen beletsel voor 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 het personeel dat de conformiteitsbeoordelingstaken verricht, zijn niet rechtstreeks of als vertegenwoordiger van de betrokken partijen betrokken bij het ontwerpen, ontwikkelen, vervaardigen, importeren, distribueren, verhandelen, installeren, gebruiken of onderhouden van de door hen beoordeelde producten met digitale elementen. Zij voeren geen activiteiten uit die hun onafhankelijk oordeel of hun integriteit met betrekking tot de conformiteitsbeoordelingsactiviteiten waarvoor zij zijn aangemeld, in het gedrang kunnen brengen. Dat 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 conformiteitsbeoordelingsactiviteiten.

5. Conformiteitsbeoordelingsinstanties en hun personeel voeren de conformiteitsbeoordelingsactiviteiten uit met de hoogste mate van professionele integriteit en met de vereiste technische bekwaamheid op het specifieke gebied, zonder druk of aansporing, met name van financiële aard, die hun oordeel of de resultaten van hun conformiteitsbeoordelingsactiviteiten kunnen beïnvloeden, met name van personen of groepen van personen die belang hebben bij de resultaten van die activiteiten.

6. Een conformiteitsbeoordelingsinstantie is in staat alle in bijlage VIII 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) het nodige personeel met technische kennis en voldoende passende ervaring om de conformiteitsbeoordelingstaken te verrichten;

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

c) de nodige procedures voor de uitoefening van haar activiteiten die naar behoren rekening houden met de omvang van een onderneming, de sector waarin die actief is, haar structuur, de mate van complexiteit van de producttechnologie in kwestie en het massa- of seriële karakter van het productieproces.

Een conformiteitsbeoordelingsinstantie beschikt over de middelen die nodig zijn om de technische en administratieve taken in verband met de conformiteitsbeoordelingsactiviteiten op passende wijze uit te voeren en heeft toegang tot alle vereiste apparatuur en faciliteiten.

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

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

b) toereikende kennis van de vereisten inzake de beoordelingen die het verricht en voldoende bevoegdheden om die beoordelingen uit te voeren;

c) voldoende kennis van en inzicht in de essentiële cyberbeveiligingsvereisten van bijlage I, de toepasselijke geharmoniseerde normen en gemeenschappelijke specificaties, en de relevante bepalingen van harmonisatiewetgeving van de Unie en uitvoeringshandelingen;

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 wordt 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 de wettelijke aansprakelijkheid op basis van het nationale recht door hun 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 haar taken uit hoofde van bijlage VIII of van een bepaling van nationaal recht die daaraan uitvoering geven, behalve ten opzichte 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 coördinatiegroep van aangemelde instanties die is opgericht uit hoofde van artikel 51, en hanteren de door die groep genomen administratieve beslissingen en geproduceerde documenten als algemene richtsnoeren.

12. Conformiteitsbeoordelingsinstanties handelen overeenkomstig een reeks consistente, billijke, evenredige en redelijke voorwaarden, waarbij voorkomen wordt de marktdeelnemers onnodig te belasten, en met name rekening wordt gehouden met de belangen van micro-ondernemingen en kleine en middelgrote ondernemingen met betrekking tot vergoedingen.

Artikel 40

Vermoeden van conformiteit van aangemelde instanties

Wanneer een conformiteitsbeoordelingsinstantie aantoont dat zij voldoet aan de criteria in de ter zake doende geharmoniseerde normen of delen ervan, waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, wordt zij geacht aan de vereisten van artikel 39 te voldoen, voor zover die vereisten door de van toepassing zijnde geharmoniseerde normen worden bestreken.

Artikel 41

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 vereisten van artikel 39 voldoet, en brengt zij de aanmeldende autoriteit daarvan op de hoogte.

2. Aangemelde instanties nemen de volledige verantwoordelijkheid op zich voor de taken die worden verricht door onderaannemers of dochterondernemingen, ongeacht waar zij 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 42

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 gaat vergezeld van een beschrijving van de conformiteitsbeoordelingsactiviteiten, de conformiteitsbeoordelingsprocedure(s) en het product of de producten met digitale elementen waarvoor de instantie verklaart bekwaam te zijn, alsook, in voorkomend geval, van een accreditatiecertificaat dat is afgegeven door een nationale accreditatie-instantie, waarin wordt verklaard dat de conformiteitsbeoordelingsinstantie voldoet aan de vereisten van artikel 39.

3. Wanneer de betrokken conformiteitsbeoordelingsinstantie geen accreditatiecertificaat kan overleggen, verschaft zij de aanmeldende autoriteit alle bewijsstukken die nodig zijn om haar conformiteit met de vereisten van artikel 39 te verifiëren en te erkennen en die geregeld te monitoren.

Artikel 43

Aanmeldingsprocedure

1. Aanmeldende autoriteiten melden uitsluitend conformiteitsbeoordelingsinstanties aan die aan de vereisten van artikel 39 hebben voldaan.

2. De aanmeldende autoriteit verricht de aanmelding bij de Commissie en de andere lidstaten door middel van het door de Commissie ontwikkelde en beheerde informatiesysteem (*New Approach Notified and Designated Organisations*).

3. Bij de aanmelding worden de conformiteitsbeoordelingsactiviteiten, de conformiteitsbeoordelingsmodule(s), het product of de producten met digitale elementen en het relevante bekwaamheidsattest uitvoerig beschreven.

4. Wanneer een aanmelding niet gebaseerd is op een accreditatiecertificaat als bedoeld in artikel 42, 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 gemonitord en zal blijven voldoen aan de vereisten van artikel 39.

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 aangemelde instantie beschouwd.

6. Aan de Commissie en aan de andere lidstaten wordt melding gedaan van alle relevante latere wijzigingen in de aanmelding.

Artikel 44

Identificatienummers en lijsten van aangemelde instanties

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

Zij kent per instantie slechts één nummer toe, ook als de instantie uit hoofde van diverse rechtshandelingen 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 voor de bijwerking van die lijst.

Artikel 45

Wijzigingen van aanmeldingen

1. Wanneer een aanmeldende autoriteit heeft geconstateerd of vernomen dat een aangemelde instantie niet meer aan de vereisten van artikel 39 voldoet of haar verplichtingen niet nakomt, wordt de aanmelding door de aanmeldende autoriteit naargelang van het geval beperkt, geschorst of ingetrokken, afhankelijk van de ernst van het niet-voldoen aan die vereisten of het niet-nakomen van die verplichtingen. Zij brengt de Commissie en de andere lidstaten daarvan onmiddellijk 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 behandeld, hetzij aan de verantwoordelijke aanmeldende autoriteiten en markttoezichtautoriteiten op hun verzoek ter beschikking kunnen worden gesteld.

Artikel 46

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 om aan de vereisten te voldoen en haar verantwoordelijkheden na te komen, of over de vraag of een aangemelde instantie nog aan de vereisten voldoet en haar verantwoordelijkheden nakomt.

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

3. Alle gevoelige informatie die de Commissie in het kader van haar onderzoek ontvangt, wordt door haar vertrouwelijk behandeld.

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

Artikel 47

Operationele verplichtingen van aangemelde instanties

1. Aangemelde instanties voeren conformiteitsbeoordelingen uit volgens de conformiteitsbeoordelingsprocedures van artikel 32 en bijlage VIII.

2. De conformiteitsbeoordelingen worden op evenredige wijze uitgevoerd, waarbij voorkomen wordt de marktdeelnemers onnodig te belasten. Conformiteitsbeoordelingsinstanties houden bij de uitoefening van hun activiteiten naar behoren rekening met de omvang van ondernemingen, met name met betrekking tot micro-ondernemingen en kleine en middelgrote ondernemingen, de sector waarin zij actief zijn, hun structuur, hun relatieve complexiteit en het cyberbeveiligingsrisico van de producten met digitale elementen en de technologie in kwestie en het massa- of seriële karakter van het productieproces.

3. Aangemelde instanties eerbiedigen echter de striktheid en het beschermingsniveau die nodig zijn opdat producten met digitale elementen aan deze verordening voldoen.

4. Wanneer een aangemelde instantie vaststelt dat een fabrikant niet heeft voldaan aan de vereisten van bijlage I of in de overeenkomstige in artikel 27 bedoelde geharmoniseerde normen of gemeenschappelijke specificaties, vereist zij van die fabrikant dat hij passende corrigerende maatregelen neemt en verleent zij geen conformiteitscertificaat.

5. Wanneer een aangemelde instantie bij de monitoring van de conformiteit na verlening van een certificaat vaststelt dat een product met digitale elementen niet langer aan de vereisten van deze verordening voldoet, vereist zij van de fabrikant dat hij passende corrigerende maatregelen neemt; zo nodig schorst zij het certificaat of trekt dat 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, geschorst of ingetrokken.

Artikel 48

Beroep tegen besluiten van aangemelde instanties

De lidstaten voorzien in een beroepsprocedure tegen besluiten van de aangemelde instanties.

Artikel 49

Informatieplicht voor aangemelde instanties

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

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

b) omstandigheden die van invloed zijn op de werkingssfeer van en de voorwaarden voor aanmelding;

c) informatieverzoeken over conformiteitsbeoordelingsactiviteiten die zij van markttoezichtautoriteiten ontvangen;

d) op verzoek, de binnen de werkingssfeer van hun aanmelding verrichte conformiteitsbeoordelingsactiviteiten en andere activiteiten, waaronder grensoverschrijdende activiteiten en onderaanneming.

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

Artikel 50

Uitwisseling van ervaringen

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

Artikel 51

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 52

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

1. Verordening (EU) 2019/1020 is van toepassing op 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. De krachtens lid 2 van dit artikel aangewezen markttoezichtautoriteiten zijn ook verantwoordelijk voor het uitvoeren van markttoezichtactiviteiten met betrekking tot de in artikel 24 vastgestelde verplichtingen voor opensourcesoftwarestewards. Wanneer een markttoezichtautoriteit vaststelt dat een opensourcesoftwaresteward niet voldoet aan de verplichtingen van dat artikel, vereist zij van de opensourcesoftwaresteward dat hij ervoor zorgt dat alle passende corrigerende maatregelen worden genomen. Opensourcesoftwarestewards zorgen ervoor dat alle passende corrigerende maatregelen worden genomen met betrekking tot hun verplichtingen uit hoofde van deze verordening.

4. Voor zover relevant werken de markttoezichtautoriteiten samen met de op grond van 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 op grond van artikel 14 van deze verordening werken de aangewezen markttoezichtautoriteiten samen en wisselen zij regelmatig informatie uit met de als coördinatoren aangewezen CSIRT's en Enisa.

5. De markttoezichtautoriteiten kunnen een als coördinator aangewezen CSIRT of Enisa verzoeken om technisch advies te verstrekken over aangelegenheden die verband houden met de uitvoering en handhaving van deze verordening. Bij het uitvoeren van een onderzoek uit hoofde van artikel 54 kunnen de markttoezichtautoriteiten het als coördinator aangewezen CSIRT of Enisa verzoeken een analyse te verstrekken ter ondersteuning van de evaluaties van de conformiteit van producten met digitale elementen.

6. Voor zover relevant werken de markttoezichtautoriteiten samen met andere markttoezichtautoriteiten die op basis van andere harmonisatiewetgeving van de Unie dan deze verordening zijn aangewezen, en wisselen zij regelmatig informatie uit.

7. De markttoezichtautoriteiten werken voor zover passend samen met de autoriteiten die toezicht houden op het gegevensbeschermingsrecht van de Unie. Die samenwerking omvat het informeren van die autoriteiten over bevindingen die relevant zijn voor de uitoefening van hun bevoegdheden, onder meer bij het verstrekken van richtsnoeren en advies op grond van lid 10, indien die richtsnoeren en adviezen betrekking hebben op de verwerking van persoonsgegevens.

De autoriteiten die toezicht houden op het gegevensbeschermingsrecht 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.

8. De lidstaten zorgen ervoor dat de aangewezen markttoezichtautoriteiten beschikken over voldoende financiële en technische middelen, indien passend met inbegrip van instrumenten voor geautomatiseerde verwerking, alsook over personele middelen met de nodige vaardigheden op het gebied van cyberbeveiliging om hun taken uit hoofde van deze verordening uit te voeren.

9. De Commissie bevordert en faciliteert de uitwisseling van ervaringen tussen de aangewezen markttoezichtautoriteiten.

10. De markttoezichtautoriteiten kunnen marktdeelnemers richtsnoeren en advies verstrekken over de uitvoering van deze verordening, met de steun van de Commissie en, indien passend, de CSIRT's en Enisa.

11. De markttoezichtautoriteiten informeren consumenten, overeenkomstig artikel 11 van Verordening (EU) 2019/1020, over waar zij klachten kunnen indienen die kunnen wijzen op niet-naleving van deze verordening, en verstrekken consumenten informatie over waar en hoe toegang kan worden verkregen tot mechanismen om de melding van kwetsbaarheden, incidenten en cyberdreigingen die gevolgen kunnen hebben voor producten met digitale elementen, te vergemakkelijken.

12. De markttoezichtautoriteiten bevorderen voor zover relevant de samenwerking met relevante belanghebbenden, met inbegrip van wetenschappelijke, onderzoeks- en consumentenorganisaties.

13. 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 betrokken nationale mededingingsautoriteiten over alle tijdens markttoezichtactiviteiten verkregen informatie die potentieel van belang kan zijn voor de toepassing van het mededingingsrecht van de Unie.

14. Voor producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen en op grond van artikel 6 van Verordening (EU) 2024/1689 als AI-systemen met een hoog risico worden aangemerkt, zijn de voor de toepassing van die verordening aangewezen markttoezichtautoriteiten de autoriteiten die belast zijn met het markttoezicht uit hoofde van deze verordening. De op grond van Verordening (EU) 2024/1689 aangewezen markttoezichtautoriteiten werken voor zover passend samen met de op grond van deze verordening aangewezen markttoezichtautoriteiten en, met betrekking tot het toezicht op de uitvoering van de rapportageverplichtingen uit hoofde van artikel 14 van deze verordening, met de als coördinatoren aangewezen CSIRT's en Enisa. De op grond van Verordening (EU) 2024/1689 aangewezen markttoezichtautoriteiten stellen met name de op grond van deze verordening aangewezen markttoezicht-autoriteiten in kennis van alle bevindingen die relevant zijn voor hun taken in verband met de uitvoering van deze verordening.

15. Voor de uniforme toepassing van deze verordening wordt op grond van artikel 30, lid 2, van Verordening (EU) 2019/1020 de ADCO opgericht. De ADCO bestaat uit vertegenwoordigers van de aangewezen markttoezichtautoriteiten en, indien relevant, vertegenwoordigers van verbindingsbureaus. De ADCO behandelt ook specifieke kwesties in verband met de markttoezichtactiviteiten met betrekking tot de verplichtingen voor opensourcesoftwarestewards.

16. De markttoezichtautoriteiten monitoren hoe fabrikanten de in artikel 13, lid 8, bedoelde criteria hebben toegepast bij het bepalen van de ondersteuningsperioden voor hun producten met digitale elementen.

De ADCO publiceert in een openbaar toegankelijke en gebruiksvriendelijke vorm relevante statistieken over categorieën producten met digitale elementen, met inbegrip van gemiddelde ondersteuningsperioden, zoals bepaald door de fabrikant op grond van artikel 13, lid 8, en verstrekt richtsnoeren met indicatieve ondersteuningsperioden voor categorieën producten met digitale elementen.

Wanneer uit de gegevens blijkt dat de ondersteuningsperioden voor specifieke categorieën producten met digitale elementen ontoereikend zijn, kan de ADCO de markttoezichtautoriteiten aanbevelingen doen om hun activiteiten te richten op dergelijke categorieën producten met digitale elementen.

Artikel 53

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 cyberbeveiligingsvereisten van bijlage I te beoordelen, krijgen de markttoezichtautoriteiten, op een met redenen omkleed verzoek, in een voor hen gemakkelijk te begrijpen taal 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 54

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, evalueert zij, zonder onnodige vertraging en, indien passend, in samenwerking met het desbetreffende CSIRT, of het betrokken product met digitale elementen voldoet aan alle vereisten van deze verordening. De desbetreffende marktdeelnemers werken zo nodig samen met de markttoezichtautoriteit.

Indien de markttoezichtautoriteit bij die evaluatie vaststelt dat het product met digitale elementen niet aan de vereisten van deze verordening voldoet, gelast zij de betrokken marktdeelnemer onverwijld alle passende corrigerende maatregelen te nemen om het product met digitale elementen binnen een door de markttoezichtautoriteit vast te stellen redelijke termijn, die evenredig is met de aard van het cyberbeveiligingsrisico, in overeenstemming te brengen met die vereisten, 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 corrigerende maatregelen.

2. Bij het bepalen van de significantie van een cyberbeveiligingsrisico als bedoeld in lid 1 van dit artikel nemen de markttoezichtautoriteiten ook niet-technische risicofactoren in aanmerking, met name die welke zijn vastgesteld als gevolg van overeenkomstig artikel 22 van Richtlijn (EU) 2022/2555 uitgevoerde, op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens. Indien een markttoezichtautoriteit voldoende redenen heeft om aan te nemen dat een product met digitale elementen in het licht van niet-technische risicofactoren een significant cyberbeveiligingsrisico vormt, stelt zij de bevoegde autoriteiten die zijn aangewezen of opgericht op grond van artikel 8 van Richtlijn (EU) 2022/2555, daarvan op de hoogte en werkt zij zo nodig met die autoriteiten samen.

3. 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 evaluatie en van de maatregelen die zij de marktdeelnemer heeft opgelegd.

4. De marktdeelnemer zorgt ervoor dat alle passende corrigerende maatregelen worden toegepast op alle betrokken producten met digitale elementen die hij in de Unie op de markt heeft aangeboden.

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

Die autoriteit stelt de Commissie en de andere lidstaten onverwijld in kennis van die maatregelen.

6. De in lid 5 bedoelde informatie omvat alle bekende bijzonderheden, met name de gegevens die nodig zijn om het non-conforme product met digitale elementen te identificeren en om de oorsprong van dat product met digitale elementen, de aard van de beweerde non-conformiteit en van het risico, en de aard en de duur van de nationale maatregelen vast te stellen, 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 met digitale elementen of de door de fabrikant ingestelde processen voldoen niet aan de essentiële cyberbeveiligingsvereisten van bijlage I;

b) tekortkomingen in de in artikel 27 bedoelde geharmoniseerde normen, Europese cyberbeveiligingscertificeringsregelingen of gemeenschappelijke specificaties.

7. De markttoezichtautoriteiten van de andere lidstaten dan die welke 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 product met digitale elementen waarover zij beschikken, en van hun bezwaren indien zij het niet eens zijn met de aangemelde nationale maatregel.

8. Indien binnen drie maanden na ontvangst van de in lid 5 van dit artikel bedoelde kennisgeving door een lidstaat of de Commissie geen bezwaar tegen een voorlopige maatregel van een lidstaat is aangetekend, wordt die maatregel geacht gerechtvaardigd te zijn. Dat doet geen afbreuk aan de procedurele rechten van de betrokken marktdeelnemer overeenkomstig artikel 18 van Verordening (EU) 2019/1020.

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

Artikel 55

Vrijwaringsprocedure van de Unie

1. Indien een lidstaat binnen drie maanden na ontvangst van de in artikel 54, lid 5, bedoelde kennisgeving bezwaar maakt tegen een door een andere lidstaat genomen maatregel of wanneer de Commissie de maatregel in strijd acht met het Unierecht, treedt de Commissie onverwijld in overleg met de betrokken lidstaat en de marktdeelnemer(s) 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 54, lid 5, 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 11 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 in artikel 27 bedoelde Europese cyberbeveiligingscertificeringsregeling, onderzoekt de Commissie of een op grond van artikel 27, lid 9, vastgestelde gedelegeerde handeling 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 in artikel 27 bedoelde gemeenschappelijke specificaties, onderzoekt de Commissie of een op grond van artikel 27, lid 2, vastgestelde uitvoeringshandeling tot vaststelling van die gemeenschappelijke specificaties moet worden gewijzigd of ingetrokken.

Artikel 56

Procedure op het niveau van de Unie 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 voldoet aan de vereisten van deze verordening, stelt zij de betrokken markttoezichtautoriteiten daarvan op de hoogte. Wanneer de markttoezichtautoriteiten evalueren of dat product met digitale elementen dat een significant cyberbeveiligingsrisico kan inhouden, voldoet aan de vereisten van deze verordening, zijn de in de artikelen 54 en 55 bedoelde procedures van toepassing.

2. Indien de Commissie voldoende redenen heeft om aan te nemen dat een product met digitale elementen in het licht van niet-technische risicofactoren een significant cyberbeveiligingsrisico vormt, stelt zij de betrokken markttoezichtautoriteiten en, indien passend, de bevoegde autoriteiten die zijn aangewezen of opgericht op grond van artikel 8 van Richtlijn (EU) 2022/2555, daarvan op de hoogte en werkt zij zo nodig met die autoriteiten samen. De Commissie houdt ook rekening met de relevantie van de vastgestelde risico's voor dat product met digitale elementen gelet op haar taken met betrekking tot de op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens die zijn bepaald in artikel 22 van Richtlijn (EU) 2022/2555, en raadpleegt zo nodig de op grond van artikel 14 van Richtlijn (EU) 2022/2555 opgerichte samenwerkingsgroep en Enisa.

3. In 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 met digitale elementen nog steeds niet aan de vereisten van deze verordening voldoet en de betrokken markttoezichtautoriteiten geen doeltreffende maatregelen hebben genomen, evalueert de Commissie de conformiteit en kan zij Enisa verzoeken ter ondersteuning daarvan een analyse te verstrekken. De Commissie stelt de betrokken markttoezichtautoriteiten daarvan in kennis. De desbetreffende marktdeelnemers werken zo nodig samen met Enisa.

4. Op basis van de in lid 3 bedoelde evaluatie 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.

5. Op basis van het in lid 4 van dit artikel bedoelde overleg kan de Commissie uitvoeringshandelingen vaststellen om te voorzien in corrigerende of beperkende maatregelen op het niveau van de Unie, onder meer door te gelasten de betrokken producten met digitale elementen binnen een redelijke termijn in verhouding tot de aard van het risico uit de handel te nemen of terug te roepen. Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

6. De Commissie stelt de betrokken marktdeelnemers onmiddellijk in kennis van de in lid 5 bedoelde uitvoeringshandelingen. De lidstaten voeren die uitvoeringshandelingen onverwijld uit en stellen de Commissie daarvan in kennis.

7. De leden 3 tot en met 6 zijn van toepassing voor de duur van de uitzonderlijke situatie die het optreden van de Commissie rechtvaardigde, mits het betrokken product met digitale elementen niet in overeenstemming is gebracht met deze verordening.

Artikel 57

Conforme producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden

1. De markttoezichtautoriteit van een lidstaat vereist van een marktdeelnemer dat hij alle passende maatregelen neemt wanneer zij na uitvoering van een evaluatie uit hoofde van artikel 54 vaststelt dat, hoewel een product met digitale elementen en de door de fabrikant ingestelde processen in overeenstemming zijn met deze verordening, deze een significant cyberbeveiligingsrisico inhoudt en, alsook een risico voor:

a) de gezondheid of veiligheid van personen;

b) de naleving van verplichtingen uit hoofde van het Unierecht of het interne recht ter bescherming van de grondrechten;

c) de beschikbaarheid, de authenticiteit, de integriteit of de vertrouwelijkheid van diensten die via een elektronisch informatiesysteem worden aangeboden door in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten, of

d) andere aspecten van de bescherming van het algemeen belang.

De in de eerste alinea bedoelde maatregelen kunnen maatregelen omvatten om ervoor te zorgen dat het betrokken product met digitale elementen en de door de fabrikant ingestelde processen de desbetreffende risico's niet meer inhouden wanneer het product op de markt wordt aangeboden, dat het product met digitale elementen uit de handel wordt genomen of dat het wordt teruggeroepen, en die maatregelen staan in verhouding tot de aard van die risico's.

2. De fabrikant of andere betrokken marktdeelnemers zorgen ervoor dat binnen de door de in lid 1 bedoelde markttoezichtautoriteit van de lidstaat vastgestelde termijn, 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 op grond van 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 en om 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 vast te stellen.

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

5. De Commissie deelt het in lid 4 bedoelde 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 van dit artikel bedoelde risico's inhoudt, stelt zij de betrokken markttoezichtautoriteiten daarvan in kennis en kan zij hen verzoeken een evaluatie uit te voeren en de in artikel 54 en in de leden 1, 2 en 3 van dit artikel bedoelde procedures te volgen.

7. In 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 met digitale elementen nog steeds de in lid 1 bedoelde risico's inhoudt en de betrokken nationale markttoezichtautoriteiten geen doeltreffende maatregelen hebben genomen, voert de Commissie een evaluatie uit van de risico's die dat product met digitale elementen inhoudt, kan zij Enisa verzoeken ter ondersteuning van die evaluatie een analyse te verstrekken en stelt zij de betrokken markttoezichtautoriteiten daarvan in kennis. De betrokken marktdeelnemers werken zo nodig samen met Enisa.

8. Op basis van de in lid 7 bedoelde evaluatie 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 van dit artikel 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 de betrokken producten met digitale elementen binnen een redelijke termijn in verhouding tot de aard van het risico uit de handel te nemen of terug te roepen. Die uitvoeringshandelingen worden volgens de in artikel 62, lid 2, bedoelde onderzoeksprocedure vastgesteld.

10. De Commissie stelt de betrokken marktdeelnemer(s) onmiddellijk in kennis van de in lid 9 bedoelde uitvoeringshandelingen. De lidstaten voeren die uitvoeringshandelingen 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 met digitale elementen de in lid 1 bedoelde risico's inhoudt.

Artikel 58

Formele non-conformiteit

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

a) de CE-markering is in strijd met artikel 29 en artikel 30 aangebracht;

b) de CE-markering 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 is, in voorkomend geval, 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 59

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 de bescherming van consumenten met betrekking tot specifieke producten met digitale elementen die in de handel worden gebracht of op de markt worden aangeboden, met name producten met digitale elementen waarvan vaak wordt vastgesteld dat zij cyberbeveiligingsrisico's inhouden.

2. De Commissie of Enisa stelt gezamenlijke activiteiten inzake toezicht op de naleving van deze verordening voor, te verrichten door markttoezichtautoriteiten op basis van indicaties of informatie dat binnen het toepassingsgebied van deze verordening vallende producten met digitale elementen in verschillende lidstaten mogelijk niet in overeenstemming zijn met de vereisten 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 gebruikmaken van alle informatie die zij heeft verkregen als gevolg van de gezamenlijke activiteiten in het kader van een door haar uitgevoerd onderzoek.

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

Artikel 60

Bezemacties

1. Markttoezichtautoriteiten voeren gelijktijdige gecoördineerde controleacties (bezemacties) uit 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. Die bezemacties kunnen inspecties omvatten van producten met digitale elementen die onder een fictieve identiteit zijn verworven.

2. Tenzij de betrokken markttoezichtautoriteiten anders overeenkomen, worden bezemacties gecoördineerd door de Commissie. De coördinator van de bezemactie maakt de geaggregeerde resultaten indien passend openbaar.

3. Wanneer Enisa bij de uitvoering van zijn taken, onder meer op basis van de op grond van artikel 14, leden 1 en 3, ontvangen meldingen, categorieën producten met digitale elementen aanwijst waarvoor bezemacties kunnen worden georganiseerd, dient het een voorstel voor een bezemactie in bij de in lid 2 van dit artikel bedoelde coördinator ter overweging door de markttoezichtautoriteiten.

4. Bij het uitvoeren van bezemacties kunnen de betrokken markttoezichtautoriteiten gebruikmaken van de in de artikelen 52 tot en met 58 bedoelde onderzoeksbevoegdheden 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 61

Uitoefening van de bevoegdheidsdelegatie

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 5, tweede alinea, artikel 7, lid 3, artikel 8, leden 1 en 2, artikel 13, lid 8, vierde alinea, artikel 14, lid 9, artikel 25, artikel 27, lid 9, artikel 28, lid 5, en artikel 31, lid 5, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor een termijn van vijf jaar met ingang van 10 december 2024. De Commissie stelt uiterlijk negen maanden voor het einde van de termijn van vijf jaar een verslag op over de bevoegdheidsdelegatie. De bevoegdheidsdelegatie wordt stilzwijgend met termijnen van dezelfde duur verlengd, tenzij het Europees Parlement of de Raad zich uiterlijk drie maanden voor het einde van elke termijn tegen die verlenging verzet.

3. Het Europees Parlement of de Raad kan de in artikel 2, lid 5, tweede alinea, artikel 7, lid 3, artikel 8, leden 1 en 2, artikel 13, lid 8, vierde alinea, artikel 14, lid 9, artikel 25, artikel 27, lid 9, artikel 28, lid 5, en artikel 31, lid 5, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het 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 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, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

6. Een op grond van artikel 2, lid 5, tweede alinea, artikel 7, lid 3, artikel 8, lid 1 of 2, artikel 13, lid 8, vierde alinea, artikel 14, lid 9, artikel 25, artikel 27, lid 9, artikel 28, lid 5, of artikel 31, 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 voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 62

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat 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, door de voorzitter van het comité daartoe wordt besloten of door een lid van het comité daarom wordt verzocht.

HOOFDSTUK VII

VERTROUWELIJKHEID EN SANCTIES

Artikel 63

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 ([37]) genoemde gevallen;

b) de doeltreffende uitvoering van deze verordening, met name ten behoeve van 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 aan 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 relevante autoriteiten van derde landen waarmee zij bilaterale of multilaterale geheimhoudingsovereenkomsten hebben gesloten die een passend beschermingsniveau waarborgen.

Artikel 64

Sancties

1. De lidstaten stellen voorschriften vast ten aanzien van de sancties die van toepassing zijn op inbreuken op deze verordening en nemen alle nodige maatregelen om ervoor te zorgen dat die sancties worden uitgevoerd. De sancties moeten doeltreffend, evenredig en afschrikkend zijn. De lidstaten stellen de Commissie onverwijld van die voorschriften en maatregelen in kennis en delen haar onverwijld alle latere wijzigingen daarvan mee.

2. Niet-naleving van de essentiële cyberbeveiligingsvereisten van bijlage I en de in de artikelen 13 en 14 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.

3. Niet-naleving van de in de artikelen 18 tot en met 23, artikel 28, artikel 30, leden 1 tot en met 4, artikel 31, leden 1 tot en met 4, artikel 32, leden 1, 2 en 3, artikel 33, lid 5, en de artikelen 39, 41, 47, 49 en 53 vastgestelde verplichtingen 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.

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

([37]) 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).

5. 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 dezelfde of andere markttoezichtautoriteiten voor een soortgelijke inbreuk op dezelfde marktdeelnemer zijn toegepast;

c) de omvang, met name met betrekking tot micro-ondernemingen en kleine en middelgrote ondernemingen, met inbegrip van start-ups, en het marktaandeel van de marktdeelnemer die de inbreuk pleegt.

6. Markttoezichtautoriteiten die administratieve geldboeten toepassen, delen de toepassing daarvan mee aan de markttoezichtautoriteiten van andere lidstaten via het in artikel 34 van Verordening (EU) 2019/1020 bedoelde informatie- en communicatiesysteem.

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

8. 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.

9. 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.

10. In afwijking van de leden 3 tot en met 9 zijn de in die leden bedoelde administratieve geldboeten niet van toepassing op:

a) fabrikanten die kunnen worden aangemerkt als micro-ondernemingen of kleine ondernemingen met betrekking tot het niet naleven van de in artikel 14, lid 2, punt a), of artikel 14, lid 4, punt a), bedoelde termijn;

b) inbreuken op deze verordening door opensourcesoftwarestewards.

Artikel 65

Representatieve vorderingen

Richtlijn (EU) 2020/1828 is van toepassing op de representatieve vorderingen die worden ingesteld tegen marktdeelnemers wegens inbreuken op bepalingen van deze verordening die de collectieve belangen van consumenten schaden of kunnen schaden.

HOOFDSTUK VIII

OVERGANGS- EN SLOTBEPALINGEN

Artikel 66

Wijziging van Verordening (EU) 2019/1020

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

"72. Verordening (EU) 2024/2847 van het Europees Parlement en de Raad (*).

(*) Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (PB L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj)".

Artikel 67

Wijziging van Richtlijn (EU) 2020/1828

Aan bijlage I bij Richtlijn (EU) 2020/1828 wordt het volgende punt toegevoegd:

"69) Verordening (EU) 2024/2847 van het Europees Parlement en de Raad (*).

(*) Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (PB L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj)".

Artikel 68

Wijziging van Verordening (EU) nr. 168/2013

In deel C1 van de tabel van bijlage II bij Verordening (EU) nr. 168/2013 van het Europees Parlement en de Raad ([38]) wordt de volgende vermelding ingevoegd:

"

16	18	bescherming van het voertuig tegen cyberaanvallen		x	x	x	x	x	x	x	x	x	x	x	x	x	x

"

Artikel 69

Overgangsbepalingen

1. Certificaten van EU-typeonderzoek en goedkeuringsbesluiten die zijn afgegeven met betrekking tot cyberbeveiligingsvereisten voor onder andere harmonisatiewetgeving van de Unie dan deze verordening vallende producten met digitale elementen, blijven geldig tot en met 11 juni 2028, tenzij zij vóór die datum vervallen, of tenzij anders bepaald in dergelijke andere harmonisatiewetgeving van de Unie, in welk geval zij geldig blijven als bedoeld in die wetgeving.

2. Voor producten met digitale elementen die vóór 11 december 2027 in de handel zijn gebracht, gelden de vereisten van deze verordening alleen indien die producten vanaf die datum ingrijpend worden gewijzigd.

3. In afwijking van lid 2 van dit artikel zijn de in artikel 14 vastgestelde verplichtingen van toepassing op alle producten met digitale elementen die binnen het toepassingsgebied van deze verordening vallen en die vóór 11 december 2027 in de handel zijn gebracht.

Artikel 70

Evaluatie en toetsing

1. Uiterlijk op 11 december 2030 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. Die verslagen worden openbaar gemaakt.

2. Uiterlijk op 11 september 2028 dient de Commissie, na raadpleging van Enisa en het CSIRT-netwerk, bij het Europees Parlement en de Raad een verslag in met een beoordeling van de doeltreffendheid van het in artikel 16 bedoelde centrale meldingsplatform en van het effect van de toepassing van de in artikel 16, lid 2, bedoelde cyberbeveiligingsgerelateerde redenen door de als coördinatoren aangewezen CSIRT's op de doeltreffendheid van het centrale meldingsplatform wat de tijdige verspreiding van ontvangen meldingen naar andere relevante CSIRT's betreft.

Artikel 71

Inwerkingtreding en toepassing

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

([38]) Verordening (EU) nr. 168/2013 van het Europees Parlement en de Raad van 15 januari 2013 betreffende de goedkeuring van en het markttoezicht op twee- of driewielige voertuigen en vierwielers (PB L 60 van 2.3.2013, blz. 52).

2. Deze verordening is van toepassing met ingang van 11 december 2027.

Artikel 14 is evenwel van toepassing met ingang van 11 september 2026, en hoofdstuk IV (de artikelen 35 tot en met 51) is van toepassing met ingang van 11 juni 2026.

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

Gedaan te Straatsburg, 23 oktober 2024.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
R. METSOLA	ZSIGMOND B. P.

BIJLAGE I

ESSENTIËLE CYBERBEVEILIGINGSVEREISTEN

Deel I Cyberbeveiligingsvereisten met betrekking tot de eigenschappen van producten met digitale elementen

1) Producten met digitale elementen worden zodanig ontworpen, ontwikkeld en geproduceerd dat zij een passend cyberbeveiligingsniveau op basis van de risico's waarborgen.

2) Op basis van de in artikel 13, lid 2, bedoelde beoordeling van cyberbeveiligingsrisico's en indien van toepassing, moeten producten met digitale elementen:

   a) op de markt worden aangeboden zonder bekende uitbuitbare kwetsbaarheden;

   b) op de markt worden aangeboden met een standaard beveiligde configuratie, tenzij anders overeengekomen tussen de fabrikant en de zakelijke gebruiker met betrekking tot een product met digitale elementen op maat, met inbegrip van de mogelijkheid om het product in zijn oorspronkelijke toestand te herstellen;

   c) garanderen dat kwetsbaarheden kunnen worden aangepakt door middel van beveiligingsupdates, waaronder, indien van toepassing, door automatische beveiligingsupdates die worden geïnstalleerd binnen een passende termijn en die als standaardinstelling zijn ingeschakeld, met een duidelijk en gebruiksvriendelijk opt-outmechanisme, door de melding van beschikbare updates aan gebruikers, en door de mogelijkheid om die tijdelijk uit te stellen;

   d) zorgen voor bescherming tegen ongeoorloofde toegang door middel van passende controlemechanismen, met inbegrip van maar niet beperkt tot authenticatie-, identiteits- of toegangsbeheersystemen, en melding maken van eventuele ongeoorloofde toegang;

   e) de vertrouwelijkheid van opgeslagen, verzonden of anderszins verwerkte persoonsgegevens of andere gegevens beschermen, bijvoorbeeld door relevante inactieve gegevens of gegevens in overdracht met behulp van geavanceerde mechanismen te versleutelen, en door andere technische middelen te gebruiken;

   f) de integriteit van opgeslagen, verzonden of anderszins verwerkte gegevens, persoonsgegevens of andere gegevens, commando's, programma's en configuraties beschermen tegen manipulatie of wijziging die niet door de gebruiker is toegestaan, en melding maken van beschadiging;

   g) uitsluitend persoons- of andere gegevens verwerken die toereikend en ter zake dienend zijn en beperkt zijn tot wat noodzakelijk is met betrekking tot het beoogde doel van het product met digitale elementen (minimale gegevensverwerking);

   h) de beschikbaarheid van essentiële en basisfuncties beschermen, ook na een incident, onder meer door middel van weerbaarheids- en beperkingsmaatregelen tegen denial of serviceaanvallen;

   i) de negatieve impact van de producten zelf of van verbonden apparaten op de beschikbaarheid van diensten die door andere apparaten of netwerken worden geleverd, tot een minimum beperken;

   j) worden ontworpen, ontwikkeld en geproduceerd om kwetsbaarheden voor aanvallen, met inbegrip van externe interfaces, te beperken;

   k) worden ontworpen, ontwikkeld en geproduceerd om de gevolgen van een incident te beperken met behulp van passende mechanismen en technieken om uitbuiting te beperken;

   l) beveiligingsgerelateerde informatie verstrekken door relevante interne activiteiten te registreren en te monitoren, met inbegrip van de toegang tot of wijziging van gegevens, diensten of functies, met een opt-outmechanisme voor de gebruiker;

   m) gebruikers de mogelijkheid bieden om alle gegevens en instellingen veilig en gemakkelijk permanent te verwijderen en, indien die gegevens naar andere producten of systemen kunnen worden overgedragen, ervoor zorgen dat dat op een veilige manier gebeurt.

Deel II Vereisten inzake de respons op kwetsbaarheden

Fabrikanten van producten met digitale elementen moeten:

1) kwetsbaarheden en componenten in producten met digitale elementen vaststellen en documenteren, onder meer door een softwarestuklijst op te stellen in een algemeen gebruikt en machineleesbaar formaat waarin ten minste de afhankelijkheden van de producten op het hoogste niveau worden aangegeven;

2) in verband met de risico's die verbonden zijn aan producten met digitale elementen, kwetsbaarheden onverwijld aanpakken en verhelpen, onder meer door beveiligingsupdates te verstrekken; indien technisch haalbaar moeten nieuwe beveiligingsupdates afzonderlijk van de functionaliteitsupdates worden verstrekt;

3) de beveiliging van het product met digitale elementen op doeltreffende en regelmatige wijze testen en evalueren;

4) zodra een beveiligingsupdate beschikbaar is gesteld, informatie delen en openbaar maken over verholpen kwetsbaarheden, met inbegrip van een beschrijving van de kwetsbaarheden, informatie aan de hand waarvan gebruikers het betreffende product met digitale elementen kunnen identificeren, de gevolgen van de kwetsbaarheden, de ernst ervan en duidelijke en toegankelijke informatie die gebruikers helpt de kwetsbaarheden te verhelpen; in naar behoren gemotiveerde gevallen kunnen fabrikanten, wanneer zij van mening zijn dat de beveiligingsrisico's van openbaarmaking zwaarder wegen dan de beveiligingsvoordelen, het openbaar maken van informatie over een verholpen kwetsbaarheid uitstellen totdat de gebruikers de mogelijkheid hebben gekregen de desbetreffende patch uit te voeren;

5) een beleid inzake gecoördineerde openbaarmaking van kwetsbaarheden invoeren en handhaven;

6) maatregelen nemen om het delen van informatie over potentiële kwetsbaarheden in hun product met digitale elementen en in componenten van derden in dat product te vergemakkelijken, onder meer door een contactadres te verstrekken voor de melding van de kwetsbaarheden die in het product met digitale elementen zijn ontdekt;

7) voorzien in mechanismen om updates voor producten met digitale elementen veilig te verspreiden om ervoor te zorgen dat kwetsbaarheden tijdig en, waar van toepassing voor beveiligingsupdates, automatisch worden verholpen of beperkt;

8) ervoor zorgen dat, wanneer er beveiligingsupdates beschikbaar zijn om vastgestelde beveiligingsproblemen aan te pakken, die onverwijld en — tenzij anders overeengekomen tussen een fabrikant en een zakelijke gebruiker met betrekking tot een product met digitale elementen op maat — kosteloos worden verspreid, vergezeld van adviezen met relevante informatie voor gebruikers, onder meer over eventueel te nemen maatregelen.

BIJLAGE II

INFORMATIE EN INSTRUCTIES VOOR DE GEBRUIKER

Het product met digitale elementen gaat ten minste vergezeld van:

1. de naam, de geregistreerde handelsnaam of het geregistreerde merk van de fabrikant, en het postadres, het e-mailadres of een ander digitaal communicatiemiddel alsook, indien beschikbaar, de website waarop contact met de fabrikant kan worden opgenomen;
2. het centraal contactpunt waar informatie over kwetsbaarheden van het product met digitale elementen kan worden gemeld en ontvangen, en waar het beleid van de fabrikant inzake gecoördineerde openbaarmaking van kwetsbaarheden kan worden gevonden;
3. naam en type en eventuele aanvullende informatie die de unieke identificatie van het product met digitale elementen mogelijk maakt;
4. het beoogde doel van het product met digitale elementen, met inbegrip van de door de fabrikant geboden beveiligingsomgeving, alsook de essentiële functies en informatie over de beveiligingseigenschappen van het product;
5. elke bekende of voorzienbare omstandigheid die verband houdt met het gebruik van het product met digitale elementen overeenkomstig het beoogde doel ervan of in een situatie van redelijkerwijs voorzienbaar verkeerd gebruik, die tot significante cyberbeveiligingsrisico's kan leiden;
6. indien van toepassing, het internetadres waarop de EU-conformiteitsverklaring kan worden geraadpleegd;
7. het soort technische beveiligingsondersteuning dat door de fabrikant wordt aangeboden en de einddatum van de ondersteuningsperiode tijdens welke gebruikers kunnen verwachten dat kwetsbaarheden worden aangepakt en zij beveiligingsupdates ontvangen;
8. gedetailleerde instructies of een internetadres met betrekking tot dergelijke gedetailleerde instructies en informatie over:
   a) de nodige maatregelen tijdens de eerste inbedrijfstelling en gedurende de hele levensduur van het product met digitale elementen om een veilig gebruik ervan te waarborgen;
   b) hoe veranderingen in het product met digitale elementen van invloed kunnen zijn op de beveiliging van gegevens;
   c) hoe veiligheidsrelevante updates kunnen worden geïnstalleerd;
   d) de veilige buitenbedrijfstelling van het product met digitale elementen, met inbegrip van informatie over de wijze waarop gebruikersgegevens veilig kunnen worden verwijderd;
   e) hoe de standaardinstelling die de automatische installatie van beveiligingsupdates mogelijk maakt, zoals voorgeschreven in deel I, punt 2, c), van bijlage I, kan worden uitgeschakeld;
   f) indien het product met digitale elementen bestemd is om te worden geïntegreerd in andere producten met digitale elementen, de informatie die de integrator nodig heeft om te voldoen aan de essentiële cyberbeveiligingsvereisten van bijlage I en de documentatievereisten van bijlage VII.
9. indien de fabrikant besluit de softwarestuklijst ter beschikking te stellen van de gebruiker, informatie over waar de softwarestuklijst kan worden geraadpleegd.

BIJLAGE III

BELANGRIJKE PRODUCTEN MET DIGITALE ELEMENTEN

Klasse I

1. software en hardware voor identiteitsbeheersystemen en voor het beheer van geprivilegieerde toegang, met inbegrip van lezers voor authenticatie en toegangscontrole, waaronder biometrische lezers
2. op zichzelf staande en ingebedde browsers
3. wachtwoordbeheer
4. software die kwaadaardige software opzoekt, verwijdert of in quarantaine plaatst
5. producten met digitale elementen met de functie van virtueel particulier netwerk (VPN)
6. netwerkbeheersystemen
7. Security information and event management-systemen (SIEM) (beveiligingsinformatie en evenementenbeheer)
8. bootmanagement
9. publiekesleutelinfrastructuur en software voor de afgifte van digitale certificaten
10. fysieke en virtuele netwerkinterfaces
11. besturingssystemen
12. routers, modems bestemd voor verbinding met het internet, en netwerkswitches
13. microprocessoren met beveiligingsgerelateerde functies
14. microcontrollers met beveiligingsgerelateerde functies
15. toepassingsspecifieke geïntegreerde schakelingen (ASIC) en veld-programmeerbare gatearrays (FPGA) met beveiligingsgerelateerde functies
16. virtuele assistenten voor slimme huizen voor algemene doeleinden
17. producten voor slimme huizen met beveiligingsfuncties, met inbegrip van slimme deursloten, beveiligingscamera's, babymonitoringsystemen en alarmsystemen
18. met het internet verbonden speelgoed dat onder Richtlijn 2009/48/EG van het Europees Parlement en de Raad [1] valt en sociale interactieve functies (bv. spreken of filmen) of locatietraceringsfuncties heeft
19. persoonlijke wearables die op een menselijk lichaam moeten worden gedragen of geplaatst en bedoeld zijn voor gezondheidsmonitoring (zoals tracking) en die niet onder Verordening (EU) 2017/745 of (EU) 2017/746 vallen, of persoonlijke wearables die bestemd zijn voor gebruik door en voor kinderen

Klasse II

1. hypervisors en containerruntimesystemen die de gevirtualiseerde uitvoering van besturingssystemen en soortgelijke omgevingen ondersteunen
2. firewalls, inbraakdetectiesystemen en inbraakpreventiesystemen
3. manipulatiebestendige microprocessoren
4. manipulatiebestendige microcontrollers

[1] Richtlijn 2009/48/EG van het Europees Parlement en de Raad van 18 juni 2009 betreffende de veiligheid van speelgoed (PB L 170 van 30.6.2009, blz. 1).

BIJLAGE IV

KRITIEKE PRODUCTEN MET DIGITALE ELEMENTEN

1. hardwareapparaten met beveiligingskastje
2. gateways voor slimme meters binnen slimme-metersystemen zoals gedefinieerd in artikel 2, punt 23), van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad [1] en andere apparaten voor geavanceerde beveiligingsdoeleinden, onder meer voor beveiligde cryptoverwerking
3. smartcards of soortgelijke apparaten, met inbegrip van secure elements (beveiligde elementen)

[1] Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (PB L 158 van 14.6.2019, blz. 125).

BIJLAGE V

EU-CONFORMITEITSVERKLARING

De in artikel 28 bedoelde EU-conformiteitsverklaring omvat alle volgende informatie:

1. naam en type van het product met digitale elementen en eventuele aanvullende informatie die de unieke identificatie ervan mogelijk maakt
2. naam en adres van de fabrikant of de gemachtigde vertegenwoordiger van de fabrikant
3. een vermelding dat de EU-conformiteitsverklaring wordt verstrekt onder de uitsluitende verantwoordelijkheid van de aanbieder
4. voorwerp van de verklaring (identificatie van het product met digitale elementen aan de hand waarvan het product kan worden getraceerd; indien passend kan een foto worden bijgevoegd)
5. een verklaring dat het hierboven beschreven voorwerp van de verklaring in overeenstemming is met de desbetreffende harmonisatiewetgeving van de Unie
6. verwijzingen naar alle gebruikte relevante geharmoniseerde normen of andere gemeenschappelijke specificaties of cyberbeveiligingscertificering met betrekking waartoe de conformiteitsverklaring is aangegeven
7. indien van toepassing, de naam en het nummer van de aangemelde instantie, een beschrijving van de uitgevoerde conformiteitsbeoordelingsprocedure en de identificatie van het afgegeven certificaat;
8. aanvullende informatie:

   Ondertekend voor en namens:

   (plaats en datum van afgifte):

   (naam, functie) (handtekening):

BIJLAGE VI

VEREENVOUDIGDE EU-CONFORMITEITSVERKLARING

De in artikel 13, lid 20, bedoelde vereenvoudigde EU-conformiteitsverklaring wordt als volgt geformuleerd:

Hierbij verklaart … [naam van de fabrikant] dat het product met digitale elementen type … [aanduiding van het type product met digitale elementen] in overeenstemming is met Verordening (EU) 2024/2847 ([1]).

De volledige tekst van de EU-conformiteitsverklaring kan worden geraadpleegd op het volgende internetadres:

([1]) PB L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

BIJLAGE VII

INHOUD VAN DE TECHNISCHE DOCUMENTATIE

De in artikel 31 bedoelde technische documentatie bevat ten minste de volgende informatie, voor zover van toepassing op het desbetreffende product met digitale elementen:

1. een algemene beschrijving van het product met digitale elementen, met inbegrip van:
   a) het beoogde doel ervan;
   b) versies van software die van invloed zijn op de naleving van de essentiële cyberbeveiligingsvereisten;
   c) wanneer het product met digitale elementen een hardwareproduct is, foto's of illustraties waarop de externe kenmerken, markering en interne lay-out te zien zijn;
   d) gebruikersinformatie en -instructies zoals beschreven in bijlage II;
2. een beschrijving van het ontwerp, de ontwikkeling en de productie van het product met digitale elementen en de procedures inzake de respons op kwetsbaarheden, met inbegrip van:
   a) noodzakelijke informatie over het ontwerp en de ontwikkeling van het product met digitale elementen, met inbegrip van, indien van toepassing, tekeningen en schema's en een beschrijving van de systeemarchitectuur waarin wordt uitgelegd hoe softwarecomponenten voortbouwen op elkaar of elkaar aanvullen en zijn geïntegreerd in de algemene verwerking;
   b) noodzakelijke informatie en specificaties van de door de fabrikant ingestelde processen inzake de respons op kwetsbaarheden, met inbegrip van de softwarestuklijst, het gecoördineerde beleid inzake openbaarmaking van kwetsbaarheden, bewijs van het verstrekken van een contactadres voor de melding van de kwetsbaarheden en een beschrijving van de gekozen technische oplossingen voor de veilige verspreiding van updates;
   c) noodzakelijke informatie en specificaties van de productie- en monitoringprocessen van het product met digitale elementen en de validering van die processen;
3. een beoordeling van de cyberbeveiligingsrisico's waartegen het product met digitale elementen wordt ontworpen, ontwikkeld, geproduceerd, geleverd en onderhouden op grond van artikel 13, met inbegrip van de wijze waarop de essentiële cyberbeveiligingsvereisten van deel I van bijlage I van toepassing zijn;
4. relevante informatie die in aanmerking is genomen om op grond van artikel 13, lid 8, de ondersteuningsperiode van het product met digitale elementen te bepalen;
5. een lijst van de geheel of gedeeltelijk toegepaste geharmoniseerde normen waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, gemeenschappelijke specificaties als bedoeld in artikel 27 van deze verordening of Europese cyberbeveiligingscertificeringsregelingen die zijn vastgesteld op grond van Verordening (EU) 2019/881 op grond van artikel 27, lid 8, van deze verordening en, indien die geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen niet zijn toegepast, een beschrijving van de gekozen oplossingen om aan de essentiële cyberbeveiligingsvereisten van de delen I en II van bijlage I te voldoen, met inbegrip van een lijst van andere relevante technische specificaties die zijn toegepast. In het geval van gedeeltelijk toegepaste geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen, wordt in de technische documentatie gespecificeerd welke delen zijn toegepast;
6. verslagen van de tests die zijn uitgevoerd om de conformiteit van het product met digitale elementen en van de procedures inzake de respons op kwetsbaarheden met de toepasselijke essentiële cyberbeveiligingsvereisten van de delen I en II van bijlage I te verifiëren;
7. een exemplaar van de EU-conformiteitsverklaring;
8. indien van toepassing, de softwarestuklijst, ingevolge een met redenen omkleed verzoek van een markttoezichtautoriteit, op voorwaarde dat dat noodzakelijk is om die autoriteit in staat te stellen de naleving van de essentiële cyberbeveiligingsvereisten van bijlage I te controleren.

BIJLAGE VIII

CONFORMITEITSBEOORDELINGSPROCEDURES

Deel I Conformiteitsbeoordelingsprocedure op basis van interne controle (op basis van module A)

1. Met "interne controle" wordt de conformiteitsbeoordelingsprocedure bedoeld waarbij de fabrikant de verplichtingen van de punten 2, 3 en 4 van dit deel nakomt en op eigen verantwoordelijkheid garandeert en verklaart dat de producten met digitale elementen aan alle essentiële cyberbeveiligingsvereisten van deel I van bijlage I voldoen en dat de fabrikant aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I voldoet.

2. De fabrikant stelt de in bijlage VII beschreven technische documentatie op.

3. Ontwerp, ontwikkeling, productie en respons op kwetsbaarheden van producten met digitale elementen

   De fabrikant neemt alle nodige maatregelen om ervoor te zorgen dat het ontwerp, de ontwikkeling, de productie en de procedures inzake de respons op kwetsbaarheden en de monitoring daarvan waarborgen dat de vervaardigde of ontwikkelde producten met digitale elementen en de door de fabrikant ingestelde processen in overeenstemming zijn met de essentiële cyberbeveiligingsvereisten van de delen I en II van bijlage I.

4. Conformiteitsmarkering en conformiteitsverklaring

   4.1. De fabrikant brengt de CE-markering aan op elk afzonderlijk product met digitale elementen dat aan de toepasselijke vereisten van deze verordening voldoet.

   4.2. De fabrikant stelt overeenkomstig artikel 28 voor elk product met digitale elementen een schriftelijke EU-conformiteitsverklaring op en houdt die verklaring, samen met de technische documentatie, tot tien jaar na het in de handel brengen van het product met digitale elementen of gedurende de ondersteuningsperiode, indien die langer is, ter beschikking van de nationale autoriteiten. In de EU-conformiteitsverklaring wordt het product met digitale elementen geïdentificeerd waarvoor de verklaring is opgesteld. Een kopie van de EU-conformiteitsverklaring wordt op verzoek aan de relevante autoriteiten verstrekt.

5. Gemachtigde vertegenwoordigers

   De in punt 4 vervatte verplichtingen van de fabrikant kunnen namens en onder de verantwoordelijkheid van de fabrikant worden vervuld door de gemachtigde vertegenwoordiger van de fabrikant, op voorwaarde dat de relevante verplichtingen in het mandaat gespecificeerd zijn.

Deel II EU-typeonderzoek (op basis van module B)

1. Met "EU-typeonderzoek" wordt dat gedeelte van een conformiteitsbeoordelingsprocedure bedoeld waarin een aangemelde instantie het technisch ontwerp en de ontwikkeling van een product met digitale elementen en de door de fabrikant ingestelde procedures inzake de respons op kwetsbaarheden onderzoekt en verklaart dat een product met digitale elementen aan de essentiële cyberbeveiligingsvereisten van deel I van bijlage I voldoet en dat de fabrikant aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I voldoet.

2. Het EU-typeonderzoek wordt uitgevoerd door beoordeling van de geschiktheid van het technisch ontwerp en ontwikkeling van het product met digitale elementen door middel van het onderzoek van de technische documentatie en het bewijsmateriaal die zijn bedoeld in punt 3, en het onderzoek van monsters van een of meer kritieke delen van het product (combinatie van productietype en ontwerptype).

3. De fabrikant dient een aanvraag voor het EU-typeonderzoek in bij een aangemelde instantie van zijn keuze.

   De aanvraag omvat:

   3.1. naam en adres van de fabrikant en, indien de aanvraag wordt ingediend door de gemachtigde vertegenwoordiger van de fabrikant, de naam en het adres van die gemachtigde vertegenwoordiger;

   3.2. een schriftelijke verklaring dat dezelfde aanvraag niet is ingediend bij een andere aangemelde instantie;

   3.3. de technische documentatie aan de hand waarvan kan worden beoordeeld of het product met digitale elementen voldoet aan de toepasselijke essentiële cyberbeveiligingsvereisten van deel I van bijlage I en de procedures inzake de respons op kwetsbaarheden van de fabrikant van deel II van bijlage I, en die een adequate analyse en beoordeling van de risico's omvat. In de technische documentatie worden de toepasselijke vereisten vermeld en de documentatie heeft, voor zover relevant voor de beoordeling, betrekking op het ontwerp, de vervaardiging en de werking van het product met digitale elementen. De technische documentatie bevat, indien van toepassing, ten minste de in bijlage VII vermelde elementen;

3.4. het bewijsmateriaal voor de adequaatheid van de technische ontwerp- en ontwikkelingsoplossingen en de procedures inzake de respons op kwetsbaarheden. In het bewijsmateriaal worden alle gebruikte documenten vermeld, met name wanneer de desbetreffende geharmoniseerde normen of technische specificaties niet volledig zijn toegepast. Zo nodig worden ook de resultaten vermeld van tests die door een geschikt laboratorium van de fabrikant of namens en onder de verantwoordelijkheid van de fabrikant door een ander laboratorium zijn verricht.

4. De aangemelde instantie:

4.1. onderzoekt de technische documentatie en het bewijsmateriaal om te beoordelen of het technisch ontwerp en de ontwikkeling van het product met digitale elementen voldoen aan de essentiële cyberbeveiligingsvereisten van deel I van bijlage I en of de door de fabrikant ingestelde procedures inzake de respons op kwetsbaarheden voldoen aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I;

4.2. controleert of de monsters overeenkomstig de technische documentatie zijn ontwikkeld of vervaardigd, en stelt vast welke elementen zijn ontworpen en ontwikkeld overeenkomstig de toepasselijke bepalingen van de desbetreffende geharmoniseerde normen of technische specificaties, alsook welke elementen zijn ontworpen en ontwikkeld zonder de desbetreffende bepalingen van die normen toe te passen;

4.3. verricht de nodige onderzoeken en tests, of laat die verrichten om, wanneer de fabrikant ervoor heeft gekozen de oplossingen uit de desbetreffende geharmoniseerde normen of technische specificaties voor de vereisten van bijlage I toe te passen, te controleren of die op de juiste wijze zijn toegepast;

4.4. verricht de nodige onderzoeken en tests, of laat die verrichten om, ingeval de oplossingen in de desbetreffende geharmoniseerde normen of technische specificaties voor de cyberbeveiligingsvereisten van bijlage I niet zijn toegepast, te controleren of de door de fabrikant gekozen oplossingen aan de desbetreffende essentiële cyberbeveiligingsvereisten voldoen;

4.5. stelt in overleg met de fabrikant de plaats vast waar de onderzoeken en tests zullen worden uitgevoerd.

5. De aangemelde instantie stelt een evaluatieverslag op over de overeenkomstig punt 4 verrichte activiteiten en de resultaten daarvan. Onverminderd haar verplichtingen jegens de aanmeldende autoriteiten, maakt de aangemelde instantie de inhoud van dat verslag uitsluitend met instemming van de fabrikant geheel of gedeeltelijk openbaar.

6. Wanneer het type en de procedures inzake de respons op kwetsbaarheden aan de essentiële cyberbeveiligingsvereisten van bijlage I voldoen, verstrekt de aangemelde instantie de fabrikant een certificaat van EU-typeonderzoek. Het certificaat bevat de naam en het adres van de fabrikant, de conclusies van het onderzoek, de eventuele voorwaarden voor de geldigheid ervan en de nodige gegevens voor de identificatie van het goedgekeurde type en de goedgekeurde procedures inzake de respons op kwetsbaarheden. Bij het certificaat kunnen één of meerdere bijlagen worden gevoegd.

Het certificaat en de bijlagen bevatten alle relevante informatie om de conformiteit van de vervaardigde of ontwikkelde producten met digitale elementen met het onderzochte type en de onderzochte procedures inzake de respons op kwetsbaarheden te kunnen evalueren en controle tijdens het gebruik mogelijk te maken.

Wanneer het type en de procedures inzake de respons op kwetsbaarheden niet voldoen aan de toepasselijke essentiële cyberbeveiligingsvereisten van bijlage I, weigert de aangemelde instantie een certificaat van EU-typeonderzoek af te geven en stelt zij de aanvrager daarvan in kennis, met vermelding van de gedetailleerde redenen voor haar weigering.

7. De aangemelde instantie houdt zich op de hoogte van alle veranderingen in de algemeen erkende stand van de techniek die erop wijzen dat het goedgekeurde type en de goedgekeurde procedures inzake de respons op kwetsbaarheden mogelijk niet langer voldoen aan de toepasselijke essentiële cyberbeveiligingsvereisten van bijlage I, en bepaalt of dergelijke wijzigingen nader onderzoek vereisen. Als dat het geval is, stelt de aangemelde instantie de fabrikant daarvan in kennis.

De fabrikant brengt de aangemelde instantie die de technische documentatie betreffende het certificaat van EU-typeonderzoek bewaart op de hoogte van alle wijzigingen van het goedgekeurde type en de goedgekeurde procedures inzake de respons op kwetsbaarheden die van invloed kunnen zijn op de conformiteit met de essentiële cyberbeveiligingsvereisten van bijlage I of de voorwaarden voor de geldigheid van het certificaat. Dergelijke wijzigingen vereisen een aanvullende goedkeuring in de vorm van een bijvoegsel bij het oorspronkelijke certificaat van EU-typeonderzoek.

8. De aangemelde instantie verricht periodieke audits om ervoor te zorgen dat de in deel II van bijlage I beschreven procedures inzake de respons op kwetsbaarheden adequaat worden uitgevoerd.

9. Elke aangemelde instantie brengt haar aanmeldende autoriteiten op de hoogte van de door haar verstrekte of ingetrokken certificaten van EU-typeonderzoek en eventuele bijvoegsels daarbij, en verstrekt haar aanmeldende autoriteiten op gezette tijden of op verzoek een lijst van geweigerde, geschorste of anderszins beperkte certificaten en eventuele bijvoegsels daarbij.

   Elke aangemelde instantie brengt de andere aangemelde instanties op de hoogte van de door haar geweigerde, ingetrokken, geschorste of anderszins beperkte certificaten van EU-typeonderzoek en eventuele bijvoegsels daarbij, alsook, op verzoek, van de door haar verstrekte certificaten en bijvoegsels daarbij.

   De Commissie, de lidstaten en de andere aangemelde instanties kunnen op verzoek een kopie van de certificaten van EU-typeonderzoek en eventuele bijvoegsels ontvangen. De Commissie en de lidstaten kunnen op verzoek een kopie van de technische documentatie en de resultaten van het door de aangemelde instantie verrichte onderzoek ontvangen. De aangemelde instantie bewaart een kopie van het certificaat van EU-typeonderzoek, de bijlagen en bijvoegsels daarbij, alsook het technisch dossier, met inbegrip van de door de fabrikant verstrekte documentatie, tot het einde van de geldigheidsduur van het certificaat.

10. De fabrikant houdt tot tien jaar na het in de handel brengen van het product met digitale elementen of gedurende de ondersteuningsperiode, indien die langer is, een kopie van het certificaat van EU-typeonderzoek en de bijlagen en bijvoegsels daarbij, samen met de technische documentatie, ter beschikking van de nationale autoriteiten.

11. De gemachtigde vertegenwoordiger van de fabrikant kan de in punt 3 bedoelde aanvraag indienen en de in de punten 7 en 10 vermelde verplichtingen vervullen, op voorwaarde dat de relevante verplichtingen in het mandaat gespecificeerd zijn.

Deel III Conformiteit met het type op basis van interne productiecontrole (op basis van module C)

1. Met "conformiteit met het type op basis van interne productiecontrole" wordt het gedeelte van een conformiteitsbeoordelingsprocedure bedoeld waarin de fabrikant de verplichtingen van de punten 2 en 3 nakomt en garandeert en verklaart dat de betrokken producten met digitale elementen in overeenstemming zijn met het type dat is beschreven in het certificaat van EU-typeonderzoek en aan de essentiële cyberbeveiligingsvereisten van deel I van bijlage I voldoen, en dat de fabrikant aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I voldoet.

2. Productie

   De fabrikant neemt alle nodige maatregelen om ervoor te zorgen dat de productie en de monitoring daarvan garanderen dat de vervaardigde producten met digitale elementen in overeenstemming zijn met het goedgekeurde type dat is beschreven in het certificaat van EU-typeonderzoek en met de essentiële cyberbeveiligingsvereisten van deel I van bijlage I, en garandeert dat de fabrikant aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I voldoet.

3. Conformiteitsmarkering en conformiteitsverklaring

   3.1. De fabrikant brengt de CE-markering aan op elk afzonderlijk product met digitale elementen dat in overeenstemming is met het type dat is beschreven in het certificaat van EU-typeonderzoek en voldoet aan de toepasselijke vereisten van deze verordening.

   3.2. De fabrikant stelt voor elk productmodel een schriftelijke conformiteitsverklaring op en houdt die verklaring tot tien jaar na het in de handel brengen van het product met digitale elementen of gedurende de ondersteuningsperiode, indien die langer is, ter beschikking van de nationale autoriteiten. In de conformiteitsverklaring wordt het productmodel geïdentificeerd waarvoor de verklaring is opgesteld. Een kopie van de conformiteitsverklaring wordt op verzoek aan de relevante autoriteiten verstrekt.

4. Gemachtigde vertegenwoordiger

   De in punt 3 vervatte verplichtingen van de fabrikant kunnen namens en onder de verantwoordelijkheid van de fabrikant worden vervuld door de gemachtigde vertegenwoordiger van de fabrikant, op voorwaarde dat de relevante verplichtingen in het mandaat gespecificeerd zijn.

Deel IV Conformiteit op basis van volledige kwaliteitsborging (op basis van module H)

1. Met "conformiteit op basis van volledige kwaliteitsborging" wordt de conformiteitsbeoordelingsprocedure bedoeld waarbij de fabrikant de verplichtingen van de punten 2 en 5 van dit deel nakomt en op eigen verantwoordelijkheid garandeert en verklaart dat de betrokken producten met digitale elementen of productcategorieën aan alle essentiële cyberbeveiligingsvereisten van deel I van bijlage I voldoen en dat de door de fabrikant ingestelde procedures inzake de respons op kwetsbaarheden aan de vereisten van deel II van bijlage I voldoen.

2. Ontwerp, ontwikkeling, productie en respons op kwetsbaarheden van producten met digitale elementen

De fabrikant past een goedgekeurd kwaliteitssysteem als bedoeld in punt 3 toe op het ontwerp, de ontwikkeling en de eindproductcontrole en producttests van de betrokken producten met digitale elementen en op de respons op kwetsbaarheden, handhaaft de doeltreffendheid ervan gedurende de ondersteuningsperiode en is onderworpen aan toezicht als omschreven in punt 4.

3. Kwaliteitssysteem

3.1. De fabrikant dient voor de betrokken producten met digitale elementen bij een aangemelde instantie van zijn keuze een aanvraag tot beoordeling van zijn kwaliteitssysteem in.

De aanvraag omvat:

a) de naam en het adres van de fabrikant en, indien de aanvraag wordt ingediend door de gemachtigde vertegenwoordiger van de fabrikant, de naam en het adres van die gemachtigde vertegenwoordiger;

b) de technische documentatie voor één model van elke categorie producten met digitale elementen die bestemd is om te worden vervaardigd of ontwikkeld. De technische documentatie bevat, indien van toepassing, ten minste de in bijlage VII vermelde elementen;

c) de documentatie over het kwaliteitssysteem, en

d) een schriftelijke verklaring dat dezelfde aanvraag niet is ingediend bij een andere aangemelde instantie.

3.2. Het kwaliteitssysteem waarborgt dat de producten met digitale elementen voldoen aan de essentiële cyberbeveiligingsvereisten van deel I van bijlage I en dat de door de fabrikant ingestelde procedures inzake de respons op kwetsbaarheden voldoen aan de cyberbeveiligingsvereisten van deel II van bijlage I.

Alle door de fabrikant vastgestelde elementen, vereisten en bepalingen worden systematisch en geordend gedocumenteerd in de vorm van schriftelijk vastgelegde beleidsmaatregelen, procedures en instructies. Aan de hand van die documentatie van het kwaliteitssysteem moeten de kwaliteitsprogramma's, -plannen, -handboeken en -dossiers eenduidig kunnen worden geïnterpreteerd.

Zij bevat met name een behoorlijke beschrijving van:

a) de kwaliteitsdoelstellingen en het organisatieschema, de verantwoordelijkheden en bevoegdheden van het management met betrekking tot ontwerp, ontwikkeling, productkwaliteit en respons op kwetsbaarheden;

b) de technische ontwerp- en ontwikkelingsspecificaties, met inbegrip van normen, die zullen worden toegepast en, indien de relevante geharmoniseerde normen of technische specificaties niet volledig zullen worden toegepast, de middelen die zullen worden gebruikt om ervoor te zorgen dat aan de essentiële cyberbeveiligingsvereisten van deel I van bijlage I die op de producten met digitale elementen van toepassing zijn, wordt voldaan;

c) de procedurele specificaties, met inbegrip van normen, die zullen worden toegepast en, indien de relevante geharmoniseerde normen of technische specificaties niet volledig zullen worden toegepast, de middelen die zullen worden gebruikt om ervoor te zorgen dat aan de essentiële cyberbeveiligingsvereisten van deel II van bijlage I die op de fabrikant van toepassing zijn, wordt voldaan;

d) de controle op het ontwerp en de ontwikkeling, alsook verificatietechnieken, processen en systematische maatregelen voor ontwerp en ontwikkeling die zullen worden gebruikt bij het ontwerpen en ontwikkelen van de producten met digitale elementen in de betrokken productcategorie;

e) de bijbehorende productie-, kwaliteitscontrole- en kwaliteitsborgingstechnieken, -processen en systematische maatregelen die zullen worden gebruikt;

f) de onderzoeken en tests die voor, tijdens en na de productie zullen worden verricht, en de frequentie daarvan;

g) de kwaliteitsdossiers, zoals inspectieverslagen, test- en kalibratiegegevens en rapporten betreffende de kwalificaties van het betrokken personeel;

h) de middelen om het bereiken van de vereiste ontwerp- en productkwaliteit en de doeltreffende werking van het kwaliteitssysteem te monitoren.

3.3. De aangemelde instantie beoordeelt het kwaliteitssysteem om te controleren of het aan de in punt 3.2 bedoelde vereisten voldoet.

Zij veronderstelt dat aan die vereisten wordt voldaan voor elementen van het kwaliteitssysteem die voldoen aan de desbetreffende specificaties van de nationale norm ter uitvoering van de desbetreffende geharmoniseerde norm of technische specificatie.

Het auditteam heeft ervaring met kwaliteitsmanagementsystemen. Bovendien heeft ten minste één lid van het team ervaring met beoordelingen in het betrokken productgebied en de betrokken producttechnologie en is op de hoogte van de toepasselijke vereisten van deze verordening. De audit omvat een beoordelingsbezoek aan de bedrijfsruimten van de fabrikant, indien dergelijke bedrijfsruimten bestaan. Het auditteam evalueert de in punt 3.1, b), bedoelde technische documentatie om te controleren of de fabrikant zich bewust is van de toepasselijke vereisten van deze verordening en in staat is het vereiste onderzoek te verrichten om te waarborgen dat het product met digitale elementen aan die vereisten voldoet.

De fabrikant of de gemachtigde vertegenwoordiger van de fabrikant wordt van de beslissing in kennis gesteld.

In die kennisgeving moeten de conclusies van de audit worden opgenomen, evenals de met redenen omklede beoordelingsbeslissing.

3.4. De fabrikant verbindt zich ertoe de verplichtingen die voortvloeien uit het goedgekeurde kwaliteitssysteem na te komen en ervoor te zorgen dat het systeem passend en doeltreffend blijft.

3.5. De fabrikant brengt de aangemelde instantie die het kwaliteitssysteem heeft goedgekeurd op de hoogte van elke voorgenomen wijziging van het kwaliteitssysteem.

De aangemelde instantie evalueert de voorgestelde wijzigingen en beslist of het gewijzigde kwaliteitssysteem blijft voldoen aan de in punt 3.2 bedoelde vereisten dan wel of een nieuwe beoordeling noodzakelijk is.

Zij stelt de fabrikant van haar besluit in kennis. In die kennisgeving moeten de conclusies van het onderzoek worden opgenomen, evenals de met redenen omklede beoordelingsbeslissing.

4. Toezicht onder de verantwoordelijkheid van de aangemelde instantie

4.1. Het toezicht heeft tot doel te controleren of de fabrikant naar behoren voldoet aan de verplichtingen die voortvloeien uit het goedgekeurde kwaliteitssysteem.

4.2. De fabrikant verleent de aangemelde instantie voor beoordelingsdoeleinden toegang tot de ontwerp-, ontwikkelings-, productie-, inspectie-, test- en opslaglocaties en verstrekt haar alle nodige informatie, met name:

a) de documentatie over het kwaliteitssysteem;

b) de kwaliteitsdossiers als bedoeld in het deel van het kwaliteitssysteem dat betrekking heeft op het ontwerp, zoals resultaten van analyses, berekeningen en tests;

c) de kwaliteitsdossiers als bedoeld in het deel van het kwaliteitssysteem dat betrekking heeft op de vervaardiging, zoals inspectieverslagen, test- en kalibratiegegevens en rapporten betreffende de kwalificaties van het betrokken personeel.

4.3. De aangemelde instantie verricht periodieke audits om te controleren of de fabrikant het kwaliteitssysteem onderhoudt en toepast en verstrekt de fabrikant een auditverslag.

5. Conformiteitsmarkering en conformiteitsverklaring

5.1. De fabrikant brengt de CE-markering en, onder de verantwoordelijkheid van de in punt 3.1 bedoelde aangemelde instantie, het identificatienummer van die instantie aan op elk afzonderlijk product met digitale elementen dat aan de vereisten van deel I van bijlage I voldoet.

5.2. De fabrikant stelt voor elk productmodel een schriftelijke conformiteitsverklaring op en houdt die verklaring tot tien jaar na het in de handel brengen van het product met digitale elementen of gedurende de ondersteuningsperiode, indien die langer is, ter beschikking van de nationale autoriteiten. In de conformiteitsverklaring wordt het productmodel geïdentificeerd waarvoor de verklaring is opgesteld.

Een kopie van de conformiteitsverklaring wordt op verzoek aan de relevante autoriteiten verstrekt.

6. De fabrikant houdt gedurende een periode van ten minste tien jaar nadat het product met digitale elementen in de handel is gebracht of gedurende de ondersteuningsperiode, indien die langer is, het volgende ter beschikking van de nationale autoriteiten:

a) de in punt 3.1 bedoelde technische documentatie;

b) de in punt 3.1 bedoelde documentatie over het kwaliteitssysteem;

c) de in punt 3.5 bedoelde wijzigingen zoals die zijn goedgekeurd;

d) de in de punten 3.5 en 4.3 bedoelde beslissingen en verslagen van de aangemelde instantie.

7. Elke aangemelde instantie brengt haar aanmeldende autoriteiten op de hoogte van de door haar verstrekte of ingetrokken goedkeuringen van kwaliteitssystemen en verstrekt haar aanmeldende autoriteiten op gezette tijden of op verzoek een lijst van geweigerde, geschorste of anderszins beperkte goedkeuringen voor kwaliteitssystemen.

Elke aangemelde instantie brengt de andere aangemelde instanties op de hoogte van de door haar geweigerde, geschorste of ingetrokken goedkeuringen voor kwaliteitssystemen alsook, op verzoek, van de door haar verleende goedkeuringen voor kwaliteitssystemen.

8. Gemachtigde vertegenwoordiger

De in de punten 3.1, 3.5, 5 en 6 vervatte verplichtingen van de fabrikant kunnen namens en onder de verantwoordelijkheid van de fabrikant worden vervuld door de gemachtigde vertegenwoordiger van de fabrikant, op voorwaarde dat de relevante verplichtingen in het mandaat gespecificeerd zijn.

Met betrekking tot deze verordening werd een verklaring afgelegd; die verklaring kan geraadpleegd worden in PB C, 2024/6786, 20.11.2024 en via de volgende link: ELI: http://data.europa.eu/eli/C/2024/6786/oj.