EUROPEISKA UNIONEN

EUROPAPARLAMENTET **RÅDET**

Strasbourg den 23 oktober 2024
(OR. en)

2022/0272(COD)
LEX 2395

PE-CONS 100/1/23
REV 1

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM ÖVERGRIPANDE CYBERSÄKERHETSKRAV FÖR PRODUKTER MED DIGITALA ELEMENT OCH OM ÄNDRING AV FÖRORDNINGARNA (EU) Nr 168/2013 OCH (EU) 2019/1020 OCH DIREKTIV (EU) 2020/1828 (CYBERRESILIENSFÖRORDNINGEN)

EUROPAPARLAMENTETS OCH RÅDETS
FÖRORDNING (EU) 2024/…

av den 23 oktober 2024

om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[1],

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet[2], och

---

1 EUT C 100, 16.3.2023, s. 101.

2 Europaparlamentets ståndpunkt av den 12 mars 2024 (ännu inte offentliggjord i EUT) och rådets beslut av den 10 oktober 2024.

av följande skäl:

(1) Cybersäkerhet är en av de största utmaningarna för unionen. Antalet och mångfalden av uppkopplade enheter kommer att öka exponentiellt under de kommande åren. Cyberattacker är en fråga av allmänintresse eftersom de har en avgörande inverkan inte bara på unionens ekonomi utan även på demokratin liksom på konsumenternas säkerhet och hälsa. Det är därför nödvändigt att stärka unionens strategi när det gäller cybersäkerhet, ta upp frågan om cyberresiliens på unionsnivå och förbättra den inre marknadens funktionssätt genom att fastställa en enhetlig rättslig ram för väsentliga cybersäkerhetskrav för utsläppande av produkter med digitala element på marknaden i unionen. Två stora problem som ökar kostnaderna för användarna och samhället bör lösas: en låg cybersäkerhetsnivå för produkter med digitala element, vilket visas av utbredda sårbarheter och ett otillräckligt och inkonsekvent tillhandahållande av säkerhetsuppdateringar för att åtgärda dessa sårbarheter, samt användarnas bristfälliga förståelse och tillgång till information, vilket hindrar dem från att välja produkter med tillräckliga cybersäkerhetsfunktioner eller att använda dem på ett säkert sätt.

(2) Denna förordning syftar till att fastställa randvillkor för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter som släpps ut på marknaden har färre sårbarheter och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Den syftar också till att skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element, exempelvis genom att öka transparensen när det gäller stödperioden för produkter med digitala element som släpps ut på marknaden.

(3) Den relevanta unionsrätt som för närvarande gäller omfattar flera uppsättningar övergripande regler som behandlar vissa aspekter av cybersäkerheten från olika synvinklar, inbegripet åtgärder för att förbättra säkerheten i den digitala leveranskedjan. Den befintliga unionsrätten om cybersäkerhet, inbegripet Europaparlamentets och rådets förordning (EU) 2019/881[3] och Europaparlamentets och rådets direktiv (EU) 2022/2555[4] täcker inte på ett direkt sätt obligatoriska krav avseende säkerheten för produkter med digitala element.

---

[3] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

[4] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

(4) Den befintliga unionsrätten är visserligen tillämplig på vissa produkter med digitala element, men det finns inget övergripande unionsregelverk med övergripande cybersäkerhetskrav för alla produkter med digitala element. De olika rättsakter och initiativ som hittills har vidtagits på unionsnivå och nationell nivå åtgärdar endast delvis de identifierade cybersäkerhetsrelaterade problemen och riskerna, vilket ger upphov till ett lapptäcke av lagar på den inre marknaden som ökar rättsosäkerheten för både tillverkare och användare av dessa produkter och innebär att det blir onödigt betungande för företag och organisationer som måste uppfylla många olika krav och skyldigheter för samma typer av produkter. Cybersäkerheten för dessa produkter har en särskilt stark gränsöverskridande dimension, eftersom produkter med digitala element som tillverkas i en medlemsstat eller ett tredjeland ofta används av organisationer och konsumenter på hela den inre marknaden. Därmed är det nödvändigt att reglera detta område på unionsnivå för att säkerställa ett harmoniserat regelverk och rättssäkerhet för användare, organisationer och företag, inbegripet mikroföretag och små och medelstora företag enligt definitionen i bilagan till kommissionens rekommendation 2003/361/EG[5]. Unionens regelverk bör harmoniseras genom ett införande av övergripande cybersäkerhetskrav för produkter med digitala element. Rättslig förutsebarhet för ekonomiska aktörer och användare liksom harmoniseringen på den inre marknaden och proportionaliteten för mikroföretag samt små och medelstora företag, vilket skapar hållbarare villkor för ekonomiska operatörer som vill komma in på den marknaden bör säkerställas i hela unionen.

[5] Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

(5) När det gäller mikroföretag och små och medelstora företag bör bestämmelserna i bilagan till rekommendation 2003/361/EG tillämpas i sin helhet vid fastställandet av vilken kategori ett företag omfattas av. Vid beräkningen av personalstyrkan och de finansiella taken för att fastställa företagskategorierna bör därför bestämmelserna i artikel 6 i bilagan till rekommendation 2003/361/EG om fastställande av uppgifter för ett företag med hänsyn till särskilda typer av företag, såsom partnerföretag eller anknutna företag, också tillämpas.

(6) Kommissionen bör ge vägledning för att hjälpa ekonomiska aktörer, särskilt mikroföretag och små och medelstora företag, vid tillämpningen av denna förordning. Sådan vägledning bör bland annat omfatta denna förordnings tillämpningsområde, särskilt distansbehandling av data och dess konsekvenser för utvecklare av programvara med fri och öppen källkod, tillämpningen av de kriterier som används för att fastställa stödperioder för produkter med digitala element, samspelet mellan denna förordning och annan unionsrätt och begreppet väsentlig ändring.

(7) På unionsnivå har särskilda EU-cybersäkerhetskrav efterlysts för digitala eller uppkopplade produkter med digitala element, exempelvis det gemensamma meddelandet från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik av den 16 december 2020 med titeln *EU:s strategi för cybersäkerhet för ett digitalt decennium*, rådets slutsatser av den 2 december 2020 om cybersäkerhet för uppkopplade enheter och av den 23 maj 2022 om utvecklingen av Europeiska unionens arbete på cyberområdet och Europaparlamentets resolution av den 10 juni 2021 om EU:s strategi för cybersäkerhet för ett digitalt decennium[6], och flera tredjeländer håller på att vidta åtgärder för att åtgärda denna fråga på eget initiativ. I slutrapporten från konferensen om Europas framtid efterlyste medborgarna ”En starkare roll för EU när det gäller att motverka cybersäkerhetshot”. För att unionen ska kunna spela en ledande internationell roll på cybersäkerhetsområdet är det viktigt att utarbeta ett ambitiöst regelverk.

(8) För att höja den allmänna cybersäkerhetsnivån för alla produkter med digitala element som släpps ut på den inre marknaden är det nödvändigt att införa målinriktade och teknikneutrala väsentliga cybersäkerhetskrav för dessa produkter vilka ska tillämpas övergripande.

[6] EUT C 67, 8.2.2022, s. 81.

(9) Under vissa omständigheter kan alla produkter med digitala element vilka är integrerade i eller anslutna till ett större elektroniskt informationssystem fungera som en attackvektor för fientliga aktörer. Det innebär att även hårdvara eller programvara som anses vara mindre kritisk kan underlätta en inledande kompromettering av en enhet eller ett nät, vilket gör det möjligt för fientliga aktörer att få priviligierad åtkomst till ett system eller att röra sig lateralt mellan system. Tillverkarna bör därför säkerställa att alla produkter med digitala element utformas och utvecklas i enlighet med de väsentliga cybersäkerhetskrav som fastställs i denna förordning. Denna skyldighet avser både produkter som kan anslutas fysiskt via hårdvarugränssnitt och produkter som ansluts logiskt, t.ex. via nätanslutningsuttag, rör, filer, programmeringsgränssnitt eller andra typer av programvarugränssnitt. I och med att cyberhot kan spridas via olika produkter med digitala element tills de når ett visst mål, exempelvis genom att sammanlänka flera olika attacker mot sårbarheter, bör tillverkarna också säkerställa cybersäkerheten för produkter som endast indirekt ansluts till andra enheter eller nät.

(10) Genom att cybersäkerhetskrav fastställs för utsläppandet på marknaden av produkter med digitala element är syftet att dessa produkters cybersäkerhet ska förbättras för både konsumenter och företag. Dessa krav kommer också att säkerställa att cybersäkerhet tas i beaktande genom leveranskedjorna som helhet, för att göra slutprodukterna med digitala element och deras komponenter säkrare. Detta innefattar krav för utsläppandet på marknaden av konsumentprodukter med digitala element vilka är avsedda för sårbara konsumenter, exempelvis leksaker och babyövervakningssystem. Konsumentprodukter med digitala element som i denna förordning kategoriseras som viktiga produkter med digitala element utgör en högre cybersäkerhetsrisk genom att de utför en funktion som medför en betydande risk för negativa effekter i fråga om intensitet och förmåga att skada hälsan, tryggheten eller säkerheten för användarna av sådana produkter, och bör genomgå ett striktare förfarande för bedömning av överensstämmelse. Detta är tillämpligt på sådana produkter som smarta hemprodukter med säkerhetsfunktioner, inbegripet smarta dörrlås, babyövervakningssystem och larmsystem, uppkopplade leksaker och kroppsburen medicinsk teknik. De striktare förfaranden för bedömning av överensstämmelse som andra produkter med digitala element som i denna förordning kategoriseras som viktiga eller kritiska produkter med digitala element måste genomgå kommer dessutom att bidra till att förhindra att konsumenterna kan komma att påverkas negativt av utnyttjandet av sårbarheter.

(11) Syftet med denna förordning är att säkerställa en hög cybersäkerhetsnivå för produkter med digitala element och deras integrerade lösningar för fjärrbehandling av data. Sådana lösningar för fjärrbehandling av data bör definieras som all databehandling på distans för vilken programvaran har utformats och utvecklats av tillverkaren av den berörda produkten med digitala element eller för dennes räkning, och vars avsaknad skulle innebära att produkten med digitala element inte skulle kunna utföra en av sina grundläggande funktioner. Detta tillvägagångssätt säkerställer att tillverkarna på lämpligt sätt säkrar sådana produkter i sin helhet, oavsett om uppgifterna behandlas eller lagras lokalt på användarens enhet eller på distans av tillverkaren. Samtidigt omfattas fjärrbehandling eller fjärrlagring av denna förordnings tillämpningsområde endast i den mån det är nödvändigt för att en produkt med digitala element ska kunna utföra sina funktioner. Sådan fjärrbehandling eller fjärrlagring omfattar situationer där en mobilapplikation kräver tillgång till ett programmeringsgränssnitt eller en databas som tillhandahålls genom en tjänst som utvecklats av tillverkaren. I ett sådant fall omfattas tjänsten av denna förordnings tillämpningsområde som en lösning för fjärrbehandling av uppgifter. Kraven på lösningar för fjärrdatabehandling som omfattas av denna förordning innebär därför inte några tekniska, operativa eller organisatoriska åtgärder som syftar till att hantera riskerna för säkerheten i en tillverkares nätverks- och informationssystem som helhet.

(12) Molnlösningar utgör lösningar för fjärrdatabehandling i den mening som avses i denna förordning endast om de uppfyller definitionen som fastställs i denna förordning. Till exempel omfattar denna förordning molnaktiverade funktioner som tillhandahålls av en tillverkare av enheter för smarta hem som gör det möjligt för användare att fjärrkontrollera enheten. Å andra sidan omfattas webbplatser som inte stöder funktionen hos en produkt med digitala element, eller molntjänster som utformats och utvecklats utanför en tillverkares ansvar för en produkt med digitala element, inte av denna förordnings tillämpningsområde. Direktiv (EU) 2022/2555 är tillämpligt på molntjänster och molntjänstmodeller, som Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) eller Infrastructure-as-a-Service (IaaS). Entiteter som tillhandahåller molntjänster i unionen och som räknas som medelstora företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG, eller överskrider de tak för medelstora företag som anges i punkt 1 i den artikeln, omfattas av det direktivets tillämpningsområde.

(13) I linje med målet för denna förordning, som är att avlägsna hinder för den fria rörligheten för produkter med digitala element, får medlemsstaterna inte, med hänvisning till aspekter som omfattas av denna förordning, hindra att produkter med digitala element som uppfyller kraven i denna förordning tillhandahålls på marknaden. I frågor som harmoniseras genom denna förordning kan medlemsstaterna därför inte införa ytterligare cybersäkerhetskrav för tillhandahållande på marknaden av produkter med digitala element. Varje entitet, offentlig eller privat, kan dock fastställa ytterligare krav utöver dem som fastställs i denna förordning för upphandling eller användning av produkter med digitala element för sina specifika ändamål, och kan därför välja att använda produkter med digitala element som uppfyller strängare eller mer specifika cybersäkerhetskrav än de som är tillämpliga för tillhandahållande på marknaden enligt denna förordning. Utan att det påverkar tillämpningen av Europaparlamentets och rådets direktiv 2014/24/EU[7] och 2014/25/EU[8] bör medlemsstaterna, vid upphandling av produkter med digitala element som måste uppfylla de väsentliga cybersäkerhetskrav som fastställs i denna förordning, inbegripet de som rör sårbarhetshantering, säkerställa att sådana krav beaktas i upphandlingsprocessen och att tillverkarnas förmåga att effektivt tillämpa cybersäkerhetsåtgärder och hantera cyberhot också beaktas.

---

[7] Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65).

[8] Europaparlamentets och rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG (EUT L 94, 28.3.2014, s. 243).

I direktiv (EU) 2022/2555 fastställs dessutom riskhanteringsåtgärder för cybersäkerhet för de väsentliga och viktiga entiteter som avses i artikel 3 i det direktivet som kan medföra säkerhetsåtgärder i leveranskedjan som kräver att sådana entiteter använder produkter med digitala element som uppfyller strängare cybersäkerhetskrav än de som fastställs i denna förordning. I enlighet med direktiv (EU) 2022/2555 och i linje med dess princip om minimiharmonisering kan medlemsstaterna därför införa ytterligare cybersäkerhetskrav för väsentliga eller viktiga entiteters användning av produkter för informations- och kommunikationsteknik (IKT) enligt det direktivet för att säkerställa en högre cybersäkerhetsnivå, förutsatt att sådana krav är förenliga med medlemsstaternas skyldigheter enligt unionsrätten. Frågor som inte omfattas av denna förordning kan omfatta icke-tekniska faktorer som rör produkter med digitala element och deras tillverkare. Medlemsstaterna kan därför fastställa nationella åtgärder, inbegripet begränsningar för produkter med digitala element eller leverantörer av sådana produkter, som tar hänsyn till icke-tekniska faktorer. Nationella åtgärder som rör sådana faktorer måste vara förenliga med unionsrätten.

(14) Denna förordning bör inte påverka medlemsstaternas ansvar att skydda den nationella säkerheten, i enlighet med unionsrätten. Medlemsstaterna bör kunna låta produkter med digitala element som är upphandlade eller används för ändamål som rör nationell säkerhet- eller försvar omfattas av ytterligare åtgärder, förutsatt att sådana åtgärder är förenliga med medlemsstaternas skyldigheter enligt unionsrätten.

(15) Denna förordning är tillämplig på ekonomiska aktörer endast med avseende på produkter med digitala element som tillhandahålls på marknaden och därmed levereras för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet. Tillhandahållande inom ramen för en kommersiell verksamhet kan kännetecknas inte bara av att det tas ut en avgift för en produkt med digitala element utan också av att en avgift tas ut för tekniska stödtjänster när detta inte enbart tjänar till att täcka faktiska kostnader, när syftet är att monetarisera, till exempel genom att tillhandahålla en programvaruplattform som tillverkaren använder för att monetarisera andra tjänster, genom att som ett villkor för användning kräva behandling av personuppgifter för andra syften än uteslutande för att förbättra programvarans säkerhet, kompatibilitet eller interoperabilitet, eller genom att ta emot donationer som överstiger kostnaderna för utformning, utveckling och tillhandahållande av en produkt med digitala element. Att ta emot donationer utan avsikt att göra vinst bör inte betraktas som en kommersiell verksamhet.

(16) Produkter med digitala element som tillhandahålls som en del av tillhandahållandet av en tjänst för vilka en avgift tas ut enbart för att täcka de faktiska kostnader som är direkt kopplade till driften av den tjänsten, såsom kan vara fallet med vissa produkter med digitala element som tillhandahålls av enheter inom offentlig förvaltning, bör inte i sig anses utgöra kommersiell verksamhet vid tillämpningen av denna förordning. Dessutom bör produkter med digitala element som utvecklas eller ändras av en offentlig förvaltningsentitet uteslutande för dess eget bruk inte anses vara tillgängliggjord på marknaden i den mening som avses i denna förordning.

(17) Programvara och data som delas öppet och som användarna fritt kan komma åt, använda, modifiera och redistribuera, eller modifierade versioner av dem, kan bidra till forskning och innovation på marknaden. För att främja utvecklingen och spridningen av programvara med fri och öppen källkod, särskilt av mikroföretag och små och medelstora företag, inbegripet uppstartsföretag, enskilda personer, ideella organisationer och akademiska forskningsorganisationer, bör tillämpningen av denna förordning på produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som tillhandahålls för distribution eller användning i samband med kommersiell verksamhet ta hänsyn till de olika utvecklingsmodellerna för programvara som distribueras och utvecklas inom ramen för licenser för programvara med fri och öppen källkod.

(18) Med programvara med fri och öppen källkod avses programvara vars källkod delas öppet och vars licensiering ger alla rättigheter att göra den fritt tillgänglig, samt möjlig att använda, ändra och omfördela. Programvara med fri och öppen källkod utvecklas, underhålls och distribueras öppet, inbegripet via onlineplattformar. När det gäller ekonomiska aktörer som omfattas av denna förordning bör endast programvara med fri och öppen källkod som tillhandahålls på marknaden och som därför levereras för distribution eller användning i samband med kommersiell verksamhet omfattas av denna förordnings tillämpningsområde. De omständigheter under vilka produkten med digitala element har utvecklats, eller hur utvecklingen har finansierats, bör inte beaktas vid fastställandet av huruvida denna verksamhet är av kommersiell eller icke-kommersiell karaktär. Mer specifikt bör tillhandahållandet av produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som inte monetariseras av deras tillverkare inte betraktas vara en kommersiell verksamhet vid tillämpningen av denna förordning och för de ekonomiska aktörer som omfattas av dess tillämpningsområde, för att säkerställa en tydlig åtskillnad mellan utvecklings- och leveransfaserna. Dessutom bör tillhandahållande av produkter med digitala element som klassificeras som komponenter för programvara med fri och öppen källkod och som är avsedda att integreras av andra tillverkare i deras egna produkter med digitala element betraktas som tillhandahållande på marknaden endast om komponenten monetariseras av dess ursprungliga tillverkare. Till exempel bör enbart det faktum att en programvaruprodukt med fri och öppen källkod med digitala element får ekonomiskt stöd från tillverkare, eller att tillverkarna bidrar till utvecklingen av en sådan produkt, inte i sig fastställa att verksamheten är av kommersiell karaktär.

Dessutom bör själva det faktum att en produkt regelbundet släpps ut inte i sig leda till slutsatsen att en produkt med digitala element tillhandahålls inom ramen för kommersiell verksamhet. Slutligen bör utveckling av produkter med digitala element som betraktas som programvara med fri och öppen källkod av ideella organisationer inte betraktas som kommersiell verksamhet vid tillämpningen av denna förordning, förutsatt att organisationen är inrättad på ett sätt som säkerställer att alla intäkter efter kostnader används för att uppnå icke-vinstdrivande mål. Denna förordning är inte tillämplig på fysiska eller juridiska personer som bidrar med källkod till produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som inte omfattas av deras ansvar.

(19) Med tanke på hur viktigt det är för cybersäkerheten hos många produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som offentliggörs men inte tillhandahålls på marknaden i den mening som avses i denna förordning, bör juridiska personer som ger varaktigt stöd för utvecklingen av sådana produkter som är avsedda för kommersiell verksamhet och som spelar en viktig roll för att säkerställa dessa produkters bärkraft (förvaltare av programvara med fri och öppen källkod) omfattas av ett förenklat och skräddarsytt regelverk. Förvaltare av programvara med fri och öppen källkod omfattar vissa stiftelser samt enheter som utvecklar och publicerar programvara med fri och öppen källkod i ett affärssammanhang, inbegripet icke-vinstdrivande enheter programvara med fri och öppen källkod. Regelverket bör ta hänsyn till deras särskilda karaktär och förenlighet med den typ av skyldigheter som införs. Det bör endast omfatta produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som i slutändan är avsedda för kommersiell verksamhet, såsom integrering i kommersiella tjänster eller i monetariserade produkter med digitala element. Vid tillämpningen av det regelverket omfattar en avsikt om integrering i monetariserade produkter med digitala element fall där tillverkare som integrerar en komponent i sina egna produkter med digitala element antingen bidrar till utvecklingen av den komponenten på ett regelbundet sätt eller tillhandahåller regelbundet ekonomiskt stöd för att säkerställa en programvaruprodukts kontinuitet. Tillhandahållandet av varaktigt stöd till utvecklingen av en produkt med digitala element omfattar, men är inte begränsat till, hysande och förvaltning av samarbetsplattformar för programvaruutveckling, hysande av källkod eller programvara, styrning eller förvaltning av produkter med digitala element som klassificeras som fri och öppen programvara med fri och öppen källkod samt styrning av utvecklingen av sådana produkter. Eftersom det förenklade och skräddarsydda regelverket inte ålägger dem som agerar som förvaltare av programvara med fri och öppen källkod samma skyldigheter som dem som agerar som tillverkare enligt denna förordning, bör de inte ha rätt att fästa CE-märkningen på produkter med digitala element vars utveckling de stöder.

(20) Enbart hysande av produkter med digitala element i öppna databaser, inbegripet genom paketförvaltare eller på samarbetsplattformar, utgör inte i sig tillhandahållande på marknaden av en produkt med digitala element. Leverantörer av sådana tjänster bör betraktas vara distributörer endast om de tillhandahåller sådan programvara på marknaden och därmed tillhandahåller den för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet.

(21) För att stödja och underlätta tillbörlig aktsamhet hos tillverkare som i sina produkter med digitala element integrerar komponenter för programvara med fri och öppen källkod som inte omfattas av de väsentliga cybersäkerhetskrav som fastställs i denna förordning bör kommissionen kunna inrätta frivilliga program för säkerhetsintyg, antingen genom en delegerad akt som kompletterar denna förordning eller genom att enligt artikel 48 i förordning (EU) 2019/881 begära en europeisk ordning för cybersäkerhetscertifiering som tar hänsyn till särdragen hos utvecklingsmodellerna för programvara med fri och öppen källkod. Programmen för säkerhetsintyg bör utformas på ett sådant sätt att inte bara fysiska eller juridiska personer som utvecklar eller bidrar till utvecklingen av en produkt med digitala element som klassificeras som programvara med fri och öppen källkod kan initiera eller finansiera ett säkerhetsintyg, utan även tredje parter, såsom tillverkare som integrerar sådana produkter i sina egna produkter med digitala element, användare eller offentliga förvaltningar på unionsnivå och nationell nivå.

(22) Med tanke på målen för offentlig cybersäkerhet i denna förordning och för att förbättra medlemsstaternas situationsmedvetenhet när det gäller unionens beroende av programvarukomponenter, särskilt av komponenter för potentiell programvara med fri och öppen källkod, bör en särskild administrativ samarbetsgrupp (Adco-grupp) som inrättas genom denna förordning kunna besluta att gemensamt genomföra en beroendebedömning på unionsnivå. Marknadskontrollmyndigheterna bör kunna begära att tillverkare av kategorier av produkter med digitala element som inrättats av Adco-gruppen lämnar in de mjukvaruförteckningar som de har framställt enligt denna förordning. För att skydda sekretessen för mjukvaruförteckningar bör marknadskontrollmyndigheterna lämna relevant information om beroendeförhållanden till Adco-gruppen på ett anonymiserat och aggregerat sätt.

(23) Effektiviteten i genomförandet av denna förordning kommer också att vara beroende av tillgången till lämpliga cybersäkerhetskunskaper. På unionsnivå konstaterades i olika programdokument och politiska dokument, inbegripet kommissionens meddelande *Minska kompetensbristen på cybersäkerhetsområdet för att främja EU:s konkurrenskraft, tillväxt och resiliens* av den 18 april 2023 och rådets slutsatser av den 22 maj 2023 om EU:s politik för cyberförsvar, kompetensbristen inom cybersäkerhet i unionen och behovet av att ta itu med sådana utmaningar som en prioriterad fråga, både inom den offentliga och den privata sektorn. För att säkerställa ett effektivt genomförande av denna förordning bör medlemsstaterna se till att tillräckliga resurser finns tillgängliga för lämplig personal vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse för att de ska kunna utföra sina uppgifter enligt denna förordning. Dessa åtgärder bör öka arbetskraftens rörlighet på cybersäkerhetsområdet och deras tillhörande karriärvägar. De bör också bidra till att göra cybersäkerhetsarbetskraften mer resilient och inkluderande, även när det gäller kön. Medlemsstaterna bör därför vidta åtgärder för att säkerställa att dessa uppgifter utförs av tillräckligt utbildade yrkesutövare med nödvändig cybersäkerhetskompetens. På samma sätt bör tillverkarna se till att deras personal har den kompetens som krävs för att fullgöra sina skyldigheter som fastställs i denna förordning. Medlemsstaterna och kommissionen bör, i enlighet med sina rättigheter och befogenheter och de särskilda uppgifter som de tilldelas genom denna förordning, vidta åtgärder för att stödja tillverkare, särskilt mikroföretag och små och medelstora företag, inbegripet uppstartsföretag, även på områden såsom kompetensutveckling, i syfte att fullgöra de skyldigheter som fastställs i denna förordning. Eftersom direktiv (EU) 2022/2555 ålägger medlemsstaterna att anta strategier för att främja och utveckla utbildning i cybersäkerhet och cybersäkerhetskompetens som en del av sina nationella strategier för cybersäkerhet, får medlemsstaterna, när de antar sådana strategier, också överväga om de ska ta itu med de kompetensbehov inom cybersäkerhet som följer av denna förordning, inbegripet sådana som rör omskolning och kompetenshöjning.

(24) Ett säkert internet är avgörande för att kritiska infrastrukturer och samhället som helhet ska kunna fungera. Direktiv (EU) 2022/2555 syftar till att säkerställa en hög cybersäkerhetsnivå för tjänster som tillhandahålls av väsentliga och viktiga entiteter som avses i artikel 3 i det direktivet, inbegripet leverantörer av digital infrastruktur som stöder kärnfunktioner för ett öppet internet eller säkerställer internetåtkomst och tillhandahåller internettjänster. Det är därför viktigt att de produkter med digitala element som behövs för att leverantörer av digital infrastruktur ska kunna säkerställa ett fungerande internet utvecklas på ett säkert sätt och att de uppfyller väletablerade internetsäkerhetsstandarder. Denna förordning, som är tillämplig på alla uppkopplingsbara hårdvaru- och programvaruprodukter, syftar också till att främja att leverantörer av digital infrastruktur uppfyller leveranskedjekraven enligt direktiv (EU) 2022/2555 genom att säkerställa att de produkter med digitala element som de använder för tillhandahållandet av sina tjänster utvecklas på ett säkert sätt och att de har tillgång till säkerhetsuppdateringar i rätt tid för sådana produkter.

(25) I Europaparlamentets och rådets förordning (EU) 2017/745[9] fastställs regler om medicintekniska produkter och i Europaparlamentets och rådets förordning (EU) 2017/746[10] fastställs regler om medicintekniska produkter för in vitro-diagnostik. De förordningarna behandlar cybersäkerhetsrisker enligt särskilda tillvägagångssätt som också behandlas i den här förordningen. Närmare bestämt fastställs i förordningarna (EU) 2017/745 och (EU) 2017/746 väsentliga krav för medicintekniska produkter som fungerar genom ett elektroniskt system eller som själva utgörs av programvara. Viss icke-inbyggd programvara och ett livscykelperspektiv täcks också av dessa förordningar. Dessa krav innebär att tillverkarna ska utveckla och bygga sina produkter genom att tillämpa riskhanteringsprinciper och genom att fastställa krav på it-säkerhetsåtgärder, samt motsvarande förfaranden för bedömning av överensstämmelse. Vidare finns det sedan december 2019 särskilda riktlinjer för cybersäkerheten för medicintekniska produkter, som ger tillverkarna av medicintekniska produkter, däribland för in vitro-diagnostik, vägledning för hur alla berörda väsentliga krav som anges i bilaga I till dessa förordningar ska uppfyllas när det gäller cybersäkerhet. Produkter med digitala element på vilka någon av dessa förordningar är tillämpliga bör därför inte omfattas av den här förordningen.

---

[9] Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1).

[10] Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176).

(26) Produkter med digitala element som utvecklas eller ändras uteslutande för ändamål som rör nationell säkerhet eller försvar eller produkter som är särskilt utformade för att behandla säkerhetsskyddsklassificerade uppgifter omfattas inte av denna förordnings tillämpningsområde. Medlemsstaterna uppmanas att säkerställa samma eller en högre skyddsnivå för dessa produkter som för de produkter som omfattas av denna förordnings tillämpningsområde.

(27) Genom Europaparlamentets och rådets förordning (EU) 2019/2144[11] fastställs krav för typgodkännande av fordon och deras system och komponenter, som innebär att vissa cybersäkerhetskrav införs, inbegripet när det gäller användning av ett certifierat ledningssystem för cybersäkerhet och uppdateringar av programvara, som täcker organisationers policyer och processer för cybersäkerhetsrisker under hela livscykeln för fordon, utrustning och tjänster i enlighet med tillämpliga Förenta nationernas (FN) föreskrifter om tekniska specifikationer och cybersäkerhet, i synnerhet FN-föreskrift nr 155 – Enhetliga bestämmelser om godkännande av fordon med avseende på cybersäkerhet och ledningssystem för cybersäkerhet[12], och föreskrivs särskilda förfaranden för bedömning av överensstämmelse.

---

[11] Europaparlamentets och rådets förordning (EU) 2019/2144 av den 27 november 2019 om krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, med avseende på deras allmänna säkerhet och skydd för personer i fordonet och oskyddade trafikanter, om ändring av Europaparlamentets och rådets förordning (EU) 2018/858 och om upphävande av Europaparlamentets och rådets förordningar (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 samt kommissionens förordningar (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 och (EU) 2015/166 (EUT L 325, 16.12.2019, s. 1).

[12] EUT L 82, 9.3.2021, s. 30.

På luftfartsområdet är huvudsyftet för Europaparlamentets och rådets förordning (EU) 2018/1139[13] att fastställa och upprätthålla en hög och enhetlig säkerhetsnivå inom den civila luftfarten i unionen. Förordningen ger en ram för väsentliga krav på luftvärdighet för luftfartsprodukter, delar och utrustning, inbegripet programvara som inbegriper skyldigheten att skydda sig mot informationssäkerhetshot. Certifieringsförfarandena enligt förordning (EU) 2018/1139 säkerställer den assuransnivå som eftersträvas i den här förordningen. Produkter med digitala element som omfattas av förordning (EU) 2019/2144 och produkter som certifierats i enlighet med förordning (EU) 2018/1139 bör därför inte omfattas av de väsentliga cybersäkerhetskrav och förfaranden för bedömning av överensstämmelse som fastställs i den här förordningen.

[13] Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (EUT L 212, 22.8.2018, s. 1).

(28) Genom denna förordning fastställs övergripande cybersäkerhetsregler som inte är sektorsspecifika eller specifika för vissa produkter med digitala element. Sektors- eller produktspecifika unionsregler kan dock införas, med krav som omfattar alla eller vissa risker som täcks av de väsentliga cybersäkerhetskraven enligt denna förordning. I sådana fall får tillämpningen av denna förordning på sådana produkter med digitala element som omfattas av andra unionsregler, där krav fastställs avseende alla eller vissa risker som täcks av de väsentliga cybersäkerhetskrav som anges i denna förordning, begränsas eller uteslutas när en begränsning eller ett uteslutande är förenligt med den allmänna rättsliga ram som är tillämplig på dessa produkter och när sektorsreglerna ger minst samma skyddsnivå som denna förordning. Kommissionen bör ges befogenhet att anta delegerade akter för att komplettera denna förordning genom att identifiera sådana produkter och regler. För befintlig unionsrätt på vilken denna typ av begränsning eller uteslutande bör tillämpas, omfattar denna förordning särskilda bestämmelser som klargör dess förhållande till den unionsrätten.

(29) För att säkerställa att produkter med digitala element som tillhandahålls på marknaden kan repareras ändamålsenligt och deras hållbarhet förlängas bör ett undantag göras för reservdelar. Undantaget bör omfatta både reservdelar som har till syfte att reparera befintliga produkter som tillhandahålls före den dag då denna förordning börjar tillämpas och reservdelar som redan har genomgått ett förfarande för bedömning av överensstämmelse enligt denna förordning.

(30) I kommissionens delegerade förordning (EU) 2022/30[14] anges att ett antal väsentliga krav som anges i artikel 3.3 d, e och f i Europaparlamentets och rådets direktiv 2014/53/EU[15] avseende skada på nät och missbruk av nätresurser, personuppgifter och integritet samt bedrägeri ska tillämpas på viss radioutrustning. I kommissionens genomförandebeslut C(2022) 5637 av den 5 augusti 2022 om en standardiseringsbegäran till Europeiska standardiseringskommittén och Europeiska kommittén för elektroteknisk standardisering fastställs krav för utarbetandet av särskilda standarder som ytterligare specificerar hur de tre väsentliga kraven bör hanteras. De väsentliga cybersäkerhetskrav som anges i denna förordning omfattar alla aspekter av de väsentliga krav som avses i artikel 3.3 d, e och f i direktiv 2014/53/EU. De väsentliga cybersäkerhetskrav som anges i denna förordning är dessutom anpassade till syftena för kraven på särskilda standarder som omfattas av den standardiseringsbegäran. När kommissionen upphäver eller ändrar delegerad förordning (EU) 2022/30 med följden att den upphör att gälla för vissa produkter som omfattas av denna förordning, bör kommissionen och de europeiska standardiseringsorganisationerna, i samband med förberedelserna och utarbetandet av harmoniserade standarder för att underlätta genomförandet av denna förordning, ta hänsyn till det standardiseringsarbete som utförts inom ramen för genomförandebeslut C(2022)5637. Under övergångsperioden för tillämpningen av den här förordningen bör kommissionen ge vägledning till tillverkare som omfattas av den här förordningen och som också omfattas av delegerad förordning (EU) 2022/30 för att underlätta påvisandet av efterlevnaden av de båda förordningarna.

---

[14] Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet (EUT L 7, 12.1.2022, s. 6).

[15] Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG (EUT L 153, 22.5.2014, s. 62).

(31) Europaparlamentets och rådets direktiv (EU) 2024/…[16+] kompletterar denna förordning. Genom det direktivet fastställs skadeståndsansvar för produkter med säkerhetsbrister så att skadelidande kan kräva ersättning när en skada har orsakats av produkter med säkerhetsbrister. Där fastställs principen att tillverkaren av en produkt har skadeståndsansvaret för skador som orsakats av säkerhetsbrister i produkten oavsett om tillverkaren agerat oaktsamt (strikt ansvar). När sådana säkerhetsbrister består av en brist på säkerhetsuppdateringar efter att produkten släppts ut på marknaden och detta orsakar skada kan tillverkarens skadeståndsansvar utlösas. Tillverkarnas skyldigheter avseende tillhandahållandet av sådana säkerhetsuppdateringar bör fastställas i denna förordning.

---

[16] Europaparlamentets och rådets direktiv (EU) 2024/...om skadeståndsansvar för produkter med säkerhetsbrister och om upphävande av rådets direktiv 85/374/EEG (EUT L ..., ELI: ...)

[+] EUT: Vänligen för in nummer på det direktiv som finns i dokument PE-CONS 7/24 (2022/0302(COD)) i texten och för in nummer, datum och EUT-hänvisning avseende det direktivet i fotnoten.

(32) Denna förordning bör inte påverka tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679[17], inbegripet när det gäller bestämmelser om inrättandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas och personuppgiftsbiträdens databehandling uppfyller kraven i den förordningen. Sådan behandling kan vara inbyggd i en produkt med digitala element. Inbyggt dataskydd och dataskydd som standard samt allmän cybersäkerhet är viktiga aspekter av förordning (EU) 2016/679. Genom att skydda konsumenter och organisationer från cybersäkerhetsrisker bidrar de väsentliga cybersäkerhetskrav som fastställs i den här förordningen till att förbättra skyddet av personuppgifter och individers personliga integritet. När det gäller både standardiseringen och certifieringen av cybersäkerhetsaspekter bör synergier övervägas genom samarbete mellan kommissionen, europeiska standardiseringsorganisationer, Europeiska unionens cybersäkerhetsbyrå (Enisa), Europeiska dataskyddsstyrelsen, som inrättats genom förordning (EU) 2016/679, och de nationella tillsynsmyndigheterna med ansvar för dataskydd. Synergier mellan den här förordningen och unionens dataskyddsrätt bör också skapas på områdena marknadskontroll och kontroll av efterlevnaden. Därför bör de nationella marknadskontrollmyndigheter som utses enligt den här förordningen samarbeta med de myndigheter som utövar tillsyn över tillämpningen av unionens dataskyddsrätt. De sistnämnda bör också ha tillgång till information av relevans för utförandet av deras uppgifter.

---

[17] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

(33) I den mån deras produkter omfattas av denna förordning bör leverantörer av europeiska digitala identitetsplånböcker som avses i artikel 5a.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014[18] uppfylla både de övergripande väsentliga cybersäkerhetskrav som fastställs i den här förordningen och de särskilda säkerhetskrav som fastställs i artikel 5a i förordning (EU) nr 910/2014. För att främja efterlevnad bör de leverantörerna kunna visa att europeiska digitala identitetsplånböcker uppfyller de krav som fastställs i den här förordningen och i förordning (EU) nr 910/2014 genom att låta certifiera sina produkter inom en europeisk ordning för cybersäkerhetscertifiering som inrättas inom ramen för förordning (EU) 2019/881 och för vilket kommissionen genom delegerade akter har specificerat en presumtion om överensstämmelse med den här förordningen, i den mån som certifikatet, eller delar av detta, täcker dessa krav.

[18] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

(34) Vid integrering av komponenter från tredje parter i produkter med digitala element under utformnings- och utvecklingsfasen bör tillverkarna, för att säkerställa att produkterna utformas, utvecklas och tillverkas i enlighet med de väsentliga cybersäkerhetskrav som fastställs i denna förordning, iaktta tillbörlig aktsamhet med avseende på dessa komponenter, inbegripet komponenter av programvara med fri och öppen källkod som inte har tillhandahållits på marknaden. Den lämpliga nivån på tillbörlig aktsamhet beror på arten av och nivån på den cybersäkerhetsrisk som är förknippad med en viss komponent, och bör i detta syfte beakta en eller flera av följande åtgärder: Kontrollera, när så är relevant, att tillverkaren av en komponent har påvisat överensstämmelse med denna förordning, inbegripet genom att kontrollera om komponenten redan är försedd med CE-märkning. Kontrollera att en komponent får regelbundna säkerhetsuppdateringar, till exempel genom att kontrollera dess säkerhetshistorik. Kontrollera att en komponent är fri från sårbarheter som registrerats i den europeiska sårbarhetsdatabas som inrättats enligt artikel 12.2 i direktiv (EU) 2022/2555 eller andra allmänt tillgängliga sårbarhetsdatabaser, eller utföra ytterligare säkerhetstester. De skyldigheter att hantera sårbarheter som fastställs i denna förordning och som tillverkare måste uppfylla när de släpper ut en produkt med digitala element på marknaden och för stödperioden, gäller för produkter med digitala element i sin helhet, inbegripet alla integrerade komponenter. Om tillverkaren av en produkt med digitala element vid utövandet av tillbörlig aktsamhet identifierar en sårbarhet i en komponent, inbegripet i en komponent med fri och öppen källkod, bör den informera den person eller entitet som tillverkar eller underhåller komponenten, åtgärda och avhjälpa sårbarheten och, i tillämpliga fall, förse personen eller entiteten med den tillämpade säkerhetsåtgärden.

(35) Omedelbart efter övergångsperioden för tillämpningen av denna förordning kan en tillverkare av en produkt med digitala element som integrerar en eller flera komponenter från tredje parter som också omfattas av denna förordning inte kunna kontrollera, som en del av sin skyldighet att visa tillbörlig aktsamhet, att tillverkarna av dessa komponenter har visat överensstämmelse med denna förordning, till exempel genom att kontrollera om komponenterna redan är CE-märkta. Detta kan vara fallet om komponenterna har integrerats innan denna förordning blir tillämplig på tillverkarna av dessa komponenter. I sådana fall bör en tillverkare som integrerar sådana komponenter visa tillbörlig aktsamhet på andra sätt.

(36) Produkter med digitala element bör vara försedda med en CE-märkning som på ett synligt, läsligt och outplånligt sätt visar att de överensstämmer med denna förordning, så att de omfattas av den fria rörligheten på den inre marknaden. Medlemsstaterna bör inte sätta upp omotiverade hinder för utsläppandet på marknaden av produkter med digitala element som uppfyller kraven i denna förordning och är försedda med en CE-märkning. Dessutom bör medlemsstaterna vid mässor, utställningar och demonstrationer eller liknande evenemang inte förhindra presentation eller användning av en produkt med digitala element som inte uppfyller kraven i denna förordning, inbegripet prototyper, förutsatt att produkten presenteras med en synlig skylt som tydligt anger att produkten inte uppfyller kraven i denna förordning och att den inte får tillhandahållas på marknaden förrän den gör det.

(37) För att säkerställa att tillverkarna kan släppa ut programvara i testsyfte innan deras produkter med digitala element genomgår en bedömning av överensstämmelse bör medlemsstaterna inte hindra tillhandahållandet av ofärdig programvara, såsom alfaversioner, betaversioner eller lanseringskandidater, förutsatt att inte färdigställd programvara endast görs tillgänglig så lång tid som de behöver för att testa den och få återkoppling. Tillverkarna bör säkerställa att programvara som görs tillgänglig under de villkoren endast släpps ut efter att en riskbedömning har gjorts och att den i möjligaste mån uppfyller de säkerhetskrav som enligt denna förordning föreskrivs för egenskaper hos produkter med digitala element. Tillverkarna bör också i möjligaste mån uppfylla sårbarhetshanteringskraven. Tillverkarna bör inte tvinga användare att uppgradera till versioner som endast släppts ut i testsyfte.

(38) För att säkerställa att produkter med digitala element inte utgör cybersäkerhetsrisker för personer och organisationer när de släpps ut på marknaden bör väsentliga cybersäkerhetskrav fastställas för sådana produkter. Dessa väsentliga cybersäkerhetskrav, inbegripet krav på hantering av sårbarhetshantering, är tillämpliga för varje enskild produkt med digitala element när den släpps ut på marknaden, oavsett om produkten med digitala element tillverkas som en enskild enhet eller i serie. För en produkttyp bör till exempel varje enskild produkt med digitala element ha fått alla säkerhetsprogramfixar eller uppdateringar som finns tillgängliga för att hantera relevanta säkerhetsfrågor när den släpps ut på marknaden. När produkterna med digitala element senare, fysiskt eller digitalt, ändras på ett sätt som tillverkaren inte förutsett i den ursprungliga riskbedömningen och som kan innebära att de inte längre uppfyller de relevanta väsentliga cybersäkerhetskraven, bör ändringen betraktas som väsentlig. Exempelvis kan programvarureparationer betraktas som underhållsåtgärder, förutsatt att de inte ändrar en produkt med digitala element som redan släppts ut på marknaden på ett sådant sätt att överensstämmelsen med de tillämpliga kraven kan påverkas eller att det avsedda ändamål för vilken produkten har bedömts kan ändras.

(39) Precis som vid fysiska reparationer eller ändringar bör en produkt med digitala element anses vara väsentligt ändrad genom en programvaruändring om programvaruuppdateringen ändrar produktens avsedda ändamål och dessa ändringar inte förutsågs av tillverkaren i den ursprungliga riskbedömningen, eller om farans art har ändrats eller nivån på cybersäkerhetsrisken har ökat på grund av programvaruuppdateringen, och den uppdaterade versionen av produkten tillhandahålls på marknaden. Om en säkerhetsuppdatering, som är utformad för att minska cybersäkerhetsnivån för en produkt med digitala element, inte ändrar det avsedda ändamålet för en produkt med digitala element anses det inte vara en väsentlig ändring. Detta omfattar vanligtvis situationer där säkerhetsuppdateringar endast medför smärre justeringar av källkoden. Detta kan till exempel vara fallet om en säkerhetsuppdatering åtgärdar en känd sårbarhet, inbegripet genom att ändra funktioner eller prestanda hos en produkt med digitala element enbart i syfte att minska cybersäkerhetsrisknivån. På samma sätt bör en mindre funktionsuppdatering, såsom en visuell förbättring eller tillägg av nya piktogram eller språk i användargränssnittet, inte i allmänhet betraktas som en väsentlig ändring. Omvänt gäller att om en funktionsuppdatering ändrar de ursprungligen avsedda funktionerna eller typen eller prestandan för en produkt med digitala element och uppfyller de ovannämnda kriterierna, bör den betraktas vara en väsentlig ändring, eftersom tillägg av nya funktioner vanligtvis leder till en bredare angreppsyta, vilket ökar cybersäkerhetsrisken. Detta kan till exempel vara fallet när ett nytt indataelement läggs till i en applikation, vilket kräver att tillverkaren säkerställer lämplig validering av indata. Vid bedömningen av om en uppdatering av objektet betraktas vara en väsentlig ändring är det inte relevant om den tillhandahålls som en separat uppdatering eller i kombination med en säkerhetsuppdatering. Kommissionen bör ge vägledning för fastställandet av vad som utgör en väsentlig ändring.

(40) Med tanke på programvaruutvecklingens upprepande karaktär bör tillverkare som har släppt ut efterföljande versioner av en programvaruprodukt på marknaden till följd av en senare betydande ändring av den produkten kunna tillhandahålla säkerhetsuppdateringar under stödperioden endast för den version av programvaruprodukten som de senast har släppt ut på marknaden. De bör endast kunna göra detta om användarna av de relevanta tidigare produktversionerna har kostnadsfri tillgång till den produktversion som senast släpptes ut på marknaden och inte ådrar sig ytterligare kostnader för att anpassa den maskin- eller programvarumiljö där de använder produkten. Detta kan till exempel vara fallet när en uppgradering av ett stationärt operativsystem inte kräver ny hårdvara, såsom en snabbare centralenhet eller mer minne. Tillverkaren bör dock under stödperioden fortsätta att uppfylla andra krav på hantering av sårbarheter, såsom att ha en policy för samordnad delgivning av information om sårbarheter eller åtgärder för att underlätta utbytet av information om potentiella sårbarheter för alla efterföljande väsentligt ändrade versioner av den programvara som släpps ut på marknaden. Tillverkarna bör kunna tillhandahålla mindre säkerhets- eller funktionsuppdateringar som inte utgör en väsentlig ändring endast av den senaste versionen eller underversionen av en programvaruprodukt som inte har ändrats väsentligt. Om en hårdvaruprodukt, till exempel en smarttelefon, inte är kompatibel med den senaste versionen av det operativsystem som den ursprungligen levererades med, bör tillverkaren samtidigt fortsätta att tillhandahålla säkerhetsuppdateringar åtminstone för den senaste kompatibla versionen av operativsystemet under stödperioden.

(41) I linje med det vedertagna begreppet väsentlig ändring för produkter som regleras genom unionsharmoniseringslagstiftning, är det, vid en väsentlig ändring som kan påverka överensstämmelsen med denna förordning hos produkten med digitala element eller om produktens avsedda ändamål ändras, lämpligt att produktens överensstämmelse kontrolleras och att den, om tillämpligt, genomgår en ny bedömning av överensstämmelse. Om tillverkaren låter göra en bedömning av överensstämmelse som involverar tredje part bör en förändring som kan leda till en väsentlig ändring i tillämpliga fall anmälas till denna tredje part.

(42) Om en produkt med digitala element är föremål för *renovering*, *underhåll* och *reparation* av en produkt med digitala element, enligt definitionen i artikel 2.18, 2.19 och 2.20 i Europaparlamentets och rådets förordning (EU) 2024/1781[19], medför detta inte nödvändigtvis en väsentlig ändring av produkten, exempelvis om det avsedda ändamålet och de avsedda funktionerna inte ändras och risknivån inte påverkas. Tillverkarens uppgradering av en produkt med digitala element kan dock medföra ändringar av produktens utformning och utveckling och skulle därför kunna påverka dess avsedda ändamål och uppfyllande av de krav som fastställs i den här förordningen.

---

[19] Europaparlamentets och rådets förordning (EU) 2024/1781 av den 13 juni 2024 om upprättande av en ram för att fastställa ekodesignkrav för hållbara produkter, om ändring av direktiv (EU) 2020/1828 och förordning (EU) 2023/1542 och om upphävande av direktiv 2009/125/EG (EUT L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) Produkter med digitala element bör anses vara viktiga om de negativa konsekvenserna av utnyttjandet av potentiella sårbarheter i produkten kan vara allvarliga på grund av, bland annat, cybersäkerhetsrelaterade funktioner eller en funktion som medför en betydande risk för negativa effekter i fråga om dess intensitet och förmåga att störa, kontrollera eller orsaka skada på ett stort antal andra produkter eller på användarnas hälsa, säkerhet eller skydd genom direkt manipulering, såsom en central systemfunktion, inbegripet nätförvaltning, konfigurationsstyrning, virtualisering eller behandling av personuppgifter. I synnerhet kan sårbarheter i produkter med digitala element som har en cybersäkerhetsrelaterad funktion, såsom starthanterare, medföra att säkerhetsproblem sprids i hela leveranskedjan. Allvarlighetsgraden i en cybersäkerhetsincident kan också öka när produkten primärt utför en central systemfunktion, inbegripet nätförvaltning, konfigurationsstyrning, virtualisering eller behandling av personuppgifter.

(44) Vissa kategorier av produkter med digitala element bör omfattas av striktare förfaranden för bedömning av överensstämmelse, med bevarande av proportionaliteten. Därför bör viktiga produkter med digitala element delas in i två klasser som återspeglar produktkategoriernas cybersäkerhetsrisknivå. En incident som involverar viktiga produkter med digitala element som omfattas av i klass II skulle kunna få större negativa konsekvenser än en incident som involverar viktiga produkter med digitala element i klass I, exempelvis på grund av produkternas cybersäkerhetsrelaterade funktion eller utförandet av en annan funktion som medför en betydande risk för negativa effekter. Som en indikation på sådana större negativa effekter skulle produkter med digitala element som omfattas av klass II antingen kunna utföra en cybersäkerhetsrelaterad funktion eller en annan funktion som medför en betydande risk för negativa effekter som är högre än för dem som förtecknas i klass I, eller uppfylla båda ovannämnda kriterier. Viktiga produkter med digitala element som omfattas av klass II bör därför omfattas av ett striktare förfarande för bedömning av överensstämmelse.

(45) Viktiga produkter med digitala element som avses i denna förordning bör förstås som produkter som har kärnfunktionen hos en kategori av viktiga produkter med digitala element som anges i denna förordning. I denna förordning anges exempelvis kategorier av produkter med digitala element som genom sina kärnfunktioner definieras som brandväggar eller intrångsdetektions- eller intrångsskyddssystem i klass II. Därmed bör brandväggar och intrångsdetektions- eller intrångsskyddssystem genomgå en obligatorisk tredjepartsbedömning av överensstämmelse. Detta är inte fallet för andra produkter med digitala element som inte kategoriseras som viktiga produkter med digitala element som kan integrera brandväggar eller intrångsdetektions- eller intrångsskyddssystem. Kommissionen bör anta en genomförandeakt för att specificera den tekniska beskrivningen av de kategorier av viktiga produkter med digitala element som omfattas av klasserna I och II som anges i denna förordning.

(46) De kategorier av kritiska produkter med digitala element som anges i denna förordning har en cybersäkerhetsrelaterad funktion och en funktion som medför en betydande risk för negativa effekter i fråga om intensitet och förmåga att störa, kontrollera eller skada ett stort antal andra produkter med digitala element genom direkt manipulation. Dessutom anses dessa kategorier av produkter med digitala element vara kritiska beroenden för de väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555. De kategorier av kritiska produkter med digitala element som anges i en bilaga till denna förordning använder redan i stor utsträckning olika former av certifiering, och omfattas också av det europeiska gemensamma kriteriebaserade systemet för cybersäkerhetscertifiering (EUCC) som anges i kommissionens genomförandeförordning (EU) 2024/482[20]. För att säkerställa ett gemensamt tillräckligt cybersäkerhetsskydd för kritiska produkter med digitala element i unionen skulle det därför kunna vara lämpligt och proportionellt att genom en delegerad akt låta sådana produktkategorier omfattas av obligatorisk europeisk cybersäkerhetscertifiering om det redan finns en relevant europeisk ordning för cybersäkerhetscertifiering som omfattar dessa produkter och en bedömning av de potentiella marknadseffekterna av den planerade obligatoriska certifieringen har utförts av kommissionen. Bedömningen bör beakta både utbuds- och efterfrågesidan, inbegripet huruvida det finns tillräcklig efterfrågan på de berörda produkterna med digitala element från både medlemsstaterna och användarna för att europeisk cybersäkerhetscertifiering ska krävas, samt de ändamål för vilka produkterna med digitala element är avsedda att användas, inbegripet det kritiska beroendet av dem hos väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555. Bedömningen bör också analysera de potentiella effekterna av den obligatoriska certifieringen på dessa produkters tillgänglighet på den inre marknaden och medlemsstaternas kapacitet och beredskap att genomföra de relevanta europeiska ordningarna för cybersäkerhetscertifiering.

---

[20] Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) Delegerade akter som kräver obligatorisk europeisk cybersäkerhetscertifiering bör fastställa de produkter med digitala element som har kärnfunktionen hos en kategori av kritiska produkter med digitala element som anges i denna förordning och som ska omfattas av obligatorisk certifiering, samt den assuransnivå som krävs, som åtminstone bör vara ”väsentlig”. Den assuransnivå som krävs bör stå i proportion till den nivå av cybersäkerhetsrisk som är förknippad med produkten med digitala element. Om produkten med digitala element till exempel har kärnfunktionen hos en kategori av kritiska produkter med digitala element som anges i denna förordning och är avsedd för användning i en känslig eller kritisk miljö, såsom produkter avsedda för användning av väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555, får den kräva högsta assuransnivå.

(48) För att säkerställa ett gemensamt tillräckligt cybersäkerhetsskydd i unionen för produkter med digitala element som har kärnfunktionen hos en kategori av kritiska produkter med digitala element som anges i denna förordning, bör kommissionen också ges befogenhet att anta delegerade akter för att ändra denna förordning genom att lägga till eller stryka kategorier av kritiska produkter med digitala element, för vilka tillverkare skulle kunna åläggas att erhålla ett europeiskt cybersäkerhetscertifikat inom ramen för en europeisk ordning för cybersäkerhetscertifiering, enligt förordning (EU) 2019/881 för att visa överensstämmelse med denna förordning. En ny kategori av kritiska produkter med digitala element kan läggas till dessa kategorier om det finns ett kritiskt beroende av dem hos de väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555 eller om incidenter eller utnyttjade sårbarheter kan leda till avbrott i kritiska leveranskedjor. När kommissionen bedömer behovet av att lägga till eller stryka kategorier av kritiska produkter med digitala element genom en delegerad akt bör den kunna beakta huruvida medlemsstaterna på nationell nivå har identifierat produkter med digitala element som har en avgörande roll för resiliensen hos de väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555 och som i allt högre grad drabbas av cyberattacker i leveranskedjan, med potentiella allvarliga störande effekter. Dessutom bör kommissionen kunna beakta resultatet av den samordnade säkerhetsriskbedömning av kritiska leveranskedjor på unionsnivå som genomförts i enlighet med artikel 22 i direktiv (EU) 2022/2555.

(49) Kommissionen bör se till att ett brett spektrum av berörda parter rådfrågas på ett strukturerat och regelbundet sätt vid utarbetandet av åtgärder för genomförandet av denna förordning. Detta bör särskilt vara fallet när kommissionen bedömer behovet av potentiella uppdateringar av förteckningarna över kategorier av viktiga eller kritiska produkter med digitala element, där relevanta tillverkare bör rådfrågas och deras synpunkter beaktas för att analysera cybersäkerhetsriskerna samt balansen mellan kostnader och fördelar med att beteckna sådana produktkategorier som viktiga eller kritiska.

(50) Denna förordning behandlar cybersäkerhetsrisker på ett målinriktat sätt. Produkter med digitala element kan dock utgöra andra säkerhetsrisker som inte alltid rör cybersäkerheten men som kan vara en konsekvens av en säkerhetsöverträdelse. Dessa risker bör även fortsättningsvis regleras av annan relevant unionsharmoniseringslagstiftning än denna förordning. Om ingen annan del av unionsharmoniseringslagstiftningen än denna förordning är tillämplig bör de omfattas av Europaparlamentets och rådets förordning (EU) 2023/988[21]. Mot bakgrund av denna förordnings fokus och som en avvikelse från artikel 2.1 tredje stycket b i förordning (EU) 2023/988, bör kapitel III avsnitt 1, kapitel V och VII och kapitel IX–XI i förordning (EU) 2023/988 tillämpas på produkter med digitala element med avseende på säkerhetsrisker som inte omfattas av den här förordningen, om produkterna inte omfattas av särskilda krav enligt andra bestämmelser i annan unionsharmoniseringslagstiftning än den här förordningen i den mening som avses i artikel 3.27 i förordning (EU) 2023/988.

---

[21] Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG (EUT L 135, 23.5.2023, s. 1).

(51) Produkter med digitala element som klassificeras som AI-system med hög risk enligt definitionen i artikel 6 i Europaparlamentets och rådets förordning (EU) 2024/1689[22] och som omfattas av den här förordningen bör uppfylla de väsentliga cybersäkerhetskrav som fastställs i den här förordningen. När sådana AI-system med hög risk uppfyller de väsentliga cybersäkerhetskrav som anges i den här förordningen bör de anses uppfylla de cybersäkerhetskrav som fastställs i artikel 15 i förordning (EU) 2024/1689 i den mån som dessa krav omfattas av en EU-försäkran om överensstämmelse som utfärdats enligt den här förordningen, eller delar av denna. För detta ändamål bör vid bedömningen av cybersäkerhetsriskerna i samband med en produkt med digitala element som klassificeras som ett AI-system med hög risk enligt förordning (EU) 2024/1689 under planerings-, utformnings-, utvecklings-, produktions-, leverans- och underhållsfaserna för en sådan produkt, i enlighet med den här förordningen, risker för ett AI-systems cyberresiliens beaktas när det gäller obehöriga tredje parters försök att ändra dess användning, beteende eller prestanda, inbegripet AI-specifika sårbarheter såsom dataförgiftning eller kontradiktoriska angrepp, samt, i relevanta fall, risker för grundläggande rättigheter, i enlighet med förordning (EU) 2024/1689. När det gäller de förfaranden för bedömning av överensstämmelse avseende väsentliga cybersäkerhetskrav för en produkt med digitala element som omfattas av den här förordningen och klassificeras som ett AI-system med hög risk, bör artikel 43 i förordning (EU) 2024/1689 tillämpas som regel i stället för relevanta bestämmelser i den här förordningen.

---

[22] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Denna regel bör dock inte leda till att den nödvändiga assuransnivån sänks för viktiga eller kritiska produkter med digitala element enligt den här förordningen. Med avvikelse från den regeln bör därför också AI-system med hög risk som omfattas av förordning (EU) 2024/1689 och som också kategoriseras som viktiga eller kritiska produkter med digitala element enligt den här förordningen, och på vilka förfarandet för bedömning av överensstämmelse baserat på intern kontroll enligt bilaga VI i förordning (EU) 2024/1689 är tillämpligt, omfattas av den här förordningens bestämmelser om förfarandena för bedömning av överensstämmelse i den mån som de väsentliga cybersäkerhetskrav som anges i den här förordningen berörs. När det gäller alla andra aspekter som omfattas av förordning (EU) 2024/1689, bör i sådana fall relevanta bestämmelser om bedömning av överensstämmelse baserad på intern kontroll vilka fastställs i bilaga VI till den förordningen tillämpas.

(52) För att förbättra säkerheten för produkter med digitala element som släpps ut på den inre marknaden är det nödvändigt att fastställa väsentliga cybersäkerhetskrav som är tillämpliga på sådana produkter. Dessa väsentliga cybersäkerhetskrav bör inte påverka tillämpningen av samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor som avses i artikel 22 i direktiv (EU) 2022/2555, som beaktar både tekniska och, när så är relevant, icke-tekniska riskfaktorer, såsom tredjelands otillbörliga påverkan på leverantörer. De bör inte heller påverka medlemsstaternas rätt att fastställa ytterligare krav för att ta hänsyn till icke-tekniska faktorer för att säkerställa en hög resiliensnivå, inbegripet krav som definieras i kommissionens rekommendation (EU) 2019/534[23], den EU-samordnade riskbedömningen av cybersäkerhet i 5G-nät och EU-verktygslådan för 5G-cybersäkerhet som överenskommits av samarbetsgruppen som inrättats enligt artikel 14 i direktiv (EU) 2022/2555.

[23] Kommissionens rekommendation (EU) 2019/534 av den 26 mars 2019 om it-säkerhet i 5G-nät (EUT L 88, 29.3.2019, s. 42).

(53) Tillverkare av produkter som omfattas av Europaparlamentets och rådets förordning (EU) 2023/1230[24] och som också är produkter med digitala element enligt definitionen i den här förordningen bör uppfylla både de väsentliga cybersäkerhetskrav som fastställs i den här förordningen och de grundläggande hälso- och säkerhetskraven i förordning (EU) 2023/1230. De väsentliga cybersäkerhetskrav som anges i den här förordningen och vissa väsentliga krav som anges i förordning (EU) 2023/1230 skulle kunna hantera liknande cybersäkerhetsrisker. Överensstämmelse med de väsentliga cybersäkerhetskrav som anges i den här förordningen skulle därför kunna underlätta efterlevnaden av de grundläggande krav som även omfattar vissa cybersäkerhetsrisker enligt förordning (EU) 2023/1230, särskilt de som rör skydd mot korruption samt säkerhet och tillförlitlighet hos de kontrollsystem som anges i avsnitten 1.1.9 och 1.2.1 i bilaga III till den förordningen. Sådana synergier måste påvisas av tillverkaren, till exempel genom att i förekommande fall tillämpa harmoniserade standarder eller andra tekniska specifikationer som omfattar relevanta väsentliga cybersäkerhetskrav efter en riskbedömning som omfattar dessa cybersäkerhetsrisker. Tillverkaren bör också följa de tillämpliga förfaranden för bedömning av överensstämmelse som anges i den här förordningen och i förordning (EU) 2023/1230. Kommissionen och de europeiska standardiseringsorganisationerna bör i det förberedande arbetet för genomförandet av den här förordningen och förordning (EU) 2023/1230 och de därmed sammanhängande standardiseringsprocesserna främja enhetlighet i hur cybersäkerhetsriskerna ska bedömas och hur dessa risker ska omfattas av harmoniserade standarder med avseende på de relevanta väsentliga kraven.

---

[24] Europaparlamentets och rådets förordning (EU) 2023/1230 av den 14 juni 2023 om maskiner och om upphävande av Europaparlamentets och rådets direktiv 2006/42/EG och rådets direktiv 73/361/EEG (EUT L 165, 29.6.2023, s. 1).

Kommissionen och de europeiska standardiseringsorganisationerna bör särskilt beakta den här förordningen vid förberedelserna och utarbetandet av harmoniserade standarder för att underlätta genomförandet av förordning (EU) 2023/1230, särskilt när det gäller cybersäkerhetsaspekter i samband med skydd mot förvanskning samt säkerhet och tillförlitlighet i kontrollsystemen som anges i avsnitten 1.1.9 och 1.2.1 i bilaga III till den förordningen. Kommissionen bör tillhandahålla vägledning för att stödja tillverkare som omfattas av den här förordningen och som också omfattas av förordning (EU) 2023/1230, särskilt för att underlätta påvisandet av överensstämmelse med relevanta grundläggande krav som fastställs i den här förordningen och förordning (EU) 2023/1230.

(54) För att säkerställa att produkter med digitala element är säkra både när de släpps ut på marknaden och under den tid som produkten med digitala element förväntas vara i bruk, är det nödvändigt att fastställa väsentliga cybersäkerhetskrav för sårbarhetshantering och väsentliga cybersäkerhetskrav för egenskaperna hos produkter med digitala element. Tillverkarna bör uppfylla alla väsentliga cybersäkerhetskrav som rör sårbarhetshantering under produktens hela stödperiod och de bör fastställa vilka andra väsentliga cybersäkerhetskrav på produktegenskaper som är relevanta för den berörda typen av produkt med digitala element. Därför bör tillverkarna göra en bedömning av vilka cybersäkerhetsrisker som är förbundna med en produkt med digitala element, för att identifiera relevanta risker och relevanta väsentliga cybersäkerhetskrav för att tillhandahålla sina produkter med digitala element utan kända sårbarheter som kan utnyttjas och som kan påverka dessa produkters säkerhet och tillämpa lämpliga harmoniserade standarder, gemensamma specifikationer eller europeiska eller internationella standarder.

(55) I de fall då vissa väsentliga cybersäkerhetskrav inte är tillämpliga på en produkt med digitala element ska tillverkaren inkludera en tydlig motivering till detta i bedömningen av cybersäkerhetsrisker inbegripet i den tekniska dokumentationen. Detta kan vara fallet om ett väsentligt cybersäkerhetskrav är oförenligt med beskaffenheten hos en produkt med digitala element. Till exempel kan det avsedda ändamålet med en produkt med digitala element kräva att tillverkaren följer allmänt erkända interoperabilitetsstandarder även om dess säkerhetsdetaljer inte längre anses vara den senaste tekniken. På samma sätt kräver annan unionsrätt att tillverkarna tillämpar särskilda interoperabilitetskrav. Om ett väsentligt cybersäkerhetskrav inte är tillämpligt på en produkt med digitala element, men tillverkaren har identifierat cybersäkerhetsrisker i samband med det väsentliga cybersäkerhetskravet, bör tillverkaren vidta åtgärder för att hantera dessa risker på andra sätt, till exempel genom att begränsa produktens avsedda ändamål till tillförlitliga miljöer eller genom att informera användarna om dessa risker.

(56) En av de viktigaste åtgärderna som användarna ska vidta för att skydda sina produkter med digitala element från cyberattacker är att installera de senaste tillgängliga säkerhetsuppdateringarna så snart som möjligt. Tillverkarna bör därför utforma sina produkter och införa processer för att säkerställa att produkter med digitala element omfattar funktioner som möjliggör anmälan, distribution, nedladdning och installation av automatiska säkerhetsuppdateringar, särskilt när det gäller konsumentprodukter. De bör också ge möjlighet att godkänna nedladdning och installation av säkerhetsuppdateringar som ett sista steg. Användarna bör behålla möjligheten att avaktivera automatiska uppdateringar, med en tydlig och lättanvänd mekanism som stöds av tydliga instruktioner om hur användarna kan frånsäga sig dem. De krav avseende automatiska uppdateringar som anges i en bilaga till denna förordning är inte tillämpliga på produkter med digitala element som främst är avsedda att integreras som komponenter i andra produkter. De är inte heller tillämpliga på produkter med digitala element för vilka användarna inte rimligen skulle förvänta sig automatiska uppdateringar, inbegripet produkter med digitala element som är avsedda att användas i IKT-nätverk för yrkesmässigt bruk, särskilt i kritiska miljöer och industrimiljöer där en automatisk uppdatering skulle kunna störa verksamheten. Oavsett om en produkt med digitala element är utformad för att få automatiska uppdateringar eller inte bör tillverkaren informera användarna om sårbarheter och göra säkerhetsuppdateringar tillgängliga utan dröjsmål. Om en produkt med digitala element har ett användargränssnitt eller liknande tekniska medel som möjliggör direkt interaktion med användarna bör tillverkaren använda sådana funktioner för att informera användarna om att deras produkt med digitala element har nått slutet av stödperioden. Anmälningar bör begränsas till vad som är nödvändigt för att säkerställa ett effektivt mottagande av denna information och bör inte ha en negativ inverkan på användarupplevelsen av produkten med digitala element.

(57) För att förbättra insynen i processer för sårbarhetshantering och för att säkerställa att användarna inte är skyldiga att installera nya funktionsuppdateringar enbart i syfte att ta emot de senaste säkerhetsuppdateringarna, bör tillverkarna, när det är tekniskt möjligt, säkerställa att nya säkerhetsuppdateringar tillhandahålls separat från funktionsuppdateringar.

(58) I det gemensamma meddelandet *Europeisk strategi för ekonomisk säkerhet* från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik av den 20 juni 2023 anges att unionen måste maximera fördelarna med sin ekonomiska öppenhet och samtidigt minimera riskerna med ekonomiskt beroende av högriskleverantörer, genom en gemensam strategisk ram för unionens ekonomiska säkerhet. Beroenden av högriskleverantörer av produkter med digitala element kan utgöra en strategisk risk som måste hanteras på unionsnivå, särskilt om produkterna med digitala element är avsedda för användning av väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555. Sådana risker kan vara kopplade till, men inte begränsas till, den jurisdiktion som är tillämplig på tillverkaren, egenskaperna hos dess företagsägande och kopplingarna till kontrollen till en tredjelandsregering där den är etablerad, särskilt om ett land ägnar sig åt ekonomiskt spionage eller oansvarigt statligt beteende i cyberrymden och dess lagstiftning tillåter godtycklig tillgång till alla typer av företagsverksamhet eller uppgifter, inbegripet kommersiellt känsliga uppgifter, och kan införa skyldigheter för underrättelseändamål utan demokratiska kontroller och motvikter, tillsynsmekanismer, rättssäkerhet eller rätt att överklaga till en oberoende domstol. Vid fastställandet av betydelsen av en cybersäkerhetsrisk i den mening som avses i denna förordning bör kommissionen och marknadskontrollmyndigheterna, i enlighet med sina ansvarsområden enligt denna förordning, också beakta icke-tekniska riskfaktorer, särskilt de som fastställts till följd av samordnade säkerhetsriskbedömningar av kritiska leveranskedjor på unionsnivå som genomförts i enlighet med artikel 22 i direktiv (EU) 2022/2555.

(59) För att säkerställa säkerheten för produkter med digitala element efter deras utsläppande på marknaden bör tillverkarna fastställa stödperioder som bör återspegla den tid som produkten med digitala element förväntas vara i bruk. Vid fastställandet av en stödperiod bör en tillverkare särskilt ta hänsyn till rimliga förväntningar från användarna, produktens beskaffenhet samt relevant unionsrätt som fastställer livslängden för produkter med digitala element. Tillverkarna bör också kunna ta hänsyn till andra relevanta faktorer. Kriterierna bör tillämpas på ett sätt som säkerställer proportionalitet vid fastställandet av stödperioden. På begäran bör en tillverkare förse marknadskontrollmyndigheterna med den information som beaktades för att fastställa stödperioden för en produkt med digitala element.

(60) Den stödperiod under vilken tillverkaren säkerställer en effektiv hantering av sårbarheter bör vara minst fem år, såvida inte livslängden för produkten med digitala element är kortare än fem år, och i sådana fall bör tillverkaren säkerställa sårbarhetshanteringen under den livslängden. Om den tid som produkten med digitala element rimligen förväntas vara i bruk är längre än fem år, vilket ofta är fallet för maskinvarukomponenter såsom moderkort eller mikroprocessorer, nätverksenheter såsom routrar, modem eller växlar samt programvara såsom operativsystem eller videoredigeringsverktyg, bör tillverkarna följaktligen säkerställa längre stödperioder. I synnerhet produkter med digitala element som är avsedda att användas i industriella miljöer, såsom industriella styrsystem, används ofta under betydligt längre perioder. En tillverkare bör kunna fastställa en stödperiod på mindre än fem år endast om detta är motiverat på grund av beskaffenheten av den berörda produkten med digitala element och om produkten förväntas användas i mindre än fem år, och i sådana fall bör stödperioden motsvara den förväntade användningstiden. Exempelvis skulle livslängden för en kontaktspårningsapplikation som är avsedd att användas under en pandemi kunna begränsas till pandemins varaktighet. Dessutom kan vissa programvaruapplikationer av naturliga skäl endast göras tillgängliga på grundval av en abonnemangsmodell, särskilt om applikationen inte är tillgänglig för användaren och följaktligen inte längre används när abonnemanget löper ut.

(61) När produkter med digitala element når slutet av sina stödperioder bör tillverkarna, för att säkerställa att sårbarheter kan hanteras efter stödperiodens slut, överväga att frigöra källkoden för sådana produkter med digitala element, antingen till andra företag som åtar sig att utvidga tillhandahållandet av tjänster för sårbarhetshantering, eller till allmänheten. Om tillverkare frigör källkoden till andra företag bör de kunna skydda äganderätten till produkten med digitala element och förhindra att källkoden sprids till allmänheten, till exempel genom avtalsarrangemang.

(62) För att säkerställa att tillverkare i hela unionen fastställer liknande stödperioder för jämförbara produkter med digitala element bör Adco-gruppen offentliggöra statistik över de genomsnittliga stödperioder som fastställs av tillverkarna för kategorier av produkter med digitala element och utfärda riktlinjer som anger lämpliga stödperioder för sådana kategorier. För att säkerställa ett harmoniserat tillvägagångssätt på hela den inre marknaden bör kommissionen dessutom kunna anta delegerade akter för att specificera minsta tillåtna stödperioder för specifika produktkategorier i de fall då de uppgifter som tillhandahålls av marknadskontrollmyndigheterna tyder på att de stödperioder som fastställts av tillverkarna systematiskt inte stämmer överens med kriterierna för att fastställa stödperioderna enligt denna förordning, eller att tillverkare i olika medlemsstater på ett omotiverat sätt fastställer olika stödperioder.

(63) Tillverkarna bör inrätta en gemensam kontaktpunkt som gör det möjligt för användarna att enkelt kommunicera med dem, inbegripet i syfte att rapportera och ta emot information om sårbarheter hos produkten med digitala element. De bör göra den gemensamma kontaktpunkten lättillgänglig för användarna och tydligt ange dess tillgänglighet och hålla denna information uppdaterad. Om tillverkarna väljer att erbjuda automatiserade verktyg, t.ex. chattbotar, bör de också erbjuda ett telefonnummer eller andra digitala kontaktmöjligheter, såsom en e-postadress eller ett kontaktformulär. Den gemensamma kontaktpunkten bör inte uteslutande förlita sig på automatiserade verktyg.

(64) Tillverkarna bör tillhandahålla sina produkter med digitala element på marknaden med en säker standardkonfiguration och tillhandahålla användarna säkerhetsuppdateringar utan kostnad. Tillverkarna bör endast kunna avvika från dessa väsentliga cybersäkerhetskrav när det gäller skräddarsydda produkter som är anpassade för ett visst ändamål och för en viss företagsanvändare och om både tillverkaren och användaren uttryckligen har samtyckt till en annan uppsättning avtalsvillkor.

(65) Tillverkarna bör samtidigt, via den gemensamma rapporteringsplattformen, anmäla aktivt utnyttjade sårbarheter i produkter med digitala element samt allvarliga incidenter som påverkar dessa produkters säkerhet till både den enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet) som utsetts till samordnare och till Enisa. Anmälningarna bör lämnas in med hjälp av slutpunkten för elektronisk anmälan hos en CSIRT-enhet som utsetts till samordnare och bör samtidigt vara tillgängliga för Enisa.

(66) Tillverkarna bör anmäla aktivt utnyttjade sårbarheter för att säkerställa att de CSIRT-enheter som utsetts till samordnare, och Enisa, har en adekvat överblick över sådana sårbarheter och förses med den information som de behöver för att utföra sina uppgifter som anges i direktiv (EU) 2022/2555 och höja den allmänna cybersäkerhetsnivån för de väsentliga och viktiga entiteter som avses i artikel 3 i det direktivet, och för att säkerställa att marknadskontrollmyndigheterna fungerar effektivt. I och med att de flesta produkter med digitala element saluförs på hela den inre marknaden bör varje utnyttjad sårbarhet i en produkt med digitala element anses som ett hot mot en fungerande inre marknad. Enisa bör, i samförstånd med tillverkaren, meddela åtgärdade sårbarheter till den europeiska sårbarhetsdatabas som inrättats enligt artikel 12.2 i direktiv (EU) 2022/2555. Den europeiska sårbarhetsdatabasen kommer att hjälpa tillverkarna att upptäcka kända sårbarheter i deras produkter som kan utnyttjas, för att säkerställa att säkra produkter tillhandahålls på marknaden.

(67) Tillverkarna bör också anmäla alla allvarliga incidenter som påverkar säkerheten för produkter med digitala element till den CSIRT-enhet som utsetts till samordnare och Enisa. För att säkerställa att användarna kan reagera snabbt på allvarliga incidenter som påverkar säkerheten för deras produkter med digitala element, bör tillverkarna också underrätta sina användare om alla sådana incidenter och, om tillämpligt, om eventuella korrigerande åtgärder som användarna kan vidta för att begränsa konsekvenserna av incidenten, exempelvis genom att offentliggöra relevant information på sina webbplatser eller, om tillverkaren kan kontakta användarna och det är motiverat med tanke på cybersäkerhetsriskerna, genom att vända sig direkt till användarna.

(68) Aktivt utnyttjade sårbarheter rör fall där en tillverkare fastställer att en säkerhetsöverträdelse som påverkar dess användare eller någon annan fysisk eller juridisk person har orsakats av en fientlig aktör som utnyttjar en brist i en av de produkter med digitala element som tillverkaren tillhandahåller på marknaden. Exempel på sådana sårbarheter skulle kunna vara svagheter i en produkts identifierings- och autentiseringsfunktioner. Sårbarheter som upptäcks utan ont uppsåt för att i god tro testa, utreda, korrigera eller delge information i syfte att stödja systemägarens och dess användares säkerhet eller trygghet bör inte omfattas av kravet på obligatorisk anmälan. Allvarliga incidenter som påverkar säkerheten för produkten med digitala element avser å andra sidan situationer där en cybersäkerhetsincident påverkar tillverkarens utvecklings-, produktions- eller underhållsprocesser på ett sådant sätt att det skulle kunna leda till en ökad cybersäkerhetsrisk för användare eller andra personer. En sådan allvarlig incident skulle kunna vara en situation då en angripare har lyckats införa en skadlig kod i den kanal genom vilken tillverkaren släpper säkerhetsuppdateringar till användarna.

(69) För att säkerställa att anmälningar snabbt kan spridas till alla relevanta CSIRT-enheter som utsetts till samordnare och för att tillverkare ska kunna lämna in en enda anmälan i varje skede av anmälningsprocessen, bör Enisa inrätta en gemensam rapporteringsplattform med nationella slutpunkter för elektronisk anmälan. Den dagliga driften av den gemensamma rapporteringsplattformen bör skötas och upprätthållas av Enisa. De CSIRT-enheter som utsetts till samordnare bör informera sina respektive marknadskontrollmyndigheter om anmälda sårbarheter eller incidenter. Den gemensamma rapporteringsplattformen bör utformas på ett sådant sätt att den säkerställer konfidentialitet för anmälningar, särskilt när det gäller sårbarheter för vilka en säkerhetsuppdatering ännu inte är tillgänglig. Enisa bör dessutom införa förfaranden för att hantera information på ett säkert och konfidentiellt sätt. På grundval av sin insamlade information bör Enisa vartannat år utarbeta en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element, och lämna den till samarbetsgruppen enligt artikel 14 i direktiv (EU) 2022/2555.

(70) Under exceptionella omständigheter, och särskilt på begäran av tillverkaren, bör den CSIRT-enhet som utsetts till samordnare och som först tar emot anmälan kunna besluta att skjuta upp spridningen av den till de andra relevanta CSIRT-enheter som utsetts till samordnare via den gemensamma rapporteringsplattformen, om detta kan motiveras på grundval av cybersäkerhetsrelaterade skäl och under en tidsperiod som är absolut nödvändig. Den CSIRT-enhet som utsetts till samordnare bör omedelbart informera Enisa om beslutet att skjuta upp spridningen och skälen till detta samt när den avser att återuppta spridningen av anmälan. Kommissionen bör genom en delegerad akt utarbeta specifikationer om villkoren för när cybersäkerhetsrelaterade skäl kan tillämpas och bör samarbeta med det CSIRT-nätverk som inrättas enligt artikel 15 i direktiv (EU) 2022/2555, och med Enisa när det gäller att utarbeta utkastet till delegerad akt. Exempel på cybersäkerhetsrelaterade skäl är en pågående samordnad delgivning av information om sårbarheter eller situationer då en tillverkare snabbt förväntas tillhandahålla en riskreducerande åtgärd och då cybersäkerhetsriskerna med en omedelbar spridning via den gemensamma rapporteringsplattformen väger tyngre än fördelarna. På begäran av den CSIRT-enhet som utsetts till samordnare bör Enisa kunna stödja denna CSIRT-enhet i tillämpningen av cybersäkerhetsrelaterade skäl när det gäller att skjuta upp spridningen av anmälan på grundval av den information Enisa har mottagit från den CSIRT-enheten om beslutet att undanhålla en anmälan utifrån dessa cybersäkerhetsrelaterade skäl. Under särskilt exceptionella omständigheter bör Enisa dessutom inte få alla uppgifter som rör en anmälan om en aktivt utnyttjad sårbarhet samtidigt.

Detta skulle vara fallet om tillverkaren i sin anmälan anger att den anmälda sårbarheten aktivt har utnyttjats av en fientlig aktör och att den, enligt tillgänglig information, inte har utnyttjats i någon annan medlemsstat än den där CSIRT-enheten har utsetts till samordnare och till vilken tillverkaren har anmält sårbarheten, när all omedelbar fortsatt spridning av den anmälda sårbarheten sannolikt skulle leda till tillhandahållande av information vars utlämnande skulle strida mot den medlemsstatens väsentliga intressen, eller när den anmälda sårbarheten utgör en överhängande hög cybersäkerhetsrisk till följd av den fortsatta spridningen. I sådana fall kommer Enisa endast att få samtidig tillgång till information om att tillverkaren har gjort en anmälan och till generell information om den berörda produkten med digitala element, information om den allmänna karaktären av utnyttjandet och information om att dessa säkerhetsskäl har angetts av tillverkaren och att det fullständiga innehållet i anmälan därför undanhålls. Den fullständiga anmälan bör sedan göras tillgänglig för Enisa och andra relevanta CSIRT-enheter som utsetts till samordnare när den CSIRT-enhet som utsetts till samordnare och som först tar emot anmälan konstaterar att dessa säkerhetsskäl, som utgör ovanligt exceptionella omständigheter enligt denna förordning, inte längre föreligger. Om Enisa, på grundval av den tillgängliga informationen, anser att det finns en systemrisk som påverkar säkerheten på den inre marknaden bör Enisa rekommendera den mottagande CSIRT-enheten att sprida den fullständiga anmälan till de andra CSIRT-enheter som utsetts till samordnare och till Enisa själv.

(71) När tillverkarna anmäler en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala element bör de ange hur känslig de anser att den anmälda informationen är. Den CSIRT-enhet som utsetts till samordnare och som först tar emot anmälan bör ta hänsyn till denna information när den bedömer huruvida anmälan ger upphov till exceptionella omständigheter som motiverar att spridningen av anmälan till de andra relevanta CSIRT-enheter som utsetts till samordnare på grundval av motiverade cybersäkerhetsrelaterade skäl skjuts upp. Den bör också ta hänsyn till denna information när den bedömer huruvida anmälan om en aktivt utnyttjad sårbarhet ger upphov till ovanligt exceptionella omständigheter som motiverar att den fullständiga anmälan inte samtidigt görs tillgänglig för Enisa. Slutligen bör CSIRT-enheter som utsetts till samordnare kunna beakta denna information när de fastställer lämpliga åtgärder för att begränsa de risker som härrör från sådana sårbarheter och incidenter.

(72) För att förenkla rapporteringen av den information som krävs enligt denna förordning, med beaktande av andra kompletterande rapporteringskrav som fastställs i unionsrätten, såsom förordning (EU) 2016/679, Europaparlamentets och rådets förordning (EU) 2022/2554[25], Europaparlamentets och rådets direktiv 2002/58/EG[26] och direktiv (EU) 2022/2555, samt för att minska den administrativa bördan för entiteterna, uppmuntras medlemsstaterna att överväga att tillhandahålla gemensamma kontaktpunkter på nationell nivå för sådana rapporteringskrav. Användningen av sådana nationella gemensamma kontaktpunkter för att rapportera säkerhetsincidenter enligt förordning (EU) 2016/679 och direktiv 2002/58/EG bör inte påverka tillämpningen av bestämmelserna i förordning (EU) 2016/679 och direktiv 2002/58/EG, särskilt de som rör oberoendet för de myndigheter som avses i dessa. Vid inrättandet av den gemensamma rapporteringsplattform som avses i den här förordningen bör Enisa beakta möjligheten att integrera de nationella slutpunkter för elektronisk anmälan som avses i den här förordningen i nationella gemensamma kontaktpunkter som också kan integrera andra anmälningar som krävs enligt unionsrätten.

---

[25] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).

[26] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (EGT L 201, 31.7.2002, s. 37).

(73) Vid inrättandet av den gemensamma rapporteringsplattform som avses i denna förordning och för att dra nytta av tidigare erfarenheter bör Enisa samråda med unionens andra institutioner eller byråer som förvaltar plattformar eller databaser som omfattas av stränga säkerhetskrav, såsom Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA). Enisa bör också analysera eventuell komplementaritet med den europeiska sårbarhetsdatabas som inrättats enligt artikel 12.2 i direktiv (EU) 2022/2555.

(74) Tillverkare och andra fysiska och juridiska personer bör på frivillig basis, till en CSIRT-enhet som utsetts till samordnare eller Enisa, kunna anmäla eventuella sårbarheter i en produkt med digitala element, cyberhot som skulle kunna påverka riskprofilen för en produkt med digitala element, eventuella incidenter som påverkar säkerheten för produkten med digitala element samt tillbud som skulle ha kunnat leda till en sådan incident.

(75) Medlemsstaterna bör sträva efter att i största möjliga utsträckning ta itu med de utmaningar som sårbarhetsforskare ställs inför, inbegripet deras potentiella utsatthet för straffrättsligt ansvar, i enlighet med nationell rätt. Med tanke på att fysiska och juridiska personer som forskar om sårbarheter skulle kunna riskera straff- och civilrättsligt ansvar i vissa medlemsstater uppmuntras medlemsstaterna att anta riktlinjer för icke-lagföring av forskare inom informationssäkerhet och befrielse från civilrättsligt ansvar för deras verksamhet.

(76) Tillverkare av produkter med digitala element bör införa samordnade policyer för information om sårbarheter för att underlätta individers eller entiteters rapportering av sårbarheter, antingen direkt till tillverkaren eller indirekt, och anonymt om så begärs, via CSIRT-enheter som utsetts till samordnare för att åstadkomma en samordnad delgivning av information om sårbarheter i enlighet med artikel 12.1 i direktiv (EU) 2022/2555. Tillverkarnas samordnade policy för offentliggörande av sårbarheter bör specificera en strukturerad process där sårbarheter rapporteras till en tillverkare på ett sådant sätt att tillverkaren kan diagnostisera och åtgärda dessa sårbarheter innan mer detaljerad sårbarhetsinformation lämnas ut till tredje part eller till allmänheten. Tillverkarna bör också överväga att offentliggöra sin säkerhetspolicy i maskinläsbart format. I och med att information om sårbarheter som kan utnyttjas hos allmänt använda produkter med digitala element kan säljas till höga priser på den svarta marknaden bör tillverkare av sådana produkter som ett led i sina samordnade policyer för information om sårbarheter kunna använda program för att ge incitament till rapportering av sårbarheter genom att säkerställa att individer eller entiteter får erkännande och ersättning för sina insatser. Detta avser så kallade buggbelöningsprogram.

(77) För att underlätta sårbarhetsanalys bör tillverkarna identifiera och dokumentera de komponenter som ingår i produkter med digitala element, inbegripet genom att utarbeta en programvaruförteckning. En programvaruförteckning kan förse dem som tillverkar, köper och driver programvara med information som förbättrar deras förståelse av leveranskedjan, vilket har många fördelar, framför allt att det hjälper tillverkare och användare att spåra kända nya sårbarheter och cybersäkerhetsrisker. Det är särskilt viktigt att tillverkarna säkerställer att deras produkter med digitala element inte innehåller sårbara komponenter som utvecklats av tredje part. Tillverkarna bör inte vara skyldiga att offentliggöra programvaruförteckningen.

(78) Ett företag som bedriver verksamhet online inom ramen för de nya komplexa affärsmodeller som hänger samman med onlineförsäljning kan tillhandahålla en rad olika tjänster. Beroende på arten av de tjänster som tillhandahålls i samband med en viss produkt med digitala element kan samma entitet omfattas av olika kategorier av affärsmodeller eller ekonomiska aktörer. Om en entitet tillhandahåller endast onlinebaserade förmedlingstjänster för en viss produkt med digitala element och endast är leverantör av en onlinemarknadsplats, enligt definitionen i artikel 3.14 i förordning (EU) 2023/988, kan den inte kategoriseras som någon typ av ekonomisk aktör enligt definitionen i den här förordningen. Om samma entitet är leverantör av en onlinemarknadsplats och även agerar som ekonomisk aktör enligt definitionen i den här förordningen vid försäljningen av särskilda produkter med digitala element, bör den omfattas av de skyldigheter som fastställs i den här förordningen för den typen av ekonomisk aktör. Om till exempel leverantören av en onlinemarknadsplats också distribuerar en produkt med digitala element betraktas denna leverantör, med avseende på försäljningen av den produkten, som distributör. Och även när entiteten i fråga säljer sina egna märkesprodukter med digitala element betraktas den som tillverkare och måste därmed följa de tillämpliga kraven för tillverkare. Vissa entiteter kan också betraktas som leverantörer av distributionstjänster enligt definitionen i artikel 3.11 i Europaparlamentets och rådets förordning (EU) 2019/1020[27] om de erbjuder sådana tjänster. I sådana fall måste en bedömning göras i varje enskilt fall. Med tanke på den framträdande roll som onlinemarknadsplatser har när det gäller att möjliggöra elektronisk handel bör de sträva efter att samarbeta med medlemsstaternas marknadskontrollmyndigheter för att hjälpa till att säkerställa att produkter med digitala element som köps via onlinemarknadsplatser uppfyller de cybersäkerhetskrav som fastställs i den här förordningen.

[27] Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 (EUT L 169, 25.6.2019, s. 1).

(79) För att underlätta bedömningen av överensstämmelse med de krav som fastställs i denna förordning bör det finnas en presumtion om överensstämmelse för produkter med digitala element som överensstämmer med harmoniserade standarder som omsätter de väsentliga cybersäkerhetskrav som anges i denna förordning till detaljerade tekniska specifikationer och som antas i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012[28]. Den förordningen fastställer ett förfarande för invändningar mot harmoniserade standarder som inte helt uppfyller kraven som anges i den här förordningen. Standardiseringsförfarandet bör säkerställa en balanserad representation av intressen och ett aktivt deltagande av berörda parter i det civila samhället, inbegripet konsumentorganisationer. Internationella standarder som stämmer överens med den nivå av cybersäkerhetsskydd som eftersträvas genom de väsentliga cybersäkerhetskrav som fastställs i den här förordningen bör också beaktas, för att underlätta utvecklingen av harmoniserade standarder och genomförandet av den här förordningen samt för att underlätta efterlevnaden för företag, särskilt mikroföretag samt små och medelstora företag och företag som är verksamma på global nivå.

---

[28] Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut nr 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

(80) En snabb utveckling av harmoniserade standarder under övergångsperioden för tillämpningen av denna förordning och tillgängligheten före den dag då denna förordning börjar tillämpas kommer att vara särskilt viktigt för ett effektivt genomförande av den. Detta gäller särskilt viktiga produkter med digitala element som omfattas av klass I. Tillgängliga harmoniserade standarder kommer att göra det möjligt för tillverkarna av sådana produkter att bedöma överensstämmelsen via förfarandet för intern kontroll, och flaskhalsar och förseningar kan därför undvikas när organ för bedömning av överensstämmelse utför sitt arbete.

(81) Genom förordning (EU) 2019/881 inrättas en frivillig europeisk ram för cybersäkerhetscertifiering av IKT-produkter, IKT-processer och IKT-tjänster. De europeiska ordningarna för cybersäkerhetscertifiering förser användarna med en gemensam tillförlitlig ram för användning av produkter med digitala element vilka omfattas av den här förordningens tillämpningsområde. Den här förordningen bör följaktligen skapa synergier med förordning (EU) 2019/881. För att underlätta bedömningen av överensstämmelse med kraven i den här förordningen, när det gäller produkter med digitala element som är certifierade eller för vilka en försäkran om överensstämmelse har utfärdats inom en europeisk ordning för cybersäkerhet enligt förordning (EU) 2019/881 som har identifierats av kommissionen i en genomförandeakt, bör det finnas en presumtion om överensstämmelse med de väsentliga cybersäkerhetskraven i den här förordningen i den mån som det europeiska cybersäkerhetscertifikatet eller försäkran om överensstämmelse – eller delar av dessa – täcker dessa krav. Behovet av nya europeiska ordningar för cybersäkerhetscertifiering av produkter med digitala element bör bedömas i ljuset av den här förordningen, inbegripet när unionens löpande arbetsprogram utarbetas i enlighet med förordning (EU) 2019/881. Om det behövs ett nytt system som omfattar produkter med digitala element, bland annat för att underlätta efterlevnaden av den här förordningen, kan kommissionen begära att Enisa utarbetar förslag till certifieringsordning i enlighet med artikel 48 i förordning (EU) 2019/881. Sådana framtida europeiska ordningar för cybersäkerhet som omfattar produkter med digitala element bör beakta de väsentliga cybersäkerhetskrav och förfaranden för bedömning av överensstämmelse som fastställs i den här förordningen och främja efterlevnaden av den här förordningen. För europeiska ordningar för cybersäkerhetscertifiering som träder i kraft innan den här förordningen träder i kraft kan ytterligare specifikationer behövas om detaljerade aspekter av hur en presumtion om överensstämmelse kan tillämpas.

Kommissionen bör, genom delegerade akter, ha befogenhet att specificera på vilka villkor de europeiska ordningarna för cybersäkerhetscertifiering kan användas för att visa överensstämmelse med de väsentliga cybersäkerhetskrav som fastställs i den här förordningen. För att undvika onödiga administrativa bördor bör det inte finnas någon skyldighet för tillverkarna att genomföra en tredjepartsbedömning av överensstämmelse i enlighet med den här förordningen för motsvarande krav om ett europeiskt cybersäkerhetscertifikat har utfärdats enligt sådana europeiska ordningar för cybersäkerhetscertifiering, på åtminstone assuransnivån ”betydande”.

(82) Vid ikraftträdandet av genomförandeförordning (EU) 2024/482 som avser produkter som omfattas av den här förordningens tillämpningsområde, såsom säkerhetsmoduler i maskinvara och mikroprocessorer, bör kommissionen genom en delegerad akt kunna specificera hur EUCC ger en presumtion om överensstämmelse med de väsentliga cybersäkerhetskrav som anges i den här förordningen eller delar av dessa. En sådan delegerad akt får dessutom specificera hur ett certifikat som utfärdas inom ramen för EUCC befriar tillverkaren från skyldigheten att genomföra en tredjepartsbedömning av överensstämmelse som krävs enligt den här förordningen för de motsvarande kraven.

(83) Den nuvarande europeiska standardiseringsramen, som bygger på de principer enligt den nya metoden som fastställs i rådets resolution av den 7 maj 1985 om en ny metod för teknisk harmonisering och standarder och på förordning (EU) nr 1025/2012, utgör automatiskt ramen för utarbetande av standarder som föreskriver en presumtion om överensstämmelse med de relevanta väsentliga cybersäkerhetskraven i den här förordningen. Europeiska standarder bör vara marknadsdrivna, ta hänsyn till allmänintresset och de politiska mål som tydligt anges i kommissionens begäran till en eller flera europeiska standardiseringsorganisationer att utarbeta harmoniserade standarder inom en fastställd tidsfrist, och bör bygga på samförstånd. I avsaknad av relevanta hänvisningar till harmoniserade standarder bör kommissionen dock kunna anta genomförandeakter för att fastställa gemensamma specifikationer för de väsentliga cybersäkerhetskrav som anges i den här förordningen, förutsatt att den på lämpligt sätt respekterar de europeiska standardiseringsorganisationernas roll och funktioner, som en exceptionell reservlösning för att underlätta tillverkarens skyldighet att uppfylla dessa väsentliga cybersäkerhetskrav, om standardiseringsprocessen blockeras eller om fastställandet av lämpliga harmoniserade standarder försenas. Om en sådan försening beror på den tekniska komplexiteten hos standarden i fråga bör kommissionen beakta detta innan den överväger att fastställa gemensamma specifikationer.

(84) I syfte att så effektivt som möjligt fastställa gemensamma specifikationer som omfattar de väsentliga cybersäkerhetskrav som fastställs i denna förordning bör kommissionen involvera berörda parter i processen.

(85) *Rimlig tid* avser, när det gäller offentliggörandet av en hänvisning till harmoniserade standarder i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, en period under vilken offentliggörandet i *Europeiska unionens officiella tidning* av hänvisningen till standarden, rättelsen eller ändringen av den förväntas och den bör inte överstiga ett år efter den tidsfrist för utarbetande av en europeisk standard som fastställs i enlighet med förordning (EU) nr 1025/2012.

(86) För att underlätta bedömningen av överensstämmelse med de väsentliga cybersäkerhetskrav som anges i denna förordning bör det finnas en presumtion om överensstämmelse för produkter med digitala element som överensstämmer med de gemensamma specifikationer som antas av kommissionen enligt denna förordning i syfte att formulera detaljerade tekniska specifikationer av dessa krav.

(87) Tillämpningen av harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering, som antagits enligt förordning (EU) 2019/881 och som ger presumtion om överensstämmelse i förhållande till de väsentliga cybersäkerhetskrav som är tillämpliga på produkter med digitala element, kommer att underlätta tillverkarnas bedömning av överensstämmelse. Om tillverkaren väljer att inte tillämpa sådana metoder på vissa krav måste tillverkaren i sin tekniska dokumentation ange hur överensstämmelse i så fall uppnås. Tillämpningen av harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering, som antagits enligt förordning (EU) 2019/881 och som ger presumtion om överensstämmelse från tillverkarna, skulle dessutom göra det lättare för marknadskontrollmyndigheterna att kontrollera att produkter med digitala element överensstämmer med kraven. Därför uppmuntras tillverkare av produkter med digitala element att tillämpa sådana harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering.

(88) Tillverkarna bör utarbeta en EU-försäkran om överensstämmelse för att tillhandahålla den information som krävs enligt denna förordning vad gäller produkter med digitala elements överensstämmelse med de väsentliga cybersäkerhetskraven i denna förordning och, om tillämpligt, med andra relevanta bestämmelser i unionsharmoniseringslagstiftning som omfattar produkten med digitala element. Tillverkarna kan också åläggas att upprätta en EU-försäkran om överensstämmelse genom andra unionsrättsakter. För att säkerställa effektiv tillgång till information för marknadskontrolländamål bör en enda EU-försäkran om överensstämmelse upprättas med avseende på överensstämmelsen med alla berörda unionsrättsakter. För att minska den administrativa bördan för ekonomiska aktörer bör denna enda EU-försäkran om överensstämmelse kunna utgöras av dokumentation bestående av enskilda relevanta försäkringar om överensstämmelse.

(89) CE-märkningen visar att en produkt uppfyller kraven och utgör det synliga resultatet av en hel process, som omfattar en bedömning av överensstämmelse i vid bemärkelse. De allmänna principerna för CE-märkning fastställs i Europaparlamentets och rådets förordning (EG) nr 765/2008[29]. Bestämmelser för hur CE-märkningen ska fästas på produkter med digitala element bör fastställas i den här förordningen. CE-märkningen bör vara den enda märkning som garanterar överensstämmelse med kraven i den här förordningen för produkter med digitala element.

---

[29] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

(90) Det är nödvändigt att föreskriva förfaranden för bedömning av överensstämmelse, för att de ekonomiska aktörerna ska kunna visa överensstämmelse med de väsentliga cybersäkerhetskrav som anges i denna förordning och marknadskontrollmyndigheterna ska kunna säkerställa att de produkter med digitala element som tillhandahålls på marknaden uppfyller dessa krav. Genom Europaparlamentets och rådets beslut nr 768/2008/EG[30] fastställs moduler för bedömning av överensstämmelse som står i proportion till risknivån och den säkerhetsnivå som krävs. För att säkerställa enhetlighet mellan olika sektorer och undvika ad hoc-varianter bör förfarandena för bedömning av överensstämmelse för att kontrollera överensstämmelse med de väsentliga cybersäkerhetskraven i denna förordning för produkter med digitala element baseras på dessa moduler. Förfarandena för bedömning av överensstämmelse bör omfatta granskning och kontroll av både produkten och processrelaterade krav som omfattar hela livscykeln för produkter med digitala element, inbegripet planering, utformning, utveckling eller produktion, testning och underhåll av produkten med digitala element.

[30] Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG (EUT L 218, 13.8.2008, s. 82).

(91) Bedömningen av överensstämmelse för produkter med digitala element som inte förtecknas som viktiga eller kritiska produkter med digitala element i denna förordning kan utföras av tillverkaren på eget ansvar i enlighet med förfarandet för intern kontroll baserat på modul A i beslut nr 768/2008/EG i enlighet med denna förordning. Detta är också tillämpligt i fall där en tillverkare väljer att delvis eller inte alls tillämpa en tillämplig harmoniserad standard, gemensam specifikation eller en tillämplig europeisk ordning för cybersäkerhetscertifiering. Tillverkaren har även fortsättningsvis flexibilitet att välja ett striktare förfarande för bedömning av överensstämmelse som involverar tredje part. Inom ramen för det interna kontrollförfarandet för bedömning av överensstämmelse säkerställer och försäkrar tillverkaren på eget ansvar att produkten med digitala element och tillverkarens processer uppfyller de tillämpliga väsentliga cybersäkerhetskrav som fastställs i denna förordning. Om en viktig produkt med digitala element omfattas av klass I bör ytterligare kvalitetssäkring krävas för att visa överensstämmelsen med de väsentliga cybersäkerhetskraven i denna förordning. Tillverkaren bör tillämpa harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering antagna enligt förordning (EU) 2019/881 vilka har identifierats av kommissionen i en genomförandeakt, om den vill utföra bedömningen av överensstämmelse på eget ansvar (modul A). Om tillverkaren inte använder sådana harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering bör tillverkaren genomgå bedömning av överensstämmelse med deltagande av tredje part (baserat på modul B och C eller H). Med beaktande av den administrativa bördan för tillverkare och det faktum att cybersäkerheten har stor betydelse i utformnings- och utvecklingsfaserna för materiella och immateriella produkter med digitala element, har förfaranden för bedömning av överensstämmelse som baseras på modul B och C eller modul H i beslut nr 768/2008/EG valts som mest lämpliga för en proportionell och ändamålsenlig bedömning av överensstämmelse för viktiga produkter med digitala element.

Tillverkare som genomför en tredjepartsbedömning av överensstämmelse kan välja det förförande som bäst passar den egna utformnings- och produktionsprocessen. Med tanke på de allt större cybersäkerhetsrisker som är förbundna med användningen av viktiga produkter med digitala element som omfattas av klass II bör bedömningen av överensstämmelse alltid involvera en tredje part, även om produkten helt eller delvis överensstämmer med harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering. Tillverkare av viktiga produkter med digitala element, vilka kategoriseras som programvara med fri och öppen källkod, bör kunna följa förfarandet för intern kontroll baserat på modul A, förutsatt att de gör den tekniska dokumentationen tillgänglig för allmänheten.

(92) Medan skapandet av materiella produkter med digitala element vanligtvis innebär att tillverkaren måste göra stora ansträngningar under hela utformnings-, utvecklings- och produktionsfaserna, fokuserar skapandet av produkter med digitala element i form av programvara nästan uteslutande på utformning och utveckling, medan produktionsfasen är mindre framträdande. I många fall måste dock programvaruprodukter ändå kompileras, byggas, förpackas, göras tillgängliga för nedladdning eller kopieras till fysiska medier innan de släpps ut på marknaden. Dessa aktiviteter bör anses vara aktiviteter som motsvarar produktion vid tillämpningen av relevanta moduler för bedömning av överensstämmelse för att kontrollera överensstämmelsen med de väsentliga cybersäkerhetskrav som anges i denna förordning under hela utformnings-, utvecklings- och produktionsfaserna för produkter med digitala element.

(93) När det gäller mikroföretag och små företag bör, för att säkerställa proportionalitet, de administrativa kostnaderna minskas utan att påverka nivån av cybersäkerhetsskydd för produkter med digitala element som omfattas av denna förordnings tillämpningsområde, eller tillverkarnas lika spelregler. Det är därför lämpligt att kommissionen skapar ett förenklat formulär för teknisk dokumentation med inriktning på mikroföretags och små företags behov. Det förenklade formulär för teknisk dokumentation som antas av kommissionen bör omfatta alla tillämpliga delar av den tekniska dokumentation som anges i denna förordning och specificera hur ett mikroföretag eller ett småföretag kan tillhandahålla de begärda delarna på ett kortfattat sätt, såsom en beskrivning av utformningen, utvecklingen och produktionen av produkten med digitala element. På så sätt skulle formuläret bidra till att minska den administrativa regelbördan genom att ge de berörda företagen rättslig säkerhet om hur omfattande den information som ska lämnas ska vara och vilka uppgifter som ska ingå. Mikroföretag och små företag bör kunna välja att tillhandahålla tillämpliga delar som rör teknisk dokumentation i ett mer omfattande format och att inte använda det förenklade formulär som de har tillgång till.

(94) För att främja och skydda innovation är det viktigt att särskild hänsyn tas till intressena hos tillverkare som är mikroföretag eller små eller medelstora företag, särskilt mikroföretags och små företags, inbegripet uppstartsföretags. För detta ändamål skulle medlemsstaterna kunna utveckla initiativ som riktar sig till tillverkare som är mikroföretag eller små företag, inbegripet om utbildning, medvetandehöjande åtgärder, kommunikation, testning av information och tredjepartsbedömning av överensstämmelse, samt inrättande av sandlådor. Översättningskostnader för obligatorisk dokumentation, såsom den tekniska dokumentationen samt den information och de instruktioner till användaren som krävs enligt denna förordning, och kommunikation med myndigheter, kan innebära en betydande kostnad för tillverkarna, särskilt mindre tillverkare. Medlemsstaterna bör därför kunna anse att ett av de språk som fastställs och godtas av dem för relevant dokumentation från tillverkare och för kommunikation med tillverkare är ett språk som ett så stort antal användare som möjligt huvudsakligen förstår.

(95) För att tillämpningen av denna förordning ska fungera smidigt bör medlemsstaterna, före den dag då denna förordning börjar tillämpas, sträva efter att säkerställa att tillräckligt många anmälda organ finns tillgängliga för att tredjepartsbedömningar av överensstämmelse ska kunna utföras. Kommissionen bör sträva efter att hjälpa medlemsstaterna och andra berörda parter i detta arbete för att undvika flaskhalsar och hinder för marknadstillträde för tillverkare. Riktad utbildningsverksamhet som leds av medlemsstaterna, inbegripet när så är lämpligt med stöd av kommissionen, kan bidra till tillgången på kvalificerad arbetskraft, och även till att stödja de anmälda organens verksamhet enligt denna förordning. Med tanke på de kostnader som en tredjepartsbedömning av överensstämmelse kan medföra bör dessutom övervägas att finansiera initiativ på unionsnivå och nationell nivå som syftar till att minska sådana kostnader för mikroföretag och små företag.

(96) För att säkerställa proportionalitet bör organ för bedömning av överensstämmelse, när de fastställer avgifterna för bedömning av överensstämmelse, ta hänsyn till mikroföretags och små och medelstora företags, inbegripet uppstartsföretags, särskilda intressen och behov. I synnerhet bör organ för bedömning av överensstämmelse tillämpa det relevanta granskningsförfarande och den testning som föreskrivs i denna förordning endast när så är lämpligt och enligt en riskbaserad metod.

(97) Syftet med regulatoriska sandlådor bör vara att främja innovation och konkurrenskraft för företag genom att inrätta kontrollerade testmiljöer innan produkter med digitala element släpps ut på marknaden. Regulatoriska sandlådor bör bidra till att förbättra rättssäkerheten för alla aktörer som omfattas av denna förordning och underlätta och påskynda tillträdet till unionsmarknaden för produkter med digitala element, särskilt när de tillhandahålls av mikroföretag och små företag, inbegripet uppstartsföretag.

(98) För genomförandet av tredjepartsbedömningar av överensstämmelse för produkter med digitala element bör organ för bedömning av överensstämmelse anmälas av de nationella anmälande myndigheterna till kommissionen och övriga medlemsstater, under förutsättning att de uppfyller ett antal krav, i synnerhet vad gäller oberoende, kompetens och avsaknad av intressekonflikter.

(99) För att säkerställa en enhetlig kvalitetsnivå vid bedömning av överensstämmelse för produkter med digitala element måste också krav fastställas för de anmälande myndigheterna och andra organ som är involverade i bedömningen, anmälan och övervakningen av anmälda organ. Det system som fastställs i denna förordning bör kompletteras av ackrediteringssystemet enligt förordning (EG) nr 765/2008. Eftersom ackreditering är ett oumbärligt verktyg för att kontrollera kompetensen hos organen för bedömning av överensstämmelse bör det också användas för anmälningssyften.

(100) Organ för bedömning av överensstämmelse som har ackrediterats och anmälts enligt unionsrätten och som fastställer krav som liknar dem som fastställs i denna förordning, såsom ett organ för bedömning av överensstämmelse som har anmälts för en europeisk ordning för cybersäkerhetscertifiering vilken antagits enligt förordning (EU) 2019/881 eller som har anmälts enligt delegerad förordning (EU) 2022/30, bör bedömas på nytt och anmälas enligt den här förordningen. Synergier kan dock identifieras av relevanta myndigheter när det gäller överlappande krav för att förhindra en onödig ekonomisk och administrativ börda och säkerställa en smidig och snabb anmälningsprocess.

(101) De nationella offentliga myndigheterna inom unionen bör betrakta öppen ackreditering som föreskrivs i förordning (EG) nr 765/2008 som det bästa sättet att styrka den tekniska kompetensen hos organen för bedömning av överensstämmelse, för att säkerställa den nödvändiga nivån av förtroendet för intyg om överensstämmelse. Nationella myndigheter kan emellertid anse att de har tillräckliga möjligheter att utföra bedömningen på egen hand. I så fall bör de nationella myndigheterna, för att trygga en rimlig trovärdighetsnivå på bedömningar utförda av andra nationella myndigheter, tillhandahålla den dokumentation som krävs för att visa kommissionen och övriga medlemsstater att de utvärderade organen för bedömning av överensstämmelse uppfyller de relevanta kraven.

(102) Organ för bedömning av överensstämmelse lägger ofta ut verksamhet kopplad till bedömningen av överensstämmelse på underentreprenad eller anlitar ett dotterbolag. För att se till att den erforderliga skyddsnivån uppfylls för en produkt med digitala element som ska släppas ut på marknaden är det avgörande att underentreprenörer och dotterbolag uppfyller samma krav som de anmälda organen i fråga om utförandet av bedömning av överensstämmelse.

(103) Den anmälande myndigheten bör sända anmälan av ett organ för bedömning av överensstämmelse till kommissionen och övriga medlemsstater via databasen Nando. Databasen Nando är det elektroniska anmälningsverktyg som utvecklas och förvaltas av kommissionen och där en förteckning kan hittas över alla anmälda organ.

(104) Eftersom de anmälda organen får erbjuda sina tjänster i hela unionen är det lämpligt att medlemsstaterna och kommissionen bereds tillfälle att göra invändningar rörande ett anmält organ. Därför är det viktigt att en period fastställs under vilken eventuellt tvivel eller osäkerhet om kompetensen hos organen för bedömning av överensstämmelse kan redas ut innan de börjar fungera som anmälda organ.

(105) Av konkurrensskäl är det av avgörande betydelse att de anmälda organen tillämpar förfarandena för bedömning av överensstämmelse utan att belasta de ekonomiska aktörerna i onödan. Av samma skäl och för att säkerställa likabehandling av de ekonomiska aktörerna måste en enhetlig teknisk tillämpning av förfarandena för bedömning av överensstämmelse säkerställas. Detta bör bäst uppnås genom lämplig samordning och lämpligt samarbete mellan de anmälda organen.

(106) Marknadskontroll är ett viktigt verktyg för att säkerställa en korrekt och enhetlig tillämpning av unionsrätten. Det är därför lämpligt att upprätta en rättslig ram för ett ändamålsenligt genomförande av marknadskontroll. De regler om unionens marknadskontroll och kontroll av produkter som förs in på unionsmarknaden som föreskrivs i förordning (EU) 2019/1020 är tillämpliga på produkter med digitala element som omfattas av den här förordningens tillämpningsområde.

(107) I enlighet med förordning (EU) 2019/1020 genomför en marknadskontrollmyndighet marknadskontroll på den medlemsstats territorium som har utsett den. Den här förordningen bör inte förhindra medlemsstaterna att välja vilka behöriga myndigheter som ska utföra marknadskontroll. Varje medlemsstat bör utse en eller flera marknadskontrollmyndigheter på sitt territorium. Medlemsstaterna bör kunna välja att utse en befintlig eller en ny myndighet till att fungera som marknadskontrollmyndighet, inbegripet behöriga myndigheter utsedda eller inrättade enligt artikel 8 i direktiv (EU) 2022/2555, nationella myndigheter för cybersäkerhetscertifiering utsedda enligt artikel 58 i förordning (EU) 2019/881 eller marknadskontrollmyndigheter utsedda enligt direktiv 2014/53/EU. De ekonomiska aktörerna ska samarbeta fullt ut med marknadskontrollmyndigheterna och andra behöriga myndigheter. Varje medlemsstat bör underrätta kommissionen och övriga medlemsstater om sina marknadskontrollmyndigheter och behörighetsområdena för varje sådan myndighet och bör säkerställa de resurser och kompetenser som dessa behöver för att utföra sina marknadskontrolluppgifter enligt denna förordning. Enligt artikel 10.2 och 10.3 i förordning (EU) 2019/1020 bör varje medlemsstat tillsätta ett centralt samordningskontor som bland annat ska ansvara för att representera en samordnad ståndpunkt från marknadskontrollmyndigheterna och bistå i samarbetet mellan marknadskontrollmyndigheterna i olika medlemsstater.

(108) En särskild Adco-grupp för cyberresiliens hos produkter med digitala element bör inrättas för en enhetlig tillämpning av denna förordning, enligt artikel 30.2 i förordning (EU) 2019/1020. En Adco-grupp bör bestå av representanter för de nationella marknadskontrollmyndigheterna och, om så är lämpligt, representanter för de centrala samordningskontoren. Kommissionen bör stödja och uppmuntra samarbete mellan marknadskontrollmyndigheter genom unionsnätverket för produktöverensstämmelse, som inrättats enligt artikel 29 i förordning (EU) 2019/1020 och som består av representanter från varje medlemsstat, inbegripet en representant för varje centralt samordningskontor som avses i artikel 10 i den förordningen och en valfri nationell expert, ordförandena för Adco-grupperna och representanter för kommissionen. Kommissionen bör delta i möten i unionsnätverket för produktöverensstämmelse, och i dess undergruppers och Adco-gruppers möten. Den bör också bistå Adco-grupper genom ett verkställande sekretariat som tillhandahåller tekniskt och logistiskt stöd. En Adco-grupp får också bjuda in oberoende experter att delta och samarbeta med andra Adco-grupper, såsom den som inrättats enligt direktiv 2014/53/EU.

(109) Marknadskontrollmyndigheterna bör, genom Adco-grupper som inrättas enligt denna förordning, ha ett nära samarbete och bör kunna utarbeta vägledningsdokument för att underlätta marknadskontroller på nationell nivå, till exempel genom att utveckla bästa praxis och indikatorer för att effektivt kontrollera att produkter med digitala element överensstämmer med denna förordning.

(110) För att säkerställa att proportionella och effektiva åtgärder vidtas i rätt tid när det gäller produkter med digitala element som utgör en betydande cybersäkerhetsrisk bör ett unionsförfarande för skyddsåtgärder som innebär att berörda parter underrättas om åtgärder som är planerade att vidtas för sådana produkter erbjudas. På så sätt bör också marknadskontrollmyndigheterna få möjlighet att, i samarbete med de berörda ekonomiska aktörerna, agera i ett tidigare skede när det är nödvändigt. Om medlemsstaterna och kommissionen är överens om att en medlemsstats åtgärd är berättigad, bör kommissionen inte involveras ytterligare, utom i de fall då den bristande överensstämmelsen kan anses bero på brister i en harmoniserad standard.

(111) I vissa fall kan en produkt med digitala element som uppfyller kraven i denna förordning ändå utgöra en betydande cybersäkerhetsrisk eller utgöra en risk för människors hälsa eller säkerhet, för uppfyllandet av skyldigheter enligt sådan unionsrätt eller nationell rätt som är avsedd att skydda grundläggande rättigheter, tillgången till och autenticiteten, riktigheten eller konfidentialiteten för tjänster som väsentliga entiteter av den typ som avses i artikel 3.1 i direktiv (EU) 2022/2555 erbjuder med användning av ett elektroniskt informationssystem eller för andra aspekter av skyddet av allmänintresset. Därför är det nödvändigt att fastställa regler som säkerställer att dessa risker minskas. Följaktligen bör marknadskontrollmyndigheterna vidta åtgärder för att ålägga den ekonomiska aktören att säkerställa att produkten inte längre utgör en sådan risk, eller att återkalla eller dra tillbaka den, beroende på risken. Så snart en marknadskontrollmyndighet begränsar eller förbjuder den fria rörligheten för en produkt med digitala element på detta sätt bör medlemsstaten utan dröjsmål underrätta kommissionen och övriga medlemsstater om de provisoriska åtgärderna och motivera sitt beslut. Om en marknadskontrollmyndighet antar sådana åtgärder mot produkter med digitala element som utgör en risk bör kommissionen utan dröjsmål inleda samråd med medlemsstaterna och berörda ekonomiska aktörer (en eller flera) samt utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten bör kommissionen fastställa om den nationella åtgärden är motiverad eller inte. Kommissionen bör rikta beslutet till alla medlemsstater och omedelbart delge dem och de berörda ekonomiska aktörerna beslutet. Om åtgärden anses vara berättigad bör kommissionen också överväga att anta förslag om översyn av relevant unionsrätt.

(112) För produkter med digitala element som utgör en betydande cybersäkerhetsrisk, där det finns skäl att tro att de inte uppfyller kraven i denna förordning, eller för produkter som uppfyller kraven i denna förordning men som utgör andra viktiga risker, exempelvis risker för människors hälsa eller säkerhet, för uppfyllandet av skyldigheter enligt sådan unionsrätt eller nationell rätt som är avsedd att skydda grundläggande rättigheter eller för tillgången till och autenticiteten, riktigheten eller konfidentialiteten för tjänster som väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555 erbjuder med användning av ett elektroniskt informationssystem, bör kommissionen kunna begära att Enisa gör en utvärdering. Baserat på denna utvärdering bör kommissionen genom genomförandeakter kunna vidta korrigerande eller begränsande åtgärder på unionsnivå, inbegripet kräva att de berörda produkterna med digitala element dras tillbaka eller återkallas från marknaden, inom en rimlig tid i förhållande till typen av risk. Kommissionen bör endast kunna tillgripa en sådan åtgärd under exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en korrekt fungerande inre marknad och endast när inga verkningsfulla åtgärder har vidtagits av marknadskontrollmyndigheterna för att åtgärda situationen. Sådana exceptionella omständigheter kan vara akutsituationer där exempelvis en tillverkare gör en produkt med digitala element som inte uppfyller kraven allmänt tillgänglig i flera medlemsstater och den även används i nyckelsektorer av entiteter som omfattas av direktiv (EU) 2022/2555, och produkten samtidigt innehåller kända sårbarheter som utnyttjas av fientliga aktörer utan att tillverkaren tillhandahåller tillgängliga programfixar. Kommissionen bör vid sådana akutsituationer kunna ingripa endast under den tid som de exceptionella omständigheterna varar och om bristande överensstämmelse med denna förordning eller de betydande riskerna kvarstår.

(113) Om det finns indikationer på bristande överensstämmelse med denna förordning i flera medlemsstater bör marknadskontrollmyndigheterna kunna genomföra gemensamma åtgärder med andra myndigheter för att kontrollera överensstämmelsen och identifiera cybersäkerhetsrisker för produkter med digitala element.

(114) Samtidiga samordnade kontrollåtgärder (sweeps) är särskilda kontrollåtgärder som vidtas av marknadskontrollmyndigheterna och som kan förbättra produktsäkerheten ytterligare. Dessa samordnade kontrollåtgärder bör i synnerhet vidtas när det finns marknadstrender, klagomål från konsumenter eller andra indikationer som tyder på att vissa kategorier av produkter med digitala element ofta utgör cybersäkerhetsrisker. När marknadskontrollmyndigheterna fastställer vilka produktkategorier som ska omfattas av sweeps bör de också beakta omständigheter som rör icke-tekniska riskfaktorer. I detta syfte bör marknadskontrollmyndigheterna kunna ta hänsyn till resultaten av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor på unionsnivå som genomförs i enlighet med artikel 22 i direktiv (EU) 2022/2555, inbegripet omständigheter som rör icke-tekniska riskfaktorer. Enisa bör lämna förslag till marknadskontrollmyndigheterna på kategorier av produkter med digitala element som kan omfattas av samtidiga samordnade kontrollåtgärder, baserat på bland annat de anmälningar om sårbarheter och incidenter som inkommer till Enisa.

(115) Med tanke på Enisas sakkunskaper och uppdrag bör Enisa kunna stödja processen för genomförande av denna förordning. Enisa bör i synnerhet kunna föreslå gemensamma åtgärder som ska vidtas av marknadskontrollmyndigheter i flera medlemsstater på grundval av indikationer eller information om potentiell bristande överensstämmelse med denna förordning för produkter med digitala element eller identifiera produktkategorier där samtidiga sweeps bör organiseras. Under exceptionella omständigheter bör Enisa, på kommissionens begäran, kunna göra utvärderingar av specifika produkter med digitala element som utgör en betydande cybersäkerhetsrisk, när ett omedelbart ingripande krävs för att bevara en korrekt fungerande inre marknad.

(116) Genom denna förordning tilldelas Enisa vissa uppgifter som kräver lämpliga resurser i fråga om både sakkunskap och personal för att Enisa ska kunna utföra dessa uppgifter på ett ändamålsenligt sätt. Kommissionen kommer att föreslå nödvändiga budgetmedel för Enisas tjänsteförteckning, i enlighet med förfarandet som anges i artikel 29 i förordning (EU) 2019/881, vid utarbetandet av förslaget till unionens allmänna budget. Under den processen kommer kommissionen att beakta Enisas övergripande resurser för att den ska kunna fullgöra sina uppgifter, inbegripet dem som tilldelats Enisa enligt den här förordningen.

(117) I syfte att säkerställa att regelverket vid behov kan anpassas bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) delegeras till kommissionen med avseende på uppdatering av en bilaga till denna förordning med förteckningen över viktiga produkter med digitala element. Befogenheten att anta akter i enlighet med den artikeln bör delegeras till kommissionen för att identifiera produkter med digitala element som omfattas av andra unionsregler som ger samma skyddsnivå som denna förordning och specificera om det skulle vara nödvändigt med några begränsningar eller uteslutanden från denna förordnings tillämpningsområde samt specificera sådana begränsningars omfattning, i tillämpliga fall. Befogenheten att anta akter i enlighet med den artikeln bör också delegeras till kommissionen med avseende på det potentiella kravet på certifiering enligt en europeisk ordning för cybersäkerhetscertifiering av kritiska produkter med digitala element som anges i en bilaga till denna förordning, liksom för att uppdatera förteckningen över kritiska produkter med digitala element baserat på kritikalitetskriterier som fastställs i denna förordning, samt för att specificera de europeiska ordningarna för cybersäkerhetscertifiering som antagits enligt förordning (EU) 2019/881 och som kan användas för att visa överensstämmelse med de väsentliga cybersäkerhetskrav eller delar av dem som fastställs i en bilaga till den här förordningen. Befogenheten att anta akter bör också delegeras till kommissionen för att specificera minsta tillåtna stödperioder för specifika produktkategorier om marknadskontrolluppgifter tyder på otillräckliga stödperioder, samt för att specificera villkoren för att tillämpa cybersäkerhetsrelaterade skäl när det gäller att skjuta upp spridningen av anmälningar om aktivt utnyttjade sårbarheter.

Dessutom bör befogenheten att anta akter delegeras till kommissionen för att inrätta frivilliga program för säkerhetsintyg i syfte att bedöma överensstämmelse för produkter med digitala element som kategoriseras som programvara med fri och öppen källkod, med alla eller vissa väsentliga cybersäkerhetskrav eller andra skyldigheter som fastställs i denna förordning, samt för att specificera minimiinnehållet i EU-försäkran om överensstämmelse och i syfte att komplettera de aspekter som ska ingå i den tekniska dokumentationen. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning[31]. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter. Befogenheten att anta delegerade akter i enlighet med denna förordning bör delegeras till kommissionen för en period på fem år från och med den… [den dag då denna förordning träder i kraft]. Kommissionen bör utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet bör genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

[31] EUT L 123, 12.5.2016, s. 1.

(118) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter för att specificera den tekniska beskrivning av de kategorier av viktiga produkter med digitala element som anges i en bilaga till denna förordning, specificera formatet för och vad som ska ingå i programvaruförteckningen, ytterligare specificera formatet och förfarandet för de anmälningar om aktivt utnyttjade sårbarheter och allvarliga incidenter som påverkar säkerheten för produkter med digitala element, vilka lämnats in av tillverkarna, fastställa gemensamma specifikationer som omfattar tekniska krav vilka tillhandahåller ett sätt att uppfylla de väsentliga cybersäkerhetskrav som fastställs i en bilaga till denna förordning, fastställa tekniska specifikationer för etiketter, piktogram eller andra märkningar relaterade till säkerheten för produkter med digitala element, deras stödperiod och mekanismer för att främja användningen av sådana och öka allmänhetens medvetenhet om säkerheten för produkter med digitala element, specificera det förenklade formuläret för teknisk dokumentation med inriktning på mikroföretags och små företags behov, samt besluta om korrigerande eller begränsande åtgärder på unionsnivå vid exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en korrekt fungerande inre marknad. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[32].

(119) För att säkerställa ett konstruktivt samarbete präglat av förtroende mellan marknadskontrollmyndigheter på unionsnivå och nationell nivå bör alla parter som är involverade i tillämpningen av denna förordning respektera konfidentialiteten för information och data som de erhåller i utförandet av sina uppgifter.

---

[32] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(120) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i denna förordning bör varje marknadskontrollmyndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter. Det bör därför fastställas maxnivåer för administrativa sanktionsavgifter som kommer att föreskrivas i nationell rätt med avseende på bristande uppfyllande av de skyldigheter som fastställs i denna förordning. När det administrativa sanktionsbeloppet fastställs i varje enskilt fall bör alla relevanta omständigheter i den specifika situationen beaktas och som ett minimum de som uttryckligen fastställs i denna förordning, inbegripet huruvida tillverkaren är ett mikroföretag eller ett småföretag eller medelstort företag, inbegripet ett uppstartsföretag, och huruvida samma eller andra marknadskontrollmyndigheter redan har påfört samma ekonomiska aktör administrativa sanktionsavgifter för en liknande överträdelse. Sådana omständigheter skulle kunna vara antingen försvårande, i situationer där samma ekonomiska aktörs överträdelse fortsätter på territoriet för andra medlemsstater än den där den administrativa sanktionsavgiften redan har påförts, eller förmildrande, genom att säkerställa att eventuella administrativa sanktionsavgifter som övervägs av en annan marknadskontrollmyndighet för samma ekonomiska aktör eller samma typ av överträdelse redan bör beakta sanktioner som påförts i andra medlemsstater och storleken på dessa, tillsammans med andra relevanta särskilda omständigheter. I samtliga fall bör den kumulativa administrativa sanktionsavgift som marknadskontrollmyndigheter i flera medlemsstater kan påföra samma ekonomiska aktör för samma typ av överträdelse fastställas med iakttagande av proportionalitetsprincipen. Med tanke på att administrativa sanktionsavgifter inte tillämpas på mikroföretag eller små företag för en underlåtenhet att iaktta tidsfristen på 24 timmar avseende en tidig varning om aktivt utnyttjade sårbarheter eller allvarliga incidenter som påverkar säkerheten för produkten med digitala element, och inte heller på förvaltare av programvara med fri och öppen källkod för någon överträdelse av denna förordning, och med förbehåll för principen om att sanktioner bör vara effektiva, proportionella och avskräckande, bör medlemsstaterna inte ålägga dessa enheter andra typer av sanktioner av ekonomisk karaktär.

(121) Om administrativa sanktionsavgifter påförs en person som inte är ett företag, bör den behöriga myndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Det bör vara upp till medlemsstaterna att fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter.

(122) Medlemsstaterna bör, med beaktande av nationella omständigheter, undersöka möjligheten att använda intäkterna från de sanktioner som föreskrivs i denna förordning eller deras ekonomiska motsvarighet till att stödja cybersäkerhetsstrategier och öka cybersäkerhetsnivån i unionen genom att bland annat öka antalet kvalificerade yrkesverksamma inom cybersäkerhet, stärka kapacitetsuppbyggnaden för mikroföretag samt små och medelstora företag och förbättra allmänhetens medvetenhet om cyberhot.

(123) I sina förbindelser med tredjeländer strävar unionen efter att främja internationell handel med reglerade produkter. En mängd olika åtgärder kan vidtas för att främja handel, inbegripet flera rättsliga instrument såsom bilaterala (mellanstatliga) avtal om ömsesidigt erkännande (MRA) av bedömning av överensstämmelse och märkning av reglerade produkter. Avtal om ömsesidigt erkännande upprättas mellan unionen och tredjeländer som är på jämförbar teknisk utvecklingsnivå och har en jämförbar strategi för bedömning av överensstämmelse. Dessa avtal baseras på ett ömsesidigt godtagande av intyg, märkning om överensstämmelse och provningsrapporter som utfärdats av parternas organ för bedömning av överensstämmelse enligt varje parts lagstiftning. I dagsläget finns MRA med flera tredjeländer. Dessa MRA ingås för ett antal specifika sektorer, som kan variera från ett tredjeland till ett annat. För att ytterligare främja handel, och med beaktande av att leveranskedjorna för produkter med digitala element är globala, kan MRA om ömsesidigt erkännande av bedömning av överensstämmelse ingås av unionen i enlighet med artikel 218 i EUF-fördraget för produkter som regleras enligt denna förordning. Samarbete med partnertredjeländer är också viktigt, för att stärka cyberresiliensen globalt, eftersom det långsiktigt kommer att bidra till att stärka cybersäkerhetsramen både inom och utanför unionen.

(124) Konsumenter bör ha rätt att hävda sina rättigheter med avseende på de skyldigheter som åläggs ekonomiska aktörer enligt denna förordning genom grupptalan enligt Europaparlamentets och rådets direktiv (EU) 2020/1828[33]. För detta ändamål bör det i denna förordning föreskrivas att direktiv (EU) 2020/1828 är tillämpligt på grupptalan om överträdelser av denna förordning som skadar eller kan skada konsumenters kollektiva intressen. Bilaga I till det direktivet bör därför ändras i enlighet med detta. Det åligger medlemsstaterna att säkerställa att dessa ändringar återspeglas i de införlivandeåtgärder som antas enligt det direktivet, även om antagandet av nationella införlivandeåtgärder i det avseendet inte är ett villkor för att det direktivet ska vara tillämpligt på sådan grupptalan. Det direktivets tillämplighet på grupptalan som väcks med avseende på ekonomiska aktörers överträdelser av bestämmelser i denna förordning som skadar eller skulle kunna skada konsumenters kollektiva intressen bör börja tillämpas från och med den … [36 månader från den dag då denna förordning träder i kraft].

(125) Denna förordning bör med jämna mellanrum utvärderas och ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra behovet av ändringar mot bakgrund av samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor. Denna förordning kommer att underlätta för entiteter som omfattas av förordning (EU) 2022/2554 och direktiv (EU) 2022/2555 och som använder produkter med digitala element att fullgöra skyldigheterna avseende säkerhet i leveranskedjan. Kommissionen bör, som en del av den regelbundna översynen, utvärdera de kombinerade effekterna av unionens cybersäkerhetsram.

---

[33] Europaparlamentets och rådets direktiv (EU) 2020/1828 av den 25 november 2020 om grupptalan för att skydda konsumenters kollektiva intressen och om upphävande av direktiv 2009/22/EG (EUT L 409, 4.12.2020, s. 1).

(126) De ekonomiska aktörerna bör ges tillräckligt med tid att anpassa sig till de krav som anges i denna förordning. Förordningen bör tillämpas från och med den … [36 månader från den dag då denna förordning träder i kraft], förutom skyldigheten att rapportera aktivt utnyttjade sårbarheter och allvarliga incidenter som påverkar säkerheten för produkten med digitala element, som bör börja tillämpas från och med den…[21 månader från den dag då denna förordning träder i kraft] och bestämmelserna om anmälan av organ för bedömning av överensstämmelse som bör tillämpas från och med den … [18 månader från den dag då denna förordning träder i kraft].

(127) Det är viktigt att ge stöd till mikroföretag samt små och medelstora företag, inbegripet uppstartsföretag, vid genomförandet av denna förordning och att begränsa de risker i samband med genomförandet som följer av bristande kunskap och expertis på marknaden, samt att underlätta för tillverkarna att fullgöra sina skyldigheter enligt denna förordning. Programmet för ett digitalt Europa och andra relevanta unionsprogram tillhandahåller ekonomiskt och tekniskt stöd som gör att dessa företag kan bidra till tillväxten i unionens ekonomi och till en stärkt gemensam cybersäkerhetsnivå i unionen. Europeiska kompetenscentrumet för cybersäkerhet och nationella samordningscentrum samt europeiska digitala innovationsknutpunkter som inrättas av kommissionen och medlemsstaterna på unionsnivå eller nationell nivå skulle också kunna stödja företag och organisationer inom den offentliga sektorn och bidra till genomförandet av denna förordning. Inom ramen för sina respektive uppdrag och ansvarsområden skulle de kunna ge tekniskt och vetenskapligt stöd till mikroföretag samt små och medelstora företag, till exempel för testningsverksamhet och tredjepartsbedömningar av överensstämmelse. De skulle också kunna främja användningen av verktyg för att underlätta genomförandet av denna förordning.

(128) Dessutom bör medlemsstaterna överväga kompletterande åtgärder som syftar till att ge vägledning och stöd till mikroföretag samt små och medelstora företag, såsom att inrätta regulatoriska sandlådor och särskilda kanaler för kommunikation. För att stärka cybersäkerhetsnivån i unionen får medlemsstaterna också överväga att tillhandahålla stöd för att utveckla kapacitet och färdigheter med anknytning till cybersäkerhet för produkter med digitala element, förbättra ekonomiska aktörers cyberresiliens, särskilt för mikroföretag samt små och medelstora företag, och främja allmänhetens medvetenhet om cybersäkerheten för produkter med digitala element.

(129) Eftersom målet för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(130) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725[34] och avgav ett yttrande den 9 november 2022[35].

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

---

[34] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

[35] EUT C 452, 29.11.2022, s. 23.

Kapitel I
Allmänna bestämmelser

Artikel 1
Innehåll

I denna förordning fastställs

a) regler för tillhandahållande på marknaden av produkter med digitala element, för att säkerställa cybersäkerheten för sådana produkter,

b) väsentliga cybersäkerhetskrav för utformningen, utvecklingen och tillverkningen av produkter med digitala element, och skyldigheter för ekonomiska aktörer när det gäller cybersäkerheten för dessa produkter,

c) väsentliga cybersäkerhetskrav för de processer för sårbarhetshantering som tillverkarna inför för att säkerställa cybersäkerheten för produkter med digitala element under den tid som produkterna förväntas vara i bruk samt skyldigheter för ekonomiska aktörer i samband med dessa processer, och

d) regler om marknadskontroll, inbegripet övervakning, och kontroll av efterlevnaden av de regler och krav som avses i denna artikel.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på alla produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät.

2. Förordningen är inte tillämplig på sådana produkter med digitala element som omfattas av följande unionsrättsakter:

   a) Förordning (EU) 2017/745.

   b) Förordning (EU) 2017/746.

   c) Förordning (EU) 2019/2144.

3. Denna förordning ska inte tillämpas på produkter med digitala element som har certifierats i enlighet med förordning (EU) 2018/1139.

4. Denna förordning ska inte tillämpas på utrustning som omfattas av Europaparlamentets och rådets direktiv 2014/90/EU[36].

[36] Europaparlamentets och rådets direktiv 2014/90/EU av den 23 juli 2014 om marin utrustning och om upphävande av rådets direktiv 96/98/EG (EUT L 257, 28.8.2014, s. 146).

5. Denna förordnings tillämpning på produkter med digitala element som omfattas av andra unionsregler där krav fastställs avseende alla eller vissa risker som täcks av de väsentliga cybersäkerhetskraven i bilaga I får begränsas eller undantas om

   a) sådana begränsningar eller undantag är förenliga med den allmänna rättsliga ram som är tillämplig på dessa produkter, och

   b) sektorsreglerna ger samma eller en högre skyddsnivå än den som föreskrivs i denna förordning.

   Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att specificera om sådana begränsningar eller undantag är nödvändiga, vilka produkter och regler som berörs samt begränsningens omfattning, i förekommande fall.

6. Denna förordning ska inte tillämpas på reservdelar som tillhandahålls på marknaden för att ersätta identiska komponenter i produkter med digitala element och som tillverkas enligt samma specifikationer som de komponenter som de är avsedda att ersätta.

7. Denna förordning ska inte tillämpas på produkter med digitala element som utvecklats eller ändrats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.

8. De skyldigheter som fastställs i denna förordning får inte medföra tillhandahållande av information vars utlämnande skulle strida mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *produkt med digitala element*: programvaru- eller hårdvaruprodukt och dess lösningar för fjärrbehandling av data, inbegripet programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat.

2. *fjärrbehandling av data*: databehandling på distans för vilken programvaran utformats och utvecklats av tillverkaren eller under tillverkarens ansvar, och vars avsaknad skulle innebära att produkten med digitala element inte kan utföra en av sina funktioner.

3. *cybersäkerhet*: cybersäkerhet enligt definitionen i artikel 2.1 i förordning (EU) 2019/881.

4. *programvara*: den del av ett elektroniskt informationssystem som utgörs av datorkod.

5. *hårdvara*: ett fysiskt elektroniskt informationssystem, eller delar av ett sådant, som kan behandla, lagra eller överföra digitala data.

6. *komponent*: programvara eller hårdvara som är avsedd att vara integrerad i ett elektroniskt informationssystem.

7. *elektroniskt informationssystem*: ett system, inklusive elektrisk eller elektronisk utrustning, som kan behandla, lagra eller överföra digitala data.

8. *logisk anslutning*: en virtuell representation av en dataförbindelse som genomförs via ett programvarugränssnitt.

9. *fysisk anslutning*: en anslutning mellan elektroniska informationssystem eller komponenter som genomförs med fysiska medel, inbegripet elektriska, optiska eller mekaniska gränssnitt, tråd eller radiovågor.

10. *indirekt anslutning*: en anslutning till en enhet eller ett nät som inte sker direkt utan snarare som en del av ett större system som är direkt anslutningsbart till enheten eller nätet.

11. *slutnod*: enhet som är ansluten till ett nät och som tjänar som ingångspunkt till det nätet.

12. *ekonomisk aktör*: tillverkaren, tillverkarens representant, importören, distributören eller en annan fysisk eller juridisk person som omfattas av skyldigheter avseende tillverkning av produkter med digitala element eller avseende tillhandahållande av produkter med digitala element på marknaden i enlighet med denna förordning.

13. *tillverkare*: en fysisk eller juridisk person som utvecklar eller tillverkar produkter med digitala element, eller som låter utforma, utveckla eller tillverka produkter med digitala element, och saluför dessa under eget namn eller varumärke, vare sig mot betalning, för monetarisering eller kostnadsfritt.

14. *förvaltare av programvara med fri och öppen källkod*: en juridisk person, annan än en tillverkare, som har till syfte eller som mål att systematiskt och varaktigt tillhandahålla stöd för utvecklingen av specifika produkter med digitala element, vilka klassificeras som programvara med fri och öppen källkod och är avsedda för kommersiell verksamhet, och som säkerställer dessa produkters bärkraft.

15. *tillverkarens representant:* en fysisk eller juridisk person som är etablerad i unionen och som enligt skriftlig fullmakt från en tillverkare har rätt att i tillverkaren ställe utföra särskilda uppgifter.

16. *importör*: en fysisk eller juridisk person som är etablerad i unionen och som på marknaden släpper ut en produkt med digitala element vilken bär namnet på eller varumärket för en fysisk eller juridisk person som är etablerad utanför unionen.

17. *distributör*: en fysisk eller juridisk person i leveranskedjan, utöver tillverkaren eller importören, som tillhandahåller en produkt med digitala element på unionsmarknaden utan att påverka dess egenskaper.

18. *konsument*: en fysisk person som agerar för ändamål som faller utanför den personens näringsverksamhet, affärsverksamhet, hantverk eller yrke.

19. *mikroföretag, små företag* och *medelstora företag:* mikroföretag, små företag och medelstora företag enligt definitionen i bilagan till rekommendation 2003/361/EG.

20. *stödperiod*: den period under vilken en tillverkare måste säkerställa att sårbarheter hos en produkt med digitala element hanteras ändamålsenligt och i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.

21. *utsläppande på marknaden*: tillhandahållande för första gången av en produkt med digitala element på unionsmarknaden.

22. *tillhandahållande på marknaden*: leverans av en produkt med digitala element för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, antingen mot betalning eller kostnadsfritt.

23. *avsett ändamål*: den användning för vilken en produkt med digitala element är avsedd av leverantören, inbegripet det specifika sammanhanget och de specifika användningsvillkoren, enligt specifikationerna i de uppgifter som leverantören tillhandahåller i instruktioner till användaren, reklam- eller försäljningsmaterial och uttalanden samt i den tekniska dokumentationen.

24. *rimligen förutsebar användning*: användning som inte nödvändigtvis är det avsedda ändamål som tillverkaren anger i instruktionerna till användaren, reklam- eller försäljningsmaterial och uttalanden eller i den tekniska dokumentationen, men som är den sannolika följden av rimligen förutsebart mänskligt beteende eller tekniska åtgärder eller interaktioner.

25. *rimligen förutsebar felaktig användning*: användning av en produkt med digitala element på ett sätt som inte överensstämmer med dess avsedda ändamål, men som kan vara resultatet av rimligen förutsebart mänskligt beteende eller interaktion med andra system.

26. *anmälande myndighet*: den nationella myndighet som ansvarar för inrättandet och genomförandet av de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa.

27. *bedömning av överensstämmelse*: processen där det kontrolleras om de väsentliga cybersäkerhetskraven i bilaga I har uppfyllts.

28. *organ för bedömning av överensstämmelse*: ett organ för bedömning av överensstämmelse enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008.

29. *anmält organ*: organ för bedömning av överensstämmelse som utsetts i enlighet med artikel 43 och annan relevant unionsharmoniseringslagstiftning.

30. *väsentlig ändring*: en ändring av produkten med digitala element efter dess utsläppande på marknaden, vilken påverkar produktens överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I del I eller leder till en ändring av det avsedda ändamål för vilket produkten har bedömts.

31. *CE-märkning*: märkning genom vilken en tillverkare anger att en produkt med digitala element och de processer som införts av tillverkaren överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I och annan tillämplig unionsharmoniseringslagstiftning som föreskriver att sådan märkning ska fästas.

32. *unionsharmoniseringslagstiftning*: unionslagstiftning som förtecknas i bilaga I till förordning (EU) 2019/1020 och all annan unionslagstiftning som harmoniserar villkoren för saluföring av produkter som omfattas av den förordningen.

33. *marknadskontrollmyndighet*: en marknadskontrollmyndighet enligt definitionen i artikel 3.4 i förordning (EU) 2019/1020.

34. *internationell standard*: en internationell standard enligt definitionen i artikel 2.1 a i förordning (EU) nr 1025/2012.

35. *europeisk standard*: en europeisk standard enligt definitionen i artikel 2.1 b i förordning (EU) nr 1025/2012.

36. *harmoniserad standard*: en harmoniserad standard enligt definitionen i artikel 2.1 c i förordning (EU) nr 1025/2012.

37. *cybersäkerhetsrisk:* risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att incidenten inträffar.

38. *betydande cybersäkerhetsrisk*: en cybersäkerhetsrisk som, baserat på dess tekniska egenskaper, kan antas innebära en hög sannolikhet för en incident som kan medföra allvarliga negativa konsekvenser, inbegripet genom att orsaka betydande materiell eller immateriell förlust eller störning.

39. *programvaruförteckning*: en formell förteckning med närmare uppgifter om och leveranskedjeförhållanden för komponenter som ingår i programvaruelementen i en produkt med digitala element.

40. *sårbarhet*: en svaghet, känslighet eller brist hos en produkt med digitala element som kan utnyttjas genom ett cyberhot.

41. *sårbarhet som kan utnyttjas*: en sårbarhet som kan utnyttjas effektivt av en motståndare under praktiska operativa förhållanden.

42. *aktivt utnyttjad sårbarhet*: en sårbarhet för vilken det finns tillförlitliga bevis på att en fientlig aktör har utnyttjat den i ett system utan tillstånd från systemets ägare.

43. *incident*: en incident enligt definitionen i artikel 6.6 i direktiv (EU) 2022/2555.

44. *incident som påverkar säkerheten för en produkt med digitala element:* en incident som inverkar negativt på eller kan inverka negativt på förmågan hos en produkt med digitala element att skydda tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten för data eller funktioner.

45. *tillbud*: ett tillbud enligt definitionen i artikel 6.5 i direktiv (EU) 2022/2555.

46. *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

47. *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

48. *programvara med fri och öppen källkod*: programvara vars källkod delas öppet och som tillhandahålls inom ramen för en licens med fri och öppen källkod som ger alla rättigheter att göra den fritt tillgänglig att användas, modifieras och vidaredistribueras.

49. *återkallelse*: återkallelse enligt definitionen i artikel 3.22 i förordning (EU) 2019/1020.

50. *tillbakadragande*: tillbakadragande enligt definitionen i artikel 3.23 i förordning (EU) 2019/1020.

51. *CSIRT-enhet som utsetts till samordnare*: en CSIRT-enhet som utsetts till samordnare enligt artikel 12.1 i direktiv (EU) 2022/2555.

Artikel 4

Fri rörlighet

1. Medlemsstaterna får inte, med hänvisning till aspekter som omfattas av denna förordning, hindra att produkter med digitala element som uppfyller kraven i denna förordning tillhandahålls på marknaden.

2. Medlemsstaterna får inte förhindra att sådana produkter med digitala element som inte uppfyller kraven i denna förordning visas eller används vid mässor, utställningar och demonstrationer eller liknande evenemang, inbegripet prototyper, förutsatt att produkten visas med en synlig märkning som tydligt anger att den inte uppfyller kraven i denna förordning och att den inte kommer att tillhandahållas på marknaden förrän den gör det.

3. Medlemsstaterna får inte förhindra att ej färdigställd programvara som inte uppfyller kraven i denna förordning tillhandahålls på marknaden, under förutsättning att programvaran tillhandahålls endast under den begränsade tid som krävs för testningsändamål och med en synlig märkning som tydligt anger att den inte uppfyller kraven i denna förordning och att den inte kommer att tillhandahållas på marknaden för andra ändamål än testning.

4. Punkt 3 ska inte tillämpas på säkerhetskomponenter enligt annan unionsharmoniseringslagstiftning än denna förordning.

Artikel 5

Upphandling eller användning av produkter med digitala element

1. Denna förordning ska inte hindra medlemsstaterna från att införa ytterligare cybersäkerhetskrav för produkter med digitala element när det gäller upphandling eller användning av dessa produkter för specifika ändamål, inbegripet när dessa produkter upphandlas eller används för ändamål som rör nationell säkerhet eller försvarsändamål, förutsatt att kraven är förenliga med medlemsstaternas skyldigheter enligt unionsrätten och att de är nödvändiga och proportionella för att uppnå dessa ändamål.

2. Utan att det påverkar tillämpningen av direktiven 2014/24/EU och 2014/25/EU ska medlemsstaterna, när produkter med digitala element som omfattas av denna förordnings tillämpningsområde upphandlas, säkerställa att överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I till denna förordning, inbegripet tillverkarnas förmåga att ändamålsenligt hantera sårbarheter, beaktas i upphandlingsprocessen.

Artikel 6

Krav för produkter med digitala element

Produkter med digitala element får tillhandahållas på marknaden endast om

a) de uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I, förutsatt att de är korrekt installerade och underhållna och används för avsett ändamål eller under förhållanden som rimligen kan förutses och, i tillämpliga fall, att de nödvändiga säkerhetsuppdateringarna har installerats, och

b) de processer som införs av tillverkaren uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.

Artikel 7

Viktiga produkter med digitala element

1. Produkter med digitala element som har kärnfunktionen hos en produktkategori som anges i bilaga III till denna förordning ska anses vara viktiga produkter med digitala element och ska omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 och 32.3. Integreringen av en produkt med digitala element som har kärnfunktionen hos en produktkategori som anges i bilaga III ska inte i sig medföra att den produkt i vilken den är integrerad omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 och 32.3.

2. De kategorier av produkter med digitala element som avses i punkt 1 i denna artikel, indelade i klasserna I och II enligt bilaga III, uppfyller minst ett av följande kriterier:

a) Produkten med digitala element utför i första hand funktioner som är kritiska för cybersäkerheten för andra produkter, nät eller tjänster, inbegripet säkerställande av autentisering och åtkomst, intrångsdetektion och intrångsskydd, säkerhet vid slutnoder eller nätskydd.

b) Produkten med digitala element utför en funktion som medför en betydande risk för negativa effekter i fråga om dess intensitet och förmåga att störa, kontrollera eller orsaka skada på ett stort antal andra produkter eller på användarnas hälsa, säkerhet eller skydd genom direkt manipulering, såsom en central systemfunktion, inbegripet nätförvaltning, konfigurationsstyrning, virtualisering eller behandling av personuppgifter.

3. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att ändra bilaga III genom att införa en ny kategori inom varje klass i förteckningen över kategorier av produkter med digitala element och specificera dess definition, flytta en kategori av produkter från en klass till en annan eller stryka en befintlig kategori från förteckningen. När kommissionen bedömer behovet av en ändring av förteckningen i bilaga III ska den ta hänsyn till de cybersäkerhetsrelaterade funktionerna eller funktionen och nivån på den cybersäkerhetsrisk som produkterna med digitala element utgör enligt de kriterier som avses i punkt 2 i den här artikeln.

De delegerade akter som avses i första stycket i denna punkt ska, när så är lämpligt, föreskriva en övergångsperiod på minst tolv månader, särskilt när en ny kategori av viktiga produkter med digitala element läggs till i klass I eller II eller flyttas från klass I till II enligt bilaga III, innan de relevanta förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 och 32.3 börjar tillämpas, såvida inte en kortare övergångsperiod är motiverad av tvingande skyndsamhetskäl.

4. Senast den … [tolv månader från den dag då denna förordning träder i kraft] ska kommissionen anta en genomförandeakt som specificerar den tekniska beskrivningen av kategorierna av produkter med digitala element i klasserna I och II enligt bilaga III och den tekniska beskrivningen av kategorierna av produkter med digitala element enligt bilaga IV. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

Artikel 8

Kritiska produkter med digitala element

1. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 med för att komplettera denna förordning för att fastställa vilka produkter med digitala element och med kärnfunktionen hos en produktkategori som anges i bilaga IV till denna förordning som ska erhålla ett europeiskt cybersäkerhetscertifikat på åtminstone assuransnivån ”betydande” enligt en europeisk ordning för cybersäkerhetscertifiering som antagits enligt förordning (EU) 2019/881 för att visa överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I till den här förordningen eller delar därav, förutsatt att en europeisk ordning för cybersäkerhetscertifiering som omfattar dessa kategorier av produkter med digitala element har antagits i enlighet med förordning (EU) 2019/881 och är tillgänglig för tillverkarna. Dessa delegerade akter ska specificera den assuransnivå som krävs, vilken ska stå i proportion till den nivå av cybersäkerhetsrisk som är förbunden med produkterna med digitala element och ska ta hänsyn till deras avsedda ändamål, inbegripet det kritiska beroendet av dem av väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555.

   Innan kommissionen antar sådana delegerade akter ska den göra en bedömning av de planerade åtgärdernas potentiella marknadseffekter och samråda med berörda parter, inbegripet den europeiska grupp för cybersäkerhetscertifiering som fastställs genom förordning (EU) 2019/881. Bedömningen ska ta hänsyn till medlemsstaternas beredskap och kapacitetsnivå när det gäller att genomföra den relevanta europeiska ordningen för cybersäkerhetscertifiering. Om inga delegerade akter som avses i första stycket i denna punkt har antagits ska produkter med digitala element och med kärnfunktionen hos en produktkategori som anges i bilaga IV omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.3.

De delegerade akter som avses i första stycket ska föreskriva en övergångsperiod på minst sex månader, såvida inte en kortare övergångsperiod är motiverad av tvingande skyndsamhetsskäl.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att ändra bilaga IV genom att lägga till eller stryka kategorier av produkter med digitala element. Vid fastställandet av sådana kategorier av kritiska produkter med digitala element och den assuransnivå som krävs, i enlighet med punkt 1 i den här artikeln, ska kommissionen beakta de kriterier som avses i artikel 7.2 och säkerställa att kategorierna av produkter med digitala element uppfyller minst ett av följande kriterier:

a) Väsentliga entiteter som avses i artikel 3 i direktiv (EU) 2022/2555 har ett kritiskt beroende av kategorin av produkter med digitala element.

b) Incidenter och utnyttjade sårbarheter som rör kategorin av produkter med digitala element kan leda till allvarliga störningar i kritiska leveranskedjor på den inre marknaden.

Innan kommissionen antar sådana delegerade akter ska den göra en bedömning av den typ som avses i punkt 1.

De delegerade akter som avses i första stycket ska föreskriva en övergångsperiod på minst sex månader, såvida inte en kortare övergångsperiod är motiverad av tvingande skyndsamhetsskäl.

Artikel 9

Samråd med berörda parter

1. När kommissionen utarbetar åtgärder för genomförandet av denna förordning ska den samråda med och beakta synpunkter från berörda parter, såsom berörda myndigheter i medlemsstaterna, företag i den privata sektorn, inbegripet mikroföretag och små och medelstora företag, gemenskapen för programvara med fri och öppen källkod, konsumentorganisationer, den akademiska världen och relevanta unionsbyråer och unionsorgan samt expertgrupper som inrättats på unionsnivå. I synnerhet ska kommissionen på ett strukturerat sätt, när så är lämpligt, samråda med och inhämta synpunkter från dessa berörda parter när den

   a) utarbetar den vägledning som avses i artikel 26,

   b) utarbetar de tekniska beskrivningarna av de produktkategorier som anges i bilaga III i enlighet med artikel 7.4, bedömer behovet av eventuella uppdateringar av förteckningen över produktkategorier i enlighet med artiklarna 7.3 och 8.2 eller genomför den bedömning av potentiella marknadseffekter som avses i artikel 8.1, utan att det påverkar tillämpningen av artikel 61,

   c) gör förberedande arbete inför utvärderingen och översynen av denna förordning.

2. Kommissionen ska anordna regelbundna samråd och informationsmöten, minst en gång om året, för att inhämta synpunkter från de berörda parter som avses i punkt 1 om genomförandet av denna förordning.

Artikel 10

Förbättra kompetensen i en cyberresilient digital miljö

Vid tillämpningen av denna förordning och för att tillgodose yrkesutövarnas behov, till stöd för genomförandet av denna förordning, ska medlemsstaterna – när så är lämpligt med stöd av kommissionen, Europeiska kompetenscentrumet för cybersäkerhet och Enisa och med full respekt för medlemsstaternas ansvar på utbildningsområdet – främja åtgärder och strategier som syftar till att

a) utveckla cybersäkerhetskompetensen och skapa organisatoriska och tekniska verktyg för att säkerställa tillräcklig tillgång till kvalificerad arbetskraft för att stödja verksamheten vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse,

b) förbättra samarbetet mellan den privata sektorn, ekonomiska aktörer, bland annat genom omskolning eller kompetenshöjning för tillverkares anställda, konsumenter, utbildningsanordnare och även offentliga förvaltningar, och därmed utöka möjligheterna för unga att få jobb inom cybersäkerhetssektorn.

Artikel 11

Allmän produktsäkerhet

Som avvikelse från artikel 2.1 tredje stycket b i förordning (EU) 2023/988 ska kapitel III avsnitt 1, kapitlen V och VII och kapitlen IX–XI i den förordningen tillämpas på produkter med digitala element med avseende på aspekter och risker eller riskkategorier som inte omfattas av den här förordningen, om dessa produkter inte omfattas av särskilda säkerhetskrav som fastställs i annan av *unionsharmoniseringslagstiftning* enligt definitionen i artikel 3.27 i förordning (EU) 2023/988.

Artikel 12

AI-system med hög risk

1. Utan att det påverkar tillämpningen av kraven på noggrannhet och robusthet som fastställs i artikel 15 i förordning (EU) 2024/1689 ska produkter med digitala element vilka omfattas av denna förordning och klassificeras som AI-system med hög risk enligt artikel 6 i den förordningen anses överensstämma med de cybersäkerhetskrav som fastställs i artikel 15 i den förordningen om

   a) dessa produkter uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del I,

b) de processer som tillverkaren infört uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II, och

c) uppnåendet av den nivå av cybersäkerhetsskydd som krävs enligt artikel 15 i förordning (EU) 2024/1689 visas genom en EU-försäkran om överensstämmelse som utfärdats enligt denna förordning.

2. För de produkter med digitala element och cybersäkerhetskrav som avses i punkt 1 i denna artikel ska det relevanta förfarande för bedömning av överensstämmelse som föreskrivs i artikel 43 i förordning (EU) 2024/1689 tillämpas. Vid denna bedömning ska anmälda organ som är behöriga att kontrollera överensstämmelsen för AI-system med hög risk inom ramen för förordning (EU) 2024/1689 också vara behöriga att kontrollera överensstämmelsen med kraven i bilaga I till denna förordning för AI-system med hög risk inom ramen för denna förordning, förutsatt att dessa anmälda organs uppfyllande av kraven i artikel 39 i denna förordning har bedömts i samband med anmälningsförfarandet inom ramen för förordning (EU) 2024/1689.

3. Genom avvikelse från punkt 2 i denna artikel ska viktiga produkter med digitala element som förtecknas i bilaga III till denna förordning, vilka omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 a och b och 32.3 i denna förordning, och kritiska produkter med digitala element som förtecknas i bilaga IV till denna förordning, vilka måste få ett europeiskt cybersäkerhetscertifikat enligt artikel 8.1 i denna förordning, eller i avsaknad av det, vilka omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.3 i denna förordning, och vilka klassificeras som AI-system med hög risk enligt artikel 6 i förordning (EU) 2024/1689 och omfattas av förfarandet för bedömning av överensstämmelse som grundar sig på intern kontroll enligt bilaga VI till förordning (EU) 2024/1689, genomgå de förfaranden för bedömning av överensstämmelse som föreskrivs i den här förordningen i den mån som de väsentliga cybersäkerhetskrav som anges i den här förordningen berörs.

4. Tillverkare av produkter med digitala element som avses i punkt 1 i denna artikel får delta i de regulatoriska sandlådor för AI som avses i artikel 57 i förordning (EU) 2024/1689.

Kapitel II

Ekonomiska aktörers skyldigheter och bestämmelser om programvara med fri och öppen källkod

Artikel 13

Tillverkares skyldigheter

1. När en produkt med digitala element släpps ut på marknaden ska tillverkarna säkerställa att den har utformats, utvecklats och producerats i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I i del I.

2. För att följa punkt 1 ska tillverkarna göra en bedömning av de cybersäkerhetsrisker som är förbundna med en produkt med digitala element och beakta resultatet av bedömningen under planerings-, utformnings-, utvecklings-, produktions-, leverans- och underhållsfaserna för en produkt med digitala element, för att minimera cybersäkerhetsriskerna, förhindra incidenter och minimera deras konsekvenser, inbegripet vad gäller användarnas hälsa och säkerhet.

3. Bedömningen av cybersäkerhetsrisker ska dokumenteras och uppdateras på lämpligt sätt under en stödperiod som ska fastställas i enlighet med punkt 8 i denna artikel. Bedömningen av cybersäkerhetsrisker ska omfatta åtminstone en analys av cybersäkerhetsriskerna på grundval av det avsedda ändamålet och den rimligen förutsebara användningen samt användningsförhållandena för produkten med digitala element, såsom driftsmiljön eller de tillgångar som ska skyddas, med beaktande av hur länge produkten förväntas vara i bruk. Bedömningen av cybersäkerhetsrisker ska ange huruvida, och i så fall på vilket sätt, de säkerhetskrav som anges i bilaga I del I punkt 2 är tillämpliga på den relevanta produkten med digitala element och hur dessa krav genomförs på grundval av bedömningen av cybersäkerhetrisker. Det ska också anges hur tillverkaren tillämpar bilaga I del I punkt 1 och de krav på sårbarhetshantering som anges i bilaga I del II.

4. När en produkt med digitala element släpps ut på marknaden ska tillverkaren inkludera den bedömning av cybersäkerhetsrisker som avses i punkt 3 i denna artikel i den tekniska dokumentation som krävs enligt artikel 31 och bilaga VII. För de produkter med digitala element som avses i artikel 12 och som också omfattas av andra unionsrättsakter får bedömningen av cybersäkerhetsriskerna ingå i den riskbedömning som krävs enligt dessa unionsrättsakter. I de fall då vissa väsentliga cybersäkerhetskrav inte är tillämpliga på produkten med digitala element ska tillverkaren inkludera en tydlig motivering till detta i den tekniska dokumentationen.

5. För att uppfylla kraven i punkt 1 ska tillverkarna visa tillbörlig aktsamhet när de integrerar komponenter som kommer från tredje part så att dessa komponenter inte komprometterar cybersäkerheten för produkten med digitala element, inbegripet vid integrering av komponenter i programvara med fri och öppen källkod som inte har tillhandahållits på marknaden i samband med kommersiell verksamhet.

6. Tillverkarna ska när de identifierar en sårbarhet i en komponent, inbegripet en komponent med fri och öppen källkod, som är integrerad i en produkt med digitala element, rapportera sårbarheten till den person eller entitet som tillverkar eller underhåller komponenten och åtgärda och avhjälpa sårbarheten i enlighet med de krav på sårbarhetshantering som anges i bilaga I del II. Om tillverkarna har utvecklat en programvaru- eller hårdvaruändring för att åtgärda sårbarheten i den komponenten ska de dela den relevanta koden eller dokumentationen med den person eller entitet som tillverkar eller underhåller komponenten, när så är lämpligt, i ett maskinläsbart format.

7. Tillverkarna ska systematiskt och på ett sätt som står i proportion till cybersäkerhetsriskernas art dokumentera relevanta cybersäkerhetsaspekter som rör produkterna med digitala element, inbegripet sårbarheter de får kännedom om och all relevant information som tillhandahålls av tredje part, och ska, i förekommande fall, uppdatera bedömningen av cybersäkerhetsrisker för produkterna.

8. När en produkt med digitala element släpps ut på marknaden, och under stödperioden, ska tillverkarna säkerställa att produktens, inbegripet dess komponenters, sårbarheter hanteras effektivt och i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.

Tillverkarna ska fastställa stödperioden så att den återspeglar den tidsperiod under vilken produkten förväntas vara i bruk, med särskilt beaktande av rimliga förväntningar från användarna, produktens art, inbegripet dess avsedda ändamål, samt relevant unionsrätt som fastställer livslängden för produkter med digitala element. Vid fastställandet av stödperioden får tillverkarna också beakta stödperioderna för produkter med digitala element som erbjuder en liknande funktion som släppts ut på marknaden av andra tillverkare, tillgången till driftsmiljön, stödperioderna för integrerade komponenter som tillhandahåller kärnfunktioner och kommer från tredje parter samt relevant vägledning från den särskilda administrativa samarbetsgruppen (Adco-gruppen), som inrättats enligt artikel 52.15, och kommissionen. De faktorer som ska beaktas vid fastställandet av den stödperiod som ska beaktas på ett sätt som säkerställer proportionalitet.

Utan att det påverkar tillämpningen av andra stycket ska stödperioden vara minst fem år. Om produkten med digitala element förväntas vara i bruk i mindre än fem år ska stödperioden motsvara den förväntade användningstiden.

Med beaktande av de rekommendationer från Adco-gruppen som avses i artikel 52.16 får kommissionen anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att specificera den minsta tillåtna stödperioden för specifika produktkategorier om uppgifter från marknadskontrollen tyder på otillräckliga stödperioder.

Tillverkarna ska inkludera den information som har beaktats för att fastställa stödperioden för en produkt med digitala element i den tekniska dokumentationen enligt bilaga VII.

Tillverkarna ska ha lämpliga policyer och förfaranden, inbegripet policyer för samordnad delgivning av information om sårbarheter, enligt bilaga I del II punkt 5, för att behandla och åtgärda de potentiella sårbarheter i produkter med digitala element som rapporterats av interna eller externa källor.

9. Tillverkarna ska säkerställa att varje säkerhetsuppdatering som avses i bilaga I del II punkt 8 och som har gjorts tillgänglig för användare under stödperioden förblir tillgänglig efter det att den har utfärdats i minst tio år eller under återstoden av stödperioden, beroende på vilken period som är längst.

10. Om en tillverkare har släppt ut senare väsentligt ändrade versioner av en programvaruprodukt på marknaden får tillverkaren säkerställa överensstämmelse med det väsentliga cybersäkerhetskrav som anges i bilaga I del II punkt 2 endast för den version som tillverkaren senast släppte ut på marknaden, förutsatt att användarna av de versioner som tidigare släppts ut på marknaden kostnadsfritt har tillgång till den version som senast släpptes ut på marknaden och inte ådrar sig ytterligare kostnader för att anpassa den hårdvaru- och programvarumiljö där de använder den ursprungliga versionen av den produkten.

11. Tillverkarna får upprätthålla offentliga programvaruarkiv som förbättrar användarnas tillgång till äldre versioner. I sådana fall ska användarna på ett lättillgängligt sätt få tydlig information om riskerna med att använda programvara som inte stöds.

12. Innan en produkt med digitala element släpps ut på marknaden ska tillverkarna sammanställa den tekniska dokumentation som avses i artikel 31.

    De ska genomföra de valda förfaranden för bedömning av överensstämmelse som avses i artikel 32 eller se till att de genomförs.

    När det genom detta förfarande för bedömning av överensstämmelse har visats att produkten med digitala element uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I och att de processer som tillverkaren infört uppfyller de väsentliga cybersäkerhetskraven i bilaga I del II, ska tillverkarna upprätta EU-försäkran om överensstämmelse i enlighet med artikel 28 och fästa CE-märkningen i enlighet med artikel 30.

13. Tillverkarna ska kunna uppvisa den tekniska dokumentationen och EU-försäkran om överensstämmelse för marknadskontrollmyndigheterna i minst tio år efter det att produkten med digitala element har släppts ut på marknaden, eller under stödperioden, beroende på vilken period som är längst.

14. Tillverkarna ska säkerställa att det finns förfaranden som säkerställer att produkter med digitala element som är en del av serietillverkning fortsätter att överensstämma med kraven i denna förordning. Tillverkarna ska på lämpligt sätt ta hänsyn till förändringar i utvecklings- och tillverkningsprocessen eller i utformningen av eller egenskaperna hos produkten med digitala element samt till ändringar av de harmoniserade standarderna, de europeiska ordningarna för cybersäkerhetscertifiering eller de gemensamma specifikationer som avses i artikel 27 med hänvisning till vilka överensstämmelsen för produkten med digitala element försäkras eller genom vars tillämpning överensstämmelsen kontrolleras.

15. Tillverkarna ska säkerställa att deras produkter med digitala element är försedda med typnummer, partinummer, serienummer eller annan identifieringsmärkning eller, om detta inte är möjligt, säkerställa att den informationen fästas på produktens förpackning eller på ett dokument som åtföljer produkten med digitala element.

16. Tillverkarna ska, på produkten med digitala element, på förpackningen eller i ett dokument som åtföljer produkten med digitala element, ange sitt namn, registrerade firmanamn eller registrerade varumärke samt postadress och e-postadress eller andra digitala kontaktuppgifter och, när så är tillämpligt, webbplatsen där de kan kontaktas. Denna information ska också ingå i den information och de instruktioner till användaren som anges i bilaga II. Kontaktuppgifterna ska vara på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna.

17. Vid tillämpningen av denna förordning ska tillverkarna utse en gemensam kontaktpunkt som gör det möjligt för användarna att kommunicera direkt och snabbt med dem, bland annat för att underlätta rapportering om sårbarheter hos produkten med digitala element.

Tillverkarna ska säkerställa att den gemensamma kontaktpunkten lätt kan identifieras av användarna. De ska också inkludera den gemensamma kontaktpunkten i den information och de instruktioner till användaren som anges i bilaga II.

Den gemensamma kontaktpunkten ska göra det möjligt för användarna att välja det kommunikationsmedel som de föredrar och får inte begränsa sådana medel till automatiserade verktyg.

18. Tillverkarna ska säkerställa att produkter med digitala element åtföljs av information och instruktioner till användaren enligt bilaga II i pappersform eller elektronisk form. Sådan information och sådana instruktioner ska tillhandahållas på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna. De ska vara tydliga, begripliga och läsbara. De ska möjliggöra en säker installation, drift och användning av produkter med digitala element. Tillverkarna ska säkerställa att informationen och instruktionerna till användaren enligt bilaga II förblir tillgängliga för användarna och marknadskontrollmyndigheterna i minst tio år efter det att produkten med digitala element har släppts ut på marknaden, eller under stödperioden, beroende på vilken period som är längst. Om sådan information och sådana instruktioner tillhandahålls online ska tillverkarna säkerställa att de är åtkomliga, användarvänliga och tillgängliga online i minst tio år efter det att produkten med digitala element har släppts ut på marknaden, eller under stödperioden, beroende på vilken period som är längst.

19. Tillverkarna ska säkerställa att slutdatumet för den stödperiod som avses i punkt 8, inbegripet åtminstone månad och år, tydligt och begripligt anges vid tidpunkten för köpet på ett lättillgängligt sätt och, i tillämpliga fall, på produkten med digitala element, dess förpackning eller digitalt.

    Om det är tekniskt möjligt mot bakgrund av arten av produkt med digitala element ska tillverkarna visa ett meddelande till användarna om att deras produkt med digitala element har nått slutet av stödperioden.

20. Tillverkarna ska antingen lämna en kopia av EU-försäkran om överensstämmelse eller en förenklad EU-försäkran om överensstämmelse tillsammans med produkten med digitala element. Om en förenklad EU-försäkran om överensstämmelse lämnas ska den innehålla den exakta webbadress där det går att få tillgång till hela texten till EU-försäkran om överensstämmelse.

21. Från och med utsläppandet på marknaden och under stödperioden ska en tillverkare som vet eller har skäl att tro att produkten med digitala element eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I omedelbart vidta de korrigerande åtgärder som krävs för att bringa produkten med digitala element eller tillverkarens processer i överensstämmelse eller dra tillbaka eller återkalla produkten, såsom lämpligt.

22. Tillverkarna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element och de processer som införts av tillverkaren överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i bilaga I, i pappersform eller i elektronisk form och på ett språk som lätt kan förstås av myndigheten. Tillverkarna ska samarbeta med marknadskontrollmyndigheten, på dess begäran, om alla åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de har släppt ut på marknaden utgör.

23. En tillverkare som upphör med sin verksamhet och därmed inte kan följa denna förordning ska, innan verksamheten upphör, underrätta de berörda marknadskontrollmyndigheterna om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de relevanta produkterna med digitala element som släppts ut på marknaden om att verksamheten snart kommer att upphöra.

24. Kommissionen får genom genomförandeakter, med beaktande av europeiska eller internationella standarder och bästa praxis, specificera formatet och de aspekter som ska ingå i den programvaruförteckning som avses i bilaga I del II punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

25. För att bedöma medlemsstaternas och unionens beroende av programvarukomponenter och i synnerhet av komponenter som klassificeras som programvara med fri och öppen källkod får Adco-gruppen besluta att genomföra en unionsomfattande beroendebedömning för specifika kategorier av produkter med digitala element. För detta ändamål får marknadskontrollmyndigheterna begära att tillverkare av sådana kategorier av produkter med digitala element tillhandahåller den relevanta programvaruförteckning som avses i bilaga I del II punkt 1. På grundval av denna information får marknadskontrollmyndigheterna förse Adco-gruppen med anonymiserad och aggregerad information om programvaruberoenden. Adco-gruppen ska lämna en rapport om resultaten av beroendebedömningen till den samarbetsgrupp som inrättats enligt artikel 14 i direktiv (EU) 2022/2555.

Artikel 14

Tillverkarnas rapporteringsskyldigheter

1. En tillverkare ska till den CSIRT-enhet som utsetts till samordnare i enlighet med punkt 7 i denna artikel och samtidigt till Enisa anmäla alla aktivt utnyttjade sårbarheter i produkten med digitala element som tillverkaren får kännedom om. Tillverkaren ska anmäla den aktivt utnyttjade sårbarheten via den gemensamma rapporteringsplattform som inrättats enligt artikel 16.

2. För den anmälan som avses i punkt 1 ska tillverkaren

   a) utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter att ha fått kännedom om den, lämna in en tidig varning om en aktivt utnyttjad sårbarhet och, i tillämpliga fall, ange de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits,

b) såvida inte relevant information redan har lämnats, utan onödigt dröjsmål och under alla omständigheter senast 72 timmar efter att ha fått kännedom om den aktivt utnyttjade sårbarheten, lämna in en anmälan om sårbarhet, som ska innehålla allmän information, om sådan finns tillgänglig, om den berörda produkten med digitala element, den allmänna karaktären av utnyttjandet och sårbarheten i fråga samt eventuella korrigerande eller riskreducerande åtgärder som vidtagits och korrigerande eller riskreducerande åtgärder som användarna kan vidta, och som också, i tillämpliga fall, ska ange hur känslig tillverkaren anser att den anmälda informationen är,

c) såvida inte relevant information redan har lämnats, senast 14 dagar efter det att en korrigerande eller riskreducerande åtgärd blivit tillgänglig, lämna in en slutrapport, som ska innehålla minst följande:

   i) En beskrivning av sårbarheten och dess allvarlighetsgrad och konsekvenser.

   ii) I förekommande fall information om en fientlig aktör som har utnyttjat eller som utnyttjar sårbarheten.

   iii) Detaljer om säkerhetsuppdateringen eller andra korrigerande åtgärder som har gjorts tillgängliga för att avhjälpa sårbarheten.

3. En tillverkare ska till den CSIRT-enhet som utsetts till samordnare i enlighet med punkt 7 i denna artikel och samtidigt till Enisa anmäla alla allvarliga incidenter som påverkar säkerheten för produkten med digitala element som tillverkaren får kännedom om. Tillverkaren ska anmäla incidenten via den gemensamma rapporteringsplattform som inrättats enligt artikel 16.

4. För den anmälan som avses i punkt 3 ska tillverkaren

a) lämna in en tidig varning om en allvarlig incident som påverkar säkerheten för produkten med digitala element, utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter att ha fått kännedom om den, och åtminstone ange om tillverkaren misstänker att incidenten orsakats av olagliga eller fientliga handlingar, och i tillämpliga fall även ange de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits,

b) såvida inte relevant information redan har lämnats, utan onödigt dröjsmål och under alla omständigheter senast 72 timmar efter att ha fått kännedom om incidenten, lämna in en incidentanmälan, som ska innehålla allmän information, om sådan finns tillgänglig, om arten av incident, en första bedömning av incidenten samt eventuella korrigerande eller riskreducerande åtgärder som vidtagits och korrigerande eller riskreducerande åtgärder som användarna kan vidta, och som också, i tillämpliga fall, ska ange hur känslig tillverkaren anser att den anmälda informationen är,

c) såvida inte relevant information redan har lämnats, inom en månad efter inlämningen av den incidentanmälan som avses i led b, lämna in en slutrapport, som ska innehålla minst följande:

i) En detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser.

ii) Den typ av hot eller grundorsak som sannolikt har utlöst incidenten.

iii) Tillämpade och pågående riskreducerande åtgärder.

5. Vid tillämpning av punkt 3 ska en incident som påverkar säkerheten för produkten med digitala element anses vara allvarlig om

a) den inverkar negativt på eller kan inverka negativt på förmågan hos en produkt med digitala element att skydda tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten för känsliga eller viktiga data eller funktioner, eller

b) den har lett eller kan leda till att en skadlig kod införts eller använts i en produkt med digitala element eller i nätverks- och informationssystemet hos en användare av produkten med digitala element.

6. Vid behov får den CSIRT-enhet som utsetts till samordnare som först tog emot anmälan begära att tillverkarna lämnar en delrapport om relevanta statusuppdateringar om den aktivt utnyttjade sårbarheten eller allvarliga incidenten som påverkar säkerheten för produkten med digitala element.

7. De anmälningar som avses i punkterna 1 och 3 i denna artikel ska lämnas in via den gemensamma rapporteringsplattform som avses i artikel 16 med hjälp av en av de slutpunkter för elektronisk anmälan som avses i artikel 16.1. Anmälan ska lämnas in med hjälp av slutpunkten för elektronisk anmälan hos den CSIRT-enhet som utsetts till samordnare i den medlemsstat där tillverkarna har sitt huvudsakliga verksamhetsställe i unionen och ska samtidigt göras tillgänglig för Enisa.

Vid tillämpning av denna förordning ska en tillverkare anses ha sitt huvudsakliga verksamhetsställe i unionen i den medlemsstat där de cybersäkerhetsrelaterade besluten avseende dess produkter med digitala element i huvudsak fattas. Om en sådan medlemsstat inte kan fastställas ska det huvudsakliga verksamhetsstället anses vara beläget i den medlemsstat där den berörda tillverkaren har det verksamhetsställe som har flest anställda i unionen.

Om en tillverkare inte har något huvudsakligt verksamhetsställe i unionen ska tillverkaren lämna in de anmälningar som avses i punkterna 1 och 3 med hjälp av slutpunkten för elektronisk anmälan hos den CSIRT-enhet som utsetts till samordnare i den medlemsstat som fastställs enligt följande ordning och på grundval av den information som tillverkaren har tillgång till:

a) Den medlemsstat där tillverkarens representant som agerar för tillverkarens räkning för det största antalet produkter med digitala element från den tillverkaren är etablerad.

b) Den medlemsstat där den importör som släpper ut det största antalet produkter med digitala element från den tillverkaren är etablerad.

c) Den medlemsstat där den distributör som tillhandahåller det största antalet produkter med digitala element från den tillverkaren är etablerad.

d) Den medlemsstat där det största antalet användare av produkter med digitala element från den tillverkaren finns.

När det gäller tredje stycket d får en tillverkare lämna in anmälningar om eventuella efterföljande aktivt utnyttjade sårbarheter eller allvarliga incidenter som påverkar säkerheten för produkten med digitala element till samma CSIRT-enhet som utsetts till samordnare till vilken den först rapporterade.

8. Efter att ha fått kännedom om en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala element, ska tillverkaren underrätta de drabbade användarna av produkten med digitala element, och när så är lämpligt alla användare, om den sårbarheten eller incidenten och, vid behov, om riskreducering och eventuella korrigerande åtgärder som användarna kan vidta för att begränsa konsekvenserna av denna sårbarhet eller incident, om lämpligt i ett strukturerat, maskinläsbart format som är enkelt att automatiskt behandla. Om tillverkaren underlåter att underrätta användarna av produkten med digitala element i tid får de CSIRT-enheter som utsetts till samordnare som mottagit anmälan lämna sådan information till användarna när detta anses vara proportionellt och nödvändigt för att förebygga eller mildra konsekvenserna av sårbarheten eller incidenten.

9. Senast den … [tolv månader från den dag då denna förordning träder i kraft] ska kommissionen anta delegerade akter i enlighet med artikel 61 i denna förordning för att komplettera denna förordning genom att specificera villkoren för att tillämpa de cybersäkerhetsrelaterade skälen till att skjuta upp spridningen av anmälningar som avses i artikel 16.2 i denna förordning. Kommissionen ska samarbeta med det CSIRT-nätverk som inrättats enligt artikel 15 i direktiv (EU) 2022/2555 och Enisa vid utarbetandet av utkasten till delegerad akt.

10. Kommissionen får genom genomförandeakter ytterligare specificera formatet och förfarandena för de anmälningar som avses i denna artikel samt i artiklarna 15 och 16. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2. Kommissionen ska samarbeta med CSIRT-nätverket och Enisa vid utarbetandet av dessa utkast till genomförandeakter.

Artikel 15

Frivillig rapportering

1. Tillverkarna och andra fysiska eller juridiska personer får, på frivillig basis, till en CSIRT-enhet som utsetts till samordnare eller till Enisa anmäla eventuella sårbarheter i en produkt med digitala element samt cyberhot som kan påverka riskprofilen för en produkt med digitala element.

2. Tillverkarna och andra fysiska eller juridiska personer får, på frivillig basis, till en CSIRT-enhet som utsetts till samordnare eller till Enisa anmäla eventuella incidenter som påverkar säkerheten för produkten med digitala element och tillbud som hade kunnat leda till en sådan incident.

3. Den CSIRT-enhet som utsetts till samordnare eller Enisa ska behandla de anmälningar som avses i punkterna 1 och 2 i denna artikel i enlighet med det förfarande som anges i artikel 16.

   Den CSIRT-enhet som utsetts till samordnare får prioritera behandlingen av obligatoriska anmälningar före behandlingen av frivilliga anmälningar.

4. Om en annan fysisk eller juridisk person än tillverkaren anmäler en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för en produkt med digitala element i enlighet med punkt 1 eller 2 ska den CSIRT-enhet som utsetts till samordnare, utan onödigt dröjsmål, informera tillverkaren.

5. Den CSIRT-enhet som utsetts till samordnare och Enisa ska säkerställa konfidentialitet och lämpligt skydd för den information som tillhandahålls av den anmälande fysiska eller juridiska personen. Utan att det påverkar förebyggandet, utredningen, avslöjandet och lagföringen av brott får frivillig rapportering inte leda till att den anmälande fysiska eller juridiska personen åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in anmälan.

Artikel 16

Inrättande av en gemensam rapporteringsplattform

1. För de anmälningar som avses i artikel 14.1 och 14.3 samt artikel 15.1 och 15.2 och för att förenkla tillverkarnas rapporteringsskyldigheter ska Enisa inrätta en gemensam rapporteringsplattform. Den dagliga driften av den gemensamma rapporteringsplattformen ska skötas och upprätthållas av Enisa. Strukturen för den gemensamma rapporteringsplattformen ska göra det möjligt för medlemsstaterna och Enisa att införa sina egna slutpunkter för elektronisk anmälan.

2. Efter att ha mottagit en anmälan ska den CSIRT-enhet som utsetts till samordnare som först tog emot anmälan, utan dröjsmål, sprida anmälan via den gemensamma rapporteringsplattformen till de CSIRT-enheter som utsetts till samordnare på det territorium där tillverkaren har angett att produkten med digitala element har tillhandahållits.

Under exceptionella omständigheter, särskilt på begäran av tillverkaren och mot bakgrund av känslighetsnivån hos den anmälda information som tillverkaren angett i enlighet med artikel 14.2 a i denna förordning, får spridningen av anmälan skjutas upp på grundval av motiverade cybersäkerhetsrelaterade skäl under en tidsperiod som är absolut nödvändig, inbegripet när en sårbarhet är föremål för ett förfarande för samordnad delgivning av information om sårbarheter som avses i artikel 12.1 i direktiv (EU) 2022/2555. Om en CSIRT-enhet beslutar att undanhålla en anmälan ska den omedelbart informera Enisa om beslutet och motivera varför anmälan undanhålls och ange när den kommer att sprida anmälan i enlighet med det spridningsförfarande som fastställs i denna punkt. Enisa får stödja CSIRT-enheten i tillämpningen av cybersäkerhetsrelaterade skäl när det gäller att skjuta upp spridningen av anmälan.

Under särskilt exceptionella omständigheter, om tillverkaren i den anmälan som avses i artikel 14.2 b anger att

a) den anmälda sårbarheten aktivt har utnyttjats av en fientlig aktör och att den, enligt tillgänglig information, inte har utnyttjats i någon annan medlemsstat än den där den CSIRT-enhet som utsetts till samordnare finns till vilken tillverkaren har anmält sårbarheten,

b) all omedelbar ytterligare spridning av den anmälda sårbarheten sannolikt skulle leda till tillhandahållande av information vars utlämnande skulle strida mot den medlemsstatens väsentliga intressen, eller

c) den anmälda sårbarheten utgör en överhängande hög cybersäkerhetsrisk till följd av den fortsatta spridningen,

ska endast information om att tillverkaren har gjort en anmälan, allmän information om produkten, den allmänna karaktären av utnyttjandet och information om att säkerhetsrelaterade skäl angetts göras tillgänglig samtidigt för Enisa till dess att den fullständiga anmälan sprids till de berörda CSIRT-enheterna och Enisa. Om Enisa på grundval av denna information anser att det finns en systemrisk som påverkar säkerheten på den inre marknaden ska Enisa rekommendera den mottagande CSIRT-enheten att sprida den fullständiga anmälan till de andra CSIRT-enheter som utsetts till samordnare och till Enisa själv.

3. Efter att ha mottagit en anmälan om en aktivt utnyttjad sårbarhet i en produkt med digitala element eller om en allvarlig incident som påverkar säkerheten för en produkt med digitala element ska de CSIRT-enheter som utsetts till samordnare förse marknadskontrollmyndigheterna i sina respektive medlemsstater med den anmälda information som behövs för att marknadskontrollmyndigheterna ska kunna fullgöra sina skyldigheter enligt denna förordning.

4. Enisa ska vidta lämpliga och proportionella tekniska, operativa och organisatoriska åtgärder för att hantera säkerhetsriskerna för den gemensamma rapporteringsplattformen och den information som lämnas in eller sprids via den gemensamma rapporteringsplattformen. Enisa ska utan onödigt dröjsmål underrätta CSIRT-nätverket och kommissionen om alla säkerhetsincidenter som påverkar den gemensamma rapporteringsplattformen.

5. Enisa ska, i samarbete med CSIRT-nätverket, tillhandahålla och genomföra specifikationer för de tekniska, operativa och organisatoriska åtgärderna för inrättande, underhåll och säker drift av den gemensamma rapporteringsplattform som avses i punkt 1, inbegripet åtminstone säkerhetsarrangemangen i samband med inrättande, drift och underhåll av den gemensamma rapporteringsplattformen, samt de slutpunkter för elektronisk anmälan som inrättats av de CSIRT-enheter som utsetts till samordnare på nationell nivå och Enisa på unionsnivå, inbegripet förfarandemässiga aspekter för att – i fall där det för en anmäld sårbarhet inte finns några korrigerande eller riskreducerande åtgärder – säkerställa att information om denna sårbarhet delas i enlighet med strikta säkerhetsprotokoll och på grundval av behovsenlig behörighet.

6. Om en CSIRT-enhet som utsetts till samordnare har uppmärksammats på en aktivt utnyttjad sårbarhet, som en del av ett förfarande för samordnad delgivning av information om sårbarheter som avses i artikel 12.1 i direktiv (EU) 2022/2555, får den CSIRT-enhet som utsetts till samordnare som först tog emot anmälan skjuta upp spridningen av den berörda anmälan via den gemensamma rapporteringsplattformen på grundval av motiverade cybersäkerhetsrelaterade skäl under en period som inte är längre än vad som är absolut nödvändigt och till dess att de berörda parterna inom samordnad delgivning av information om sårbarheter har gett sitt samtycke till utlämnande. Detta krav ska inte hindra tillverkarna från att frivilligt anmäla en sådan sårbarhet i enlighet med förfarandet i denna artikel.

Artikel 17

Andra bestämmelser avseende rapportering

1. Enisa får lämna information som anmälts enligt artikel 14.1 och 14.3 samt artikel 15.1 och 15.2 i denna förordning till Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), som inrättats enligt artikel 16 i direktiv (EU) 2022/2555, om informationen är relevant för den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och -kriser på operativ nivå. För att fastställa sådan relevans får Enisa överväga tekniska analyser som utförs av CSIRT-nätverket, om sådana finns tillgängliga.

2. Om det är nödvändigt att informera allmänheten för att förebygga eller begränsa en allvarlig incident som påverkar säkerheten för produkten med digitala element eller för att hantera en pågående incident, eller om ett avslöjande av incidenten på annat sätt ligger i allmänhetens intresse, får den CSIRT-enhet som utsetts till samordnare för den berörda medlemsstaten, efter samråd med den berörda tillverkaren och, när så är lämpligt, i samarbete med Enisa, informera allmänheten om incidenten eller kräva att tillverkaren gör detta.

3. På grundval av de anmälningar som inkommer enligt artikel 14.1 och 14.3 samt artikel 15.1 och 15.2 i denna förordning ska Enisa vartannat år utarbeta en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element, och lämna den till den samarbetsgrupp som inrättats enligt artikel 14 i direktiv (EU) 2022/2555. Den första av dessa rapporter ska lämnas in inom 24 månader från det att de skyldigheter som fastställs i artikel 14.1 och 14.3 i denna förordning börjar tillämpas. Enisa ska inkludera relevant information från sina tekniska rapporter i sin rapport om cybersäkerhetssituationen i unionen enligt artikel 18 i direktiv (EU) 2022/2555.

4. Själva anmälan i enlighet med artikel 14.1 och 14.3 eller artikel 15.1 och 15.2 ska inte medföra ökat ansvar för den anmälande fysiska eller juridiska personen.

5. Efter det att en säkerhetsuppdatering eller någon annan form av korrigerande eller riskreducerande åtgärd finns tillgänglig ska Enisa, i samförstånd med tillverkaren av den berörda produkten med digitala element, lägga till den allmänt kända sårbarhet som anmälts enligt artikel 14.1 eller 15.1 i denna förordning i den europeiska sårbarhetsdatabas som inrättats enligt artikel 12.2 i direktiv (EU) 2022/2555.

6. De CSIRT-enheter som utsetts till samordnare ska tillhandahålla hjälptjänster i samband med rapporteringsskyldigheterna enligt artikel 14 till tillverkare, särskilt tillverkare som kan betecknas som mikroföretag eller små eller medelstora företag.

Artikel 18

Tillverkarens representanter

1. En tillverkare får genom skriftlig fullmakt utse en tillverkarens representant.

2. Skyldigheterna enligt artikel 13.1–13.11 och artikel 13.12 första stycket samt artikel 13.14 får inte delegeras till tillverkarens representant.

3. Tillverkarens representant ska utföra de uppgifter som anges i fullmakten från tillverkaren. Tillverkarens representant ska på begäran lämna en kopia av fullmakten till marknadskontrollmyndigheterna. Fullmakten ska ge tillverkarens representant rätt att göra minst följande:

a) Inneha den EU-försäkran om överensstämmelse som avses i artikel 28 och den tekniska dokumentation som avses i artikel 31 för att kunna uppvisa dem för marknadskontrollmyndigheterna i minst tio år efter det att produkten med digitala element har släppts ut på marknaden, eller under stödperioden, beroende på vilken period som är längst.

b) På motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa överensstämmelsen för en produkt med digitala element.

c) På marknadskontrollmyndigheternas begäran samarbeta med dem om åtgärder som vidtas för att undanröja riskerna med en produkt med digitala element som omfattas av fullmakten för tillverkarens representant.

Artikel 19

Importörers skyldigheter

1. Importörer får på marknaden endast släppa ut sådana produkter med digitala element som uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och för vilka de processer som införts av tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

2. Innan en produkt med digitala element släpps ut på marknaden ska importörerna säkerställa att

   a) de tillämpliga förfaranden för bedömning av överensstämmelse som avses i artikel 32 har genomförts av tillverkaren,

   b) tillverkaren har upprättat den tekniska dokumentationen, och

   c) produkten med digitala element är försedd med den CE-märkning som avses i artikel 30 och åtföljs av den EU-försäkran om överensstämmelse som avses i artikel 13.20 och den information och de instruktioner till användaren som anges i bilaga II på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna,

   d) tillverkaren har uppfyllt kraven i artikel 13.15, 13.16 och 13.19.

   Vid tillämpningen av denna punkt ska importörerna kunna tillhandahålla nödvändiga dokument som styrker att kraven i denna artikel är uppfyllda.

3. Om en importör anser eller har skäl att tro att en produkt med digitala element eller de processer som införts av tillverkaren inte överensstämmer med denna förordning, får importören inte släppa ut produkten på marknaden förrän produkten eller processerna som införts av tillverkaren har bringats till överensstämmelse med denna förordning. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska importören också underrätta tillverkaren och marknadskontrollmyndigheterna om detta.

Om en importör har skäl att tro att en produkt med digitala element kan utgöra en betydande cybersäkerhetsrisk mot bakgrund av icke-tekniska riskfaktorer, ska importören underrätta marknadskontrollmyndigheterna om detta. Vid mottagandet av sådan information ska marknadskontrollmyndigheterna följa de förfaranden som avses i artikel 54.2.

4. På produkter med digitala element eller på förpackningen eller i ett dokument som åtföljer produkten med digitala element ska importörer ange namn, registrerat firmanamn eller registrerat varumärke, postadress, e-postadress eller annan digital kontaktuppgift samt, i tillämpliga fall, webbplatsen där de kan kontaktas. Kontaktuppgifterna ska vara på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna.

5. Importörer som vet eller har skäl att tro att en produkt med digitala element som de har släppt ut på marknaden inte överensstämmer med denna förordning ska omedelbart vidta de korrigerande åtgärder som krävs för att säkerställa att produkten överensstämmer med denna förordning eller dra tillbaka eller återkalla produkten, om så är lämpligt.

   När importörer blir medvetna om en sårbarhet i en produkt med digitala element ska de utan dröjsmål underrätta tillverkaren om denna. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska importörerna dessutom omedelbart underrätta marknadskontrollmyndigheterna i de medlemsstater på vilkas marknad de har tillhandahållit produkten med digitala element, och lämna uppgifter om i synnerhet den bristande överensstämmelsen och de korrigerande åtgärder som vidtagits.

6. Under minst tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst, ska importörerna kunna uppvisa en kopia av EU-försäkran om överensstämmelse för marknadskontrollmyndigheterna och säkerställa att dessa myndigheter på begäran kan få tillgång till den tekniska dokumentationen.

7. Importörerna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i del I i bilaga I och att de processer som införts av tillverkaren överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i del II i bilaga I, i pappersform eller i elektronisk form och på ett språk som lätt kan förstås av myndigheten. De ska på begäran samarbeta med den myndigheten om de åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de släppt ut på marknaden utgör.

8. När en importör av en produkt med digitala element får kännedom om att produktens tillverkare upphört med sin verksamhet och därmed inte kan uppfylla de skyldigheter som fastställs i denna förordning ska importören underrätta berörda marknadskontrollmyndigheter om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de produkter med digitala element som släppts ut på marknaden.

Artikel 20

Distributörers skyldigheter

1. När distributörerna tillhandahåller en produkt med digitala element på marknaden ska de agera med vederbörligt iakttagande av kraven i denna förordning.

2. Innan distributörerna tillhandahåller en produkt med digitala element på marknaden ska de kontrollera att

a) produkten med digitala element är försedd med CE-märkning,

b) tillverkaren och importören har uppfyllt de krav som anges i artikel 13.15, 13.16, 13.18, 13.19, 13.20 och artikel 19.4, och har försett distributören med alla dokument som krävs.

3. Om en distributör på grundval av information som distributören förfogar över anser eller har skäl att tro att en produkt med digitala element eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I, får distributören inte tillhandahålla produkten på marknaden förrän produkten eller processerna som införts av tillverkaren har bringats till överensstämmelse med denna förordning. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska distributören utan onödigt dröjsmål underrätta tillverkaren och marknadskontrollmyndigheterna om detta.

4. Distributörer som på grundval av information som distributörerna förfogar över vet eller har skäl att tro att en produkt med digitala element, som de har tillhandahållit på marknaden, eller de processer som införts av tillverkaren inte överensstämmer med denna förordning ska se till att de korrigerande åtgärder som krävs för att bringa produkten eller tillverkarens processer i överensstämmelse vidtas, eller dra tillbaka eller återkalla produkten, om så är lämpligt.

När importörer blir medvetna om en sårbarhet i en produkt med digitala element ska de utan dröjsmål underrätta tillverkaren om denna. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska distributörerna dessutom omedelbart underrätta marknadskontrollmyndigheterna i de medlemsstater på vilkas marknad de har tillhandahållit produkten med digitala element, och lämna uppgifter om i synnerhet den bristande överensstämmelsen och de korrigerande åtgärder som vidtagits.

5. Distributörerna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element och de processer som införts av tillverkaren överensstämmer med denna förordning, i pappersform eller i elektronisk form och på ett språk som lätt kan förstås av myndigheten. De ska på begäran samarbeta med marknadskontrollmyndigheten om de åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de tillhandahåller på marknaden utgör.

6. När en distributör av en produkt med digitala element på grundval av information som distributören förfogar över får kännedom om att produktens tillverkare upphört med sin verksamhet och därmed inte kan uppfylla de skyldigheter som fastställs i denna förordning ska distributören utan onödigt dröjsmål underrätta berörda marknadskontrollmyndigheter om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de produkter med digitala element som släppts ut på marknaden.

Artikel 21

Fall där tillverkares skyldigheter gäller för importörer och distributörer

En importör eller distributör ska anses som tillverkare enligt denna förordning och omfattas av artiklarna 13 och 14 om importören eller distributören släpper ut en produkt med digitala element på marknaden i eget namn eller under eget varumärke eller utför en väsentlig ändring av en produkt med digitala element som redan har släppts ut på marknaden.

Artikel 22

Andra fall där tillverkarnas skyldigheter gäller

1. En fysisk eller juridisk person, annan än tillverkaren, importören eller distributören, som utför en väsentlig ändring av en produkt med digitala element och tillhandahåller den produkten på marknaden ska anses som tillverkare vid tillämpningen av denna förordning.

2. Den person som avses i punkt 1 i denna artikel ska omfattas av de skyldigheter som fastställs i artiklarna 13 och 14 när det gäller den del av produkten med digitala element som påverkas av den väsentliga ändringen eller, om den väsentliga ändringen påverkar cybersäkerheten för produkten med digitala element som helhet, för hela produkten.

Artikel 23

Identifiering av ekonomiska aktörer

1. Ekonomiska aktörer ska på begäran förse marknadskontrollmyndigheterna med följande information:

   a) Namn och adress för ekonomiska aktörer som har levererat en produkt med digitala element till dem.

   b) Namn och adress för ekonomiska aktörer som de har levererat en produkt med digitala element till, om tillgängligt.

2. De ekonomiska aktörerna ska kunna tillhandahålla den information som avses i punkt 1 i tio år efter det att de har fått en produkt med digitala element levererad och i tio år efter det att de har levererat en produkt med digitala element.

Artikel 24

Skyldigheter för förvaltare av programvara med fri och öppen källkod

1. Förvaltare av programvara med fri och öppen källkod ska på ett verifierbart sätt införa och dokumentera en cybersäkerhetspolicy så att det utvecklas en säker produkt med digitala element och så att utvecklarna av den produkten effektivt hanterar sårbarheter. I denna policy ska också ingå att utvecklarna av den produkten frivilligt rapporterar sårbarheter enligt artikel 15 och att den särskilda karaktären hos förvaltaren av programvara med fri och öppen källkod beaktas liksom de rättsliga och organisatoriska arrangemang som förvaltaren omfattas av. Policyn ska särskilt omfatta aspekter som rör dokumentering, hantering och avhjälpande av sårbarheter och främja utbyte av information om sårbarheter som upptäckts inom nätgemenskapen för öppen källkodsprojekt.

2. Förvaltarna av programvara med fri och öppen källkod ska samarbeta med marknadskontrollmyndigheterna på deras begäran i syfte att minska cybersäkerhetsriskerna med en produkt med digitala element som klassificeras som programvara med fri och öppen källkod.

   På motiverad begäran från en marknadskontroll myndighet ska förvaltare av programvara med fri och öppen källkod förse den myndigheten med den dokumentation som avses i punkt 1, på ett språk som lätt kan förstås av den myndigheten, i pappersform eller elektronisk form.

3. De skyldigheter som fastställs i artikel 14.1 ska tillämpas på förvaltare av programvara med fri och öppen källkod i den mån de deltar i utvecklingen av produkter med digitala element. De skyldigheter som fastställs i artikel 14.3 och 14.8 ska tillämpas på förvaltare av programvara med fri och öppen källkod i den mån allvarliga incidenter som påverkar säkerheten för produkter med digitala element påverkar de nätverks- och informationssystem som tillhandahålls av förvaltarna för programvara med fri och öppen källkod för utvecklingen av sådana produkter.

Artikel 25

Säkerhetsintyg för programvara med fri och öppen källkod

I syfte att underlätta den skyldighet att visa tillbörlig aktsamhet som anges i artikel 13.5, särskilt när det gäller tillverkare som införlivar komponenter av programvara med fri och öppen källkod i sina produkter med digitala element, ges kommissionen befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att inrätta frivilliga program för säkerhetsintyg som gör det möjligt för utvecklare eller användare av produkter med digitala element som klassificeras som programvara med fri och öppen källkod samt andra tredje parter att bedöma sådana produkters överensstämmelse med alla eller vissa väsentliga cybersäkerhetskrav eller andra skyldigheter som fastställs i denna förordning.

Artikel 26

Vägledning

1. För att underlätta genomförandet av denna förordning och säkerställa ett konsekvent genomförande ska kommissionen offentliggöra vägledning som ska vara till hjälp för de ekonomiska aktörerna vid tillämpningen av denna förordning, med särskilt fokus på att underlätta efterlevnaden för mikroföretag samt små och medelstora företag.

2. Om kommissionen avser att tillhandahålla sådan vägledning som avses i punkt 1 ska den ta upp åtminstone följande aspekter:

   a) Denna förordnings tillämpningsområde, med särskilt fokus på lösningar för fjärrbehandling av data och programvara med fri och öppen källkod.

   b) Tillämpningen av stödperioder med avseende på särskilda kategorier av produkter med digitala element.

   c) Vägledning för tillverkare som omfattas av denna förordning och som också omfattas av annan unionsharmoniseringslagstiftning än denna förordning eller av andra relaterade unionsrättsakter.

   d) Begreppet väsentlig ändring.

   Kommissionen ska också upprätthålla en lättillgänglig förteckning över de delegerade akter och genomförandeakter som antagits enligt denna förordning.

3. Vid utarbetandet av vägledningen enligt denna artikel ska kommissionen samråda med berörda parter.

Kapitel III

Överensstämmelse för produkten med digitala element

Artikel 27

Presumtion om överensstämmelse

1. Produkter med digitala element och processer som införts av tillverkaren som överensstämmer med harmoniserade standarder, eller delar av sådana, vilka har offentliggjorts i *Europeiska unionens officiella tidning*, ska förutsättas överensstämma med de väsentliga cybersäkerhetskrav i bilaga I som omfattas av dessa standarder eller delar av dem.

   Kommissionen ska i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder för de väsentliga cybersäkerhetskraven i bilaga I till den här förordningen. När kommissionen utarbetar begäranden om standardisering för den här förordningen ska den sträva efter att beakta befintliga europeiska och internationella standarder för cybersäkerhet som införts eller håller på att tas fram, i syfte att förenkla utvecklingen av harmoniserade standarder, i enlighet med förordning (EU) nr 1025/2012.

2. Kommissionen får anta genomförandeakter om fastställande av gemensamma specifikationer som omfattar tekniska krav som gör det möjligt att uppfylla de väsentliga cybersäkerhetskraven i bilaga I för produkter med digitala element som omfattas av denna förordnings tillämpningsområde.

Dessa genomförandeakter får endast antas om följande villkor är uppfyllda:

a) Kommissionen har, enligt artikel 10.1 i förordning (EU) nr 1025/2012, begärt att en eller flera europeiska standardiseringsorganisationer utarbetar en harmoniserad standard för de väsentliga cybersäkerhetskrav som fastställs i bilaga I och

i) begäran har inte godtagits,

ii) de harmoniserade standarder som avser begäran levereras inte inom den tidsfrist som fastställts i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012 eller

iii) de harmoniserade standarderna överensstämmer inte med begäran.

b) Ingen hänvisning till harmoniserade standarder som omfattar de relevanta väsentliga cybersäkerhetskraven i bilaga I till denna förordning har offentliggjorts i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, och ingen sådan hänvisning förväntas offentliggöras inom rimlig tid.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

3. Innan kommissionen utarbetar det utkast till genomförandeakt som avses i punkt 2 i den här artikeln ska den informera den kommitté som avses i artikel 22 i förordning (EU) nr 1025/2012 om att den anser att villkoren i punkt 2 i den här artikeln är uppfyllda.

4. När kommissionen utarbetar det utkast till genomförandeakt som avses i punkt 2 ska den ta hänsyn till synpunkter från relevanta organ och vederbörligen samråda med alla berörda parter.

5. Produkter med digitala element och processer som har införts av tillverkaren vilka överensstämmer med de gemensamma specifikationer som fastställts i de genomförandeakter som avses i punkt 2 i denna artikel, eller delar av dem, ska förutsättas överensstämma med de väsentliga cybersäkerhetskraven i bilaga I som omfattas av de gemensamma specifikationerna eller delar av dem.

6. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen i syfte att offentliggöra hänvisningen till den i *Europeiska unionens officiella tidning*, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i *Europeiska unionens officiella tidning* ska kommissionen upphäva de genomförandeakter som avses i punkt 2 i denna artikel, eller delar av dem som omfattar samma väsentliga cybersäkerhetskrav som de som omfattas av denna harmoniserade standard.

7. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga cybersäkerhetskraven i bilaga I ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.

8. Produkter med digitala element och processer som har införts av tillverkaren för vilka en EU-försäkran om överensstämmelse eller ett certifikat har utfärdats enligt förordning (EU) 2019/881, ska förutsättas överensstämma med de väsentliga cybersäkerhetskraven i bilaga I i den mån som EU-försäkran om överensstämmelse eller det europeiska cybersäkerhetscertifikatet, eller delar av dessa, täcker dessa krav.

9. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 i denna förordning, för att komplettera denna förordning genom att specificera vilka europeiska ordningar för cybersäkerhetscertifiering inom ramen för förordning (EU) 2019/881 som kan användas för att visa att produkter med digitala element överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i bilaga I till denna förordning, eller delar av dessa. Utfärdandet av ett europeiskt cybersäkerhetscertifikat inom ramen för sådana system, med åtminstone assuransnivån ”betydande”, befriar tillverkaren från skyldigheten att utföra en tredjepartsbedömning av överensstämmelse för de motsvarande kraven, i enlighet med artikel 32.2 a och b och 32.3 a och b i den här förordningen.

Artikel 28

EU-försäkran om överensstämmelse

1. EU-försäkran om överensstämmelse ska upprättas av tillverkarna i enlighet med artikel 13.12 och ska ange att det har visats att de tillämpliga väsentliga cybersäkerhetskraven i bilaga I uppfylls.

2. EU-försäkran om överensstämmelse ska utformas i enlighet med mallen i bilaga V och ska innehålla de uppgifter som anges i de relevanta förfaranden för bedömning av överensstämmelse som fastställs i bilaga VIII. En sådan försäkran ska uppdateras när så är lämpligt. Den ska tillhandahållas på de språk som krävs av den medlemsstat där produkten med digitala element släpps ut på marknaden eller tillhandahålls på marknaden.

Den förenklade EU-försäkran om överensstämmelse som avses i artikel 13.20 ska utformas i enlighet med mallen i bilaga VI. Den ska tillhandahållas på de språk som krävs av den medlemsstat där produkten med digitala element släpps ut på marknaden eller tillhandahålls på marknaden.

3. Om en produkt med digitala element omfattas av mer än en unionsrättsakt där det ställs krav på EU-försäkran om överensstämmelse ska en enda EU-försäkran om överensstämmelse upprättas med avseende på alla dessa unionsrättsakter. I denna försäkran ska det anges vilka unionsrättsakter som berörs, inbegripet EUT-hänvisningarna till dem.

4. Genom att EU-försäkran om överensstämmelse upprättas ska tillverkaren ta ansvar för att produkten överensstämmer med digitala element.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att lägga till uppgifter till det minimiinnehåll för EU-försäkran om överensstämmelse som fastställs i bilaga V, för att ta hänsyn till den tekniska utvecklingen.

Artikel 29

Allmänna principer för CE-märkning

CE-märkningen ska omfattas av de allmänna principer som fastställs i artikel 30 i förordning (EG) nr 765/2008.

Artikel 30

Regler och villkor för anbringande av CE-märkning

1. CE-märkningen ska fästas på produkten med digitala element så att den är synlig, läsbar och outplånlig. Om detta inte är möjligt eller inte är lämpligt på grund av produktens art, ska den fästas på förpackningen och på den EU-försäkran om överensstämmelse enligt artikel 28 som medföljer produkten med digitala element. För produkter med digitala element i form av programvara ska CE-märkningen fästas antingen på EU-försäkran om överensstämmelse enligt artikel 28 eller på den webbplats som åtföljer programvaruprodukten. I det sistnämnda fallet ska det relevanta avsnittet på webbplatsen kunna nås enkelt och direkt av konsumenterna.

2. På grund av arten av produkt med digitala element får höjden på den CE-märkning som fästas på produkten understiga 5 mm, förutsatt att den förblir synlig och läsbar.

3. CE-märkningen ska fästas innan produkten med digitala element släpps ut på marknaden. Den får åtföljas av ett piktogram eller annan märkning som anger en särskild cybersäkerhetsrisk eller användning som fastställs i de genomförandeakter som avses i punkt 6.

4. CE-märkningen ska följas av det anmälda organets identifikationsnummer, i de fall då det organet är involverat i det förfarande för bedömning av överensstämmelse baserat på fullständig kvalitetssäkring (baserat på modul H) som avses i artikel 32.

   Det anmälda organets identifikationsnummer ska fästas av organet självt eller, enligt organets anvisningar, av tillverkaren eller tillverkarens representant.

5. Medlemsstaterna ska utgå från befintliga mekanismer för att säkerställa att bestämmelserna om CE-märkning tillämpas korrekt och vidta lämpliga åtgärder i händelse av otillbörlig användning av märkningen. I de fall då en produkt med digitala element omfattas av annan unionsharmoniseringslagstiftning än denna förordning som också föreskriver CE-märkning ska CE-märkningen visa att produkten även uppfyller kraven som anges i sådan annan unionsharmoniseringslagstiftning.

6. Kommissionen får genom delegerade akter fastställa tekniska specifikationer för etiketter, piktogram eller andra märkningar som rör säkerheten för produkter med digitala element, deras stödperioder och mekanismer för att främja användningen av sådana och öka allmänhetens medvetenhet om säkerheten hos produkter med digitala element. När kommissionen utarbetar utkast till genomförandeakt ska den samråda med berörda parter och, enligt artikel 52.15, med Adco-gruppen om den redan har inrättats. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

Artikel 31

Teknisk dokumentation

1. Den tekniska dokumentationen ska omfatta alla relevanta data eller uppgifter om de metoder som tillverkaren använt för att säkerställa att produkter med digitala element och de processer som införts av tillverkaren uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I. Den ska åtminstone omfatta de aspekter som fastställs i bilaga VII.

2. Den tekniska dokumentationen ska upprättas innan produkten med digitala element släpps ut på marknaden och ska uppdateras kontinuerligt, vid behov, under åtminstone stödperioden.

3. För de produkter med digitala element som avses i artikel 12 vilka även omfattas av andra unionsrättsakter som föreskriver teknisk dokumentation ska en enda serie teknisk dokumentation upprättas med den information som avses i bilaga VII och den information som föreskrivs i andra unionsrättsakter.

4. Den tekniska dokumentation och korrespondens som avser förfaranden för bedömning av överensstämmelse ska upprättas på ett officiellt språk i den medlemsstat där det anmälda organet finns eller på ett språk som kan godtas av det organet.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att lägga till aspekter som ska ingå i den tekniska dokumentationen enligt bilaga VII för att ta hänsyn till den tekniska utvecklingen, samt utveckling som skett under denna förordnings genomförandeprocess. Kommissionen ska därför säkerställa att den administrativa bördan för mikroföretag samt små och medelstora företag är proportionell.

Artikel 32

Förfaranden för bedömning av överensstämmelse för produkter med digitala element

1. Tillverkaren ska genomföra en bedömning av överensstämmelse avseende produkten med digitala element och de processer som införts av tillverkaren, där det ska fastställas om de väsentliga cybersäkerhetskraven i bilaga I uppfylls. Tillverkaren ska visa överensstämmelse med de väsentliga cybersäkerhetskraven genom att använda

   a) förfarandet för intern kontroll (baserat på modul A) enligt bilaga VIII,

   b) EU-typkontroll (baserat på modul B) enligt bilaga VIII, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII,

c) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII, eller

d) en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9, om sådan finns och i tillämpliga fall.

2. Vid bedömningen av om en viktig produkt med digitala element som omfattas av klass I som anges i bilaga III och de processer som införts av dess tillverkare överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I gäller att om tillverkaren inte har tillämpat – eller endast delvis har tillämpat – harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering på minst assuransnivå ”betydande” enligt artikel 27, eller om sådana harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering saknas, ska den berörda produkten med digitala element och de processer som införts av tillverkaren genomgå något av följande förfaranden med avseende på något av dessa väsentliga cybersäkerhetskrav:

a) EU-typkontroll (baserat på modul B) som anges i bilaga VIII, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII, eller

b) bedömning av överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII.

3. Om produkten är en viktig produkt med digitala element som omfattas av klass II enligt bilaga III ska tillverkaren visa överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I genom att använda något av följande förfaranden:

a) EU-typkontroll (baserat på modul B) enligt bilaga VIII, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII,

b) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII, eller

c) en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9 i denna förordning på minst assuransnivån ”betydande” enligt förordning (EU) 2019/881, om sådan finns och i tillämpliga fall.

4. Kritiska produkter med digitala element som förtecknas i bilaga IV ska visa överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I genom att använda

a) en europeisk ordning för cybersäkerhetscertifiering i enlighet med artikel 8.1, eller

b) om villkoren i artikel 8.1 inte är uppfyllda, något av de förfaranden som avses i punkt 3 i denna artikel.

5. Tillverkare av produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som omfattas av de kategorier som anges i bilaga III ska kunna visa överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I genom att använda ett av de förfaranden som avses i punkt 1 i denna artikel, förutsatt att den tekniska dokumentation som avses i artikel 31 görs tillgänglig för allmänheten när dessa produkter släpps ut på marknaden.

6. Mikroföretags och små och medelstora företags, inklusive uppstartsföretags, särskilda intressen och behov ska beaktas när avgifterna för bedömning av överensstämmelse fastställs, och dessa avgifter ska minskas i proportion till företagens särskilda intressen och behov.

Artikel 33

Stödåtgärder för mikroföretag och små och medelstora företag, inbegripet uppstartsföretag

1. Medlemsstaterna ska, när så är lämpligt, vidta följande åtgärder som är anpassade till mikroföretags och små företags behov:

   a) Anordna särskild informations- och utbildningsverksamhet om tillämpningen av denna förordning.

b) Inrätta en särskild kanal för kommunikation med mikroföretag och små företag och, när så är lämpligt, lokala myndigheter för att ge råd och besvara frågor om genomförandet av denna förordning.

c) Stödja provning och bedömning av överensstämmelse, när så är lämpligt även med stöd av Europeiska kompetenscentrumet för cybersäkerhet.

2. Medlemsstaterna får, när så är lämpligt, inrätta regulatoriska sandlådor för cyberresiliens. Sådana regulatoriska sandlådor ska tillhandahålla kontrollerade provmiljöer för innovativa produkter med digitala element för att underlätta utvecklingen, utformningen, valideringen och provningen av dem i syfte att uppfylla kraven i denna förordning under en begränsad tidsperiod innan de släpps ut på marknaden. Kommissionen och, när så är lämpligt, Enisa får tillhandahålla tekniskt stöd, rådgivning och verktyg för inrättande och drift av regulatoriska sandlådor. De regulatoriska sandlådorna ska inrättas under marknadskontrollmyndigheternas direkta tillsyn, vägledning och stöd. Medlemsstaterna ska genom Adco-gruppen informera kommissionen och de andra marknadskontrollmyndigheterna om inrättandet av en regulatorisk sandlåda. De regulatoriska sandlådorna ska inte påverka de behöriga myndigheternas tillsynsbefogenheter och korrigerande befogenheter. Medlemsstaterna ska säkerställa öppen, rättvis och transparent tillgång till regulatoriska sandlådor, och i synnerhet underlätta tillgång för mikroföretag och små företag, inbegripet uppstartsföretag.

3. I enlighet med artikel 26 ska kommissionen ge mikroföretag och små och medelstora företag vägledning om genomförandet av denna förordning.

4. Kommissionen ska tillkännage att ekonomiskt stöd inom ramen för unionens befintliga program är tillgängligt, särskilt för att minska den ekonomiska bördan för mikroföretag och små företag.

5. Mikroföretag och små företag får tillhandahålla alla delar av den tekniska dokumentation som anges i bilaga VII med användning av ett förenklat formulär. För detta ändamål ska kommissionen genom genomförandeakter specificera det förenklade formuläret för teknisk dokumentation med hänsyn till mikroföretagens och småföretagens behov, inbegripet hur de uppgifter som anges i bilaga VII ska tillhandahållas. Om ett mikroföretag eller ett småföretag väljer att tillhandahålla den information som anges enligt bilaga VII på ett förenklat sätt ska det använda det formulär som avses i denna punkt. Anmälda organ ska godta detta formulär för bedömning av överensstämmelse.

   Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

Artikel 34

Avtal om ömsesidigt erkännande

Med beaktande av den tekniska utvecklingsnivån och ett tredjelands förhållningssätt till bedömning av överensstämmelse får unionen ingå avtal om ömsesidigt erkännande med tredjeländer, i enlighet med artikel 218 i EUF-fördraget, för att främja och underlätta internationell handel.

Kapitel IV

Anmälan av organ för bedömning av överensstämmelse

Artikel 35

Anmälan

1. Medlemsstaterna ska till kommissionen och övriga medlemsstater anmäla vilka organ som fått i uppdrag att utföra bedömningar av överensstämmelse i enlighet med denna förordning.

2. Medlemsstaterna ska sträva efter att senast den … [24 månader från dagen för denna förordnings ikraftträdande] säkerställa att det finns ett tillräckligt antal anmälda organ i unionen för att utföra bedömningar av överensstämmelse, i syfte att undvika flaskhalsar och hinder för marknadstillträde.

Artikel 36

Anmälande myndigheter

1. Varje medlemsstat ska utse en anmälande myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs vid bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och vid kontroll, inklusive överensstämmelse med artikel 41.

2. Medlemsstaterna får besluta att den bedömning och övervakning som avses i punkt 1 ska utföras av ett nationellt ackrediteringsorgan i den mening som avses i och i enlighet med förordning (EG) nr 765/2008.

3. Om den anmälande myndigheten delegerar eller på annat sätt överlåter den bedömning, anmälan eller övervakning som avses i punkt 1 i denna artikel till ett organ som inte är offentligt, ska detta organ vara en juridisk person och i tillämpliga delar följa artikel 37. Detta organ ska dessutom ha vidtagit åtgärder för att täcka det ansvar som följer av dess verksamhet.

4. Den anmälande myndigheten ska ta fullt ansvar för de uppgifter som utförs av det organ som avses i punkt 3.

Artikel 37

Krav på anmälande myndigheter

1. En anmälande myndighet ska vara inrättad på ett sådant sätt att det inte uppstår någon intressekonflikt med organen för bedömning av överensstämmelse.

2. En anmälande myndighet ska vara organiserad och fungera på ett sådant sätt att dess verksamhet är objektiv och opartisk.

3. En anmälande myndighet ska vara organiserad på ett sådant sätt att alla beslut som rör anmälan av ett organ för bedömning av överensstämmelse fattas av annan behörig personal än den som utförde bedömningen.

4. En anmälande myndighet får inte erbjuda eller utföra sådan verksamhet som utförs av organ för bedömning av överensstämmelse eller konsulttjänster på kommersiell eller konkurrensmässig grund.

5. En anmälande myndighet ska skydda den konfidentiella information som den mottar.

6. En anmälande myndighet ska ha tillgång till tillräckligt med personal med lämplig kompetens för att korrekt kunna utföra sina uppgifter.

Artikel 38

Anmälande myndigheters informationsskyldighet

1. Medlemsstaterna ska informera kommissionen om sina förfaranden för bedömning och anmälan av organ för bedömning av överensstämmelse och för övervakning av anmälda organ samt om eventuella ändringar.

2. Kommissionen ska offentliggöra den information som avses i punkt 1.

Artikel 39

Krav på anmälda organ

1. För anmälning ska ett organ för bedömning av överensstämmelse uppfylla de krav som anges i punkterna 2–12.

2. Ett organ för bedömning av överensstämmelse ska inrättas i enlighet med nationell rätt och vara juridisk person.

3. Ett organ för bedömning av överensstämmelse ska vara ett tredjepartsorgan som är oberoende av den organisation eller produkt med digitala element som den bedömer.

   Detta organ får vara ett tredjepartsorgan som hör till en näringslivsorganisation eller branschorganisation som företräder företag som är involverade i utformning, utveckling, tillverkning, tillhandahållande, montering, användning eller underhåll av de produkter med digitala element som det bedömer, förutsatt att det kan styrkas att organet är oberoende och att intressekonflikter saknas.

4. Ett organ för bedömning av överensstämmelse, dess högsta ledning och den personal som ansvarar för utförandet av bedömningen av överensstämmelse får inte utgöras av den som utformar, utvecklar, tillverkar, levererar, importerar, distribuerar, installerar, köper, äger, använder eller underhåller de produkter med digitala element som bedöms och inte heller av en representant för någon av dessa parter. Detta ska inte hindra att bedömda produkter som är nödvändiga för verksamheten vid organet för bedömning av överensstämmelse används, eller att produkterna används för personligt bruk.

Ett organ för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för utförandet av bedömningen av överensstämmelse får inte vara direkt inblandade i utformningen, utvecklingen, tillverkningen, importen, distributionen, marknadsföringen, installationen, användningen eller underhållet av de produkter med digitala element som de bedömer, och inte heller representera parter som bedriver sådan verksamhet. De får inte delta i någon verksamhet som kan påverka deras objektivitet och integritet i samband med de bedömningar av överensstämmelse för vilka de har anmälts. Detta ska framför allt gälla konsulttjänster.

Organ för bedömning av överensstämmelse ska säkerställa att deras dotterbolags eller underentreprenörers verksamhet inte påverkar konfidentialiteten, objektiviteten eller opartiskheten i organens bedömningar av överensstämmelse.

5. Organ för bedömning av överensstämmelse och deras personal ska utföra bedömningar av överensstämmelse med största möjliga yrkesintegritet, ha erforderlig teknisk kompetens på det specifika området och vara fria från alla påtryckningar och incitament, i synnerhet ekonomiska incitament, som kan påverka deras omdöme eller resultaten av deras bedömningar av överensstämmelse; detta gäller särskilt påtryckningar och incitament från personer eller grupper av personer som berörs av bedömningarnas resultat.

6. Ett organ för bedömning av överensstämmelse ska kunna utföra alla de uppgifter avseende bedömning av överensstämmelse som avses i bilaga VIII och för vilka det har anmälts, oavsett om dessa uppgifter utförs av organet självt eller för dess räkning och under dess ansvar.

   Vid alla tidpunkter och vid varje bedömning av överensstämmelse och för varje typ eller kategori av produkt med digitala element för vilka det har anmälts ska organet för bedömning av överensstämmelse ha till sitt förfogande

   a) personal med teknisk kunskap och tillräcklig och lämplig erfarenhet för att utföra bedömningen av överensstämmelse,

   b) beskrivningar av förfaranden enligt vilka bedömningar av överensstämmelse utförs; dessa beskrivningar ska säkerställa att förfarandena är transparenta och kan reproduceras. Organet ska ha lämpliga rutiner och förfaranden för att skilja mellan de uppgifter som det utför i sin egenskap av anmält organ och annan verksamhet, och

c) förfaranden som gör det möjligt för organet att utöva sin verksamhet med vederbörlig hänsyn tagen till ett företags storlek, bransch och struktur, den berörda produktteknikens komplexitet och eventuell mass- eller serietillverkning.

Organet för bedömning av överensstämmelse ska ha de nödvändiga medlen för att korrekt kunna utföra de tekniska och administrativa uppgifterna i samband med bedömningen av överensstämmelse och ska ha tillgång till den utrustning och de hjälpmedel som är nödvändiga.

7. Den personal som ansvarar för att utföra bedömningen av överensstämmelse ska ha

a) fullgod teknisk och yrkesinriktad utbildning som täcker all slags bedömning av överensstämmelse för vilken organet för bedömning av överensstämmelse har anmälts,

b) tillfredsställande kunskap om kraven för de bedömningar som de utför och befogenhet att utföra dessa bedömningar,

c) tillräcklig kännedom och insikt om de väsentliga cybersäkerhetskraven i bilaga I, de tillämpliga harmoniserade standarderna och gemensamma specifikationerna och de relevanta bestämmelserna i unionsharmoniseringslagstiftning och genomförandeakter,

d) förmåga att upprätta intyg, protokoll och rapporter som visar att bedömningarna har utförts.

8. Det ska garanteras att organen för bedömning av överensstämmelse, deras ledning och bedömningspersonal är opartiska.

Ersättningen till organets ledning och bedömningspersonal får inte vara beroende av antalet bedömningar som gjorts eller resultaten av bedömningarna.

9. Organ för bedömning av överensstämmelse ska vara ansvarsförsäkrade, såvida inte ansvaret åligger medlemsstaten enligt nationell rätt eller medlemsstaten själv tar direkt ansvar för bedömningen av överensstämmelse.

10. Personalen vid ett organ för bedömning av överensstämmelse ska iaktta tystnadsplikt beträffande all information som de erhåller vid utförandet av sina uppgifter enligt bilaga VIII eller bestämmelser i nationell rätt som genomför den, utom gentemot marknadskontrollmyndigheterna i den medlemsstat där verksamheten bedrivs. Äganderätten ska vara skyddad. Organet för bedömning av överensstämmelse ska ha dokumenterade förfaranden som säkerställer uppfyllandet av kraven i denna punkt.

11. Organ för bedömning av överensstämmelse ska delta i, eller säkerställa att deras bedömningspersonal känner till, det relevanta standardiseringsarbetet och det arbete som utförs i samordningsgruppen för anmälda organ, som inrättats enligt artikel 51, och de ska som generella riktlinjer tillämpa de administrativa beslut och dokument som är resultatet av gruppens arbete.

12. Organen för bedömning av överensstämmelse ska fungera enligt konsekventa, rättvisa, proportionella och rimliga villkor och bestämmelser, samtidigt som onödiga bördor för de ekonomiska aktörerna undviks, och när det gäller avgifter särskilt beakta mikroföretags samt små och medelstora företags intressen.

Artikel 40

Presumtion om överensstämmelse för anmälda organ

För ett organ för bedömning av överensstämmelse som kan visa att det uppfyller kriterierna i de relevanta harmoniserade standarderna eller delar av dem till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning* ska en presumtion om överensstämmelse med kraven i artikel 39 gälla, i den mån som dessa krav omfattas av de tillämpliga harmoniserade standarderna.

Artikel 41

Dotterbolag och underentreprenörer till anmälda organ

1. Om det anmälda organet lägger ut specifika uppgifter med anknytning till bedömningen av överensstämmelse på underentreprenad eller anlitar ett dotterbolag ska det säkerställa att underentreprenören eller dotterbolaget uppfyller kraven som anges i artikel 39 och informera den anmälande myndigheten om detta.

2. De anmälda organen ska ta det fulla ansvaret för underentreprenörernas eller dotterbolagens uppgifter, oavsett var de är etablerade.

3. Verksamhet får läggas ut på underentreprenad eller utföras av ett dotterbolag endast om tillverkaren samtycker till det.

4. De anmälda organen ska se till att den anmälande myndigheten har tillgång till de relevanta dokumenten rörande bedömningen av underentreprenörens eller dotterbolagets kvalifikationer och det arbete som dessa har utfört i enlighet med denna förordning.

Artikel 42

Ansökan om anmälan

1. Ett organ för bedömning av överensstämmelse ska lämna in en ansökan om anmälan till den anmälande myndigheten i den medlemsstat där det är etablerat.

2. Ansökan ska åtföljas av en beskrivning av de bedömningar av överensstämmelse, det eller de förfaranden för bedömning av överensstämmelse och den eller de produkter med digitala element som organet anser sig ha kompetens för samt ett ackrediteringsintyg, om det finns ett sådant, som utfärdats av ett nationellt ackrediteringsorgan och där det intygas att organet för bedömning av överensstämmelse uppfyller kraven i artikel 39.

3. Om organet för bedömning av överensstämmelse inte kan uppvisa något ackrediteringsbevis ska det ge den anmälande myndigheten alla de underlag som krävs för kontroll, erkännande och regelbunden tillsyn av att det uppfyller kraven i artikel 39.

Artikel 43

Anmälningsförfarande

1. De anmälande myndigheterna ska endast anmäla de organ för bedömning av överensstämmelse som har uppfyllt kraven i artikel 39.

2. Den anmälande myndigheten ska underrätta kommissionen och de andra medlemsstaterna via databasen Nando som utvecklats och förvaltas av kommissionen.

3. Anmälan ska innehålla detaljerade uppgifter om bedömningarna av överensstämmelse, modulerna för bedömning av överensstämmelse och de berörda produkterna med digitala element samt ett relevant intyg om kompetens.

4. Om en anmälan inte grundar sig på ett sådant ackrediteringsintyg som avses i artikel 42.2 ska den anmälande myndigheten ge kommissionen och de andra medlemsstaterna de skriftliga underlag som styrker att organet för bedömning av överensstämmelse har erforderlig kompetens och att de system som behövs för att se till att organet övervakas regelbundet och fortsätter att uppfylla kraven i artikel 39 har inrättats.

5. Det berörda organet får bedriva verksamhet som anmält organ endast om kommissionen eller de andra medlemsstaterna inte har rest några invändningar inom två veckor från anmälan, i de fall då ett ackrediteringsintyg används, eller inom två månader från anmälan, i de fall då ingen ackreditering används.

   Endast ett sådant organ ska anses vara ett anmält organ vid tillämpning av denna förordning.

6. Kommissionen och övriga medlemsstater ska underrättas om eventuella relevanta senare ändringar av anmälan.

Artikel 44

Identifikationsnummer och förteckningar över anmälda organ

1. Kommissionen ska tilldela varje anmält organ ett identifikationsnummer.

   Organet ska tilldelas ett enda sådant nummer även om det anmälts enligt flera unionsrättsakter.

2. Kommissionen ska offentliggöra förteckningen över de organ som anmälts enligt denna förordning, inklusive de identifikationsnummer som de har tilldelats och den verksamhet som de har anmälts för.

   Kommissionen ska säkerställa att denna förteckning hålls aktuell.

Artikel 45

Ändringar i anmälan

1. Om en anmälande myndighet har konstaterat eller har informerats om att ett anmält organ inte längre uppfyller de krav som anges i artikel 39 eller att det underlåter att fullgöra sina skyldigheter ska myndigheten i förekommande fall, beroende på hur allvarlig underlåtenheten att uppfylla kraven eller fullgöra skyldigheterna är, begränsa anmälan eller återkalla den tillfälligt eller slutgiltigt. Den ska omedelbart informera kommissionen och de andra medlemsstaterna om detta.

2. I händelse av begränsning eller tillfällig eller slutgiltig återkallelse av anmälan eller om det anmälda organet har upphört med verksamheten ska den anmälande medlemsstaten vidta lämpliga åtgärder för att säkerställa att det anmälda organets ärenden antingen behandlas av ett annat anmält organ eller hålls tillgängliga för de ansvariga anmälande myndigheterna och marknadskontrollmyndigheterna på deras begäran.

Artikel 46

Ifrågasättande av de anmälda organens kompetens

1. Kommissionen ska undersöka alla fall där den hyser tvivel, eller där den upplysts om sådana tvivel, om ett anmält organs kompetens eller ett anmält organs fortsatta uppfyllande av de krav och skyldigheter som det omfattas av.

2. Den anmälande medlemsstaten ska på begäran ge kommissionen all information om grunderna för anmälan eller det berörda organets fortsatta kompetens.

3. Kommissionen ska säkerställa att all känslig information som den erhåller under sina undersökningar behandlas konfidentiellt.

4. Om kommissionen konstaterar att ett anmält organ inte uppfyller eller inte längre uppfyller kraven för anmälan ska den meddela detta till den anmälande medlemsstaten och anmoda medlemsstaten att vidta erforderliga korrigerande åtgärder, t.ex. vid behov återta anmälan.

Artikel 47

De anmälda organens operativa skyldigheter

1. Anmälda organ ska utföra bedömningar av överensstämmelse i enlighet med förfarandena för bedömning av överensstämmelse i artikel 32 och bilaga VIII.

2. Bedömningar av överensstämmelse ska utföras på ett proportionellt sätt så att de inte blir onödigt betungande för de ekonomiska aktörerna. Organ för bedömning av överensstämmelse ska utöva sin verksamhet med vederbörlig hänsyn till företags storlek, särskilt i fråga om mikroföretag och små och medelstora företag, bransch, struktur, komplexitet och cybersäkerhetsrisknivån hos produkterna med digitala element och den berörda tekniken och om produktionsprocessen karaktäriseras som mass- eller serietillverkning.

3. Anmälda organ ska dock iaktta den grad av noggrannhet och den skyddsnivå som krävs för att produkten med digitala element ska överensstämma med denna förordning.

4. Om ett anmält organ konstaterar att en tillverkare inte uppfyller de krav som anges i bilaga I eller motsvarande harmoniserade standarder eller gemensamma specifikationer som avses i artikel 27, ska det begära att tillverkaren vidtar lämpliga korrigerande åtgärder, och det ska inte utfärda ett intyg om överensstämmelse.

5. Om ett anmält organ vid övervakning av överensstämmelse efter det att ett intyg har utfärdats konstaterar att en produkt med digitala element inte längre uppfyller kraven i denna förordning, ska det kräva att tillverkaren vidtar lämpliga korrigerande åtgärder, och vid behov ska intyget tillfälligt eller slutgiltigt återkallas.

6. Om korrigerande åtgärder inte vidtas eller inte får önskad effekt ska det anmälda organet, beroende på vad som är lämpligt, begränsa eller tillfälligt, alternativt slutgiltigt, återkalla alla intyg.

Artikel 48

Överklagande av de anmälda organens beslut

Medlemsstaterna ska säkerställa att det finns ett förfarande för överklagande av de anmälda organens beslut.

Artikel 49

De anmälda organens informationsskyldighet

1. De anmälda organen ska underrätta den anmälande myndigheten om följande:

   a) Avslag på ansökan om intyg, eller begränsning, tillfälligt tillbakadragande eller återkallelse av ett intyg.

   b) Omständigheter som inverkar på räckvidden och villkoren för anmälan.

c) Begäran från marknadskontrollmyndigheterna om information om bedömningar av överensstämmelse.

d) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

2. De anmälda organen ska ge de andra organ som anmälts enligt denna förordning, och som utför liknande bedömningar av överensstämmelse som täcker samma produkter med digitala element, relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

Artikel 50

Utbyte av erfarenhet

Kommissionen ska se till att det förekommer utbyte av erfarenhet mellan de myndigheter i medlemsstaterna som ansvarar för riktlinjerna för anmälan.

Artikel 51

Samordning av anmälda organ

1. Kommissionen ska säkerställa att lämplig samordning och samarbete mellan de anmälda organen införs och att samordningen och samarbetet bedrivs på ett tillfredsställande sätt genom en sektorsövergripande grupp av anmälda organ.

2. Medlemsstaterna ska säkerställa att de organ som de har anmält deltar i gruppens arbete direkt eller genom utsedda företrädare.

Kapitel V

Marknadskontroll och verkställighet

Artikel 52

Marknadskontroll och kontroll av produkter med digitala element på unionsmarknaden

1. Förordning (EU) 2019/1020 ska tillämpas på produkter med digitala element som omfattas av den här förordningen.

2. Varje medlemsstat ska utse en eller flera marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av denna förordning. Medlemsstaterna får utse en befintlig eller en ny myndighet till att fungera som marknadskontrollmyndighet inom ramen för denna förordning.

3. De marknadskontrollmyndigheter som utsetts enligt punkt 2 i denna artikel ska också ansvara för att utföra marknadskontroll rörande de skyldigheter för förvaltare av programvara med fri och öppen källkod som fastställs i artikel 24. Om en marknadskontrollmyndighet konstaterar att en förvaltare av programvara med fri och öppen källkod inte uppfyller de skyldigheter som anges i den artikeln ska den kräva att förvaltaren av programvaran med fri och öppen källkod säkerställer att alla lämpliga korrigerande åtgärder vidtas. Förvaltare av programvara med fri och öppen källkod ska säkerställa att alla lämpliga korrigerande åtgärder vidtas med avseende på deras skyldigheter enligt denna förordning.

4. När så är lämpligt ska marknadskontrollmyndigheterna samarbeta med de nationella myndigheter för cybersäkerhetscertifiering som utsetts enligt artikel 58 i förordning (EU) 2019/881 och regelbundet utbyta information med dessa. När det gäller tillsynen över genomförandet av rapporteringsskyldigheterna enligt artikel 14 i den här förordningen ska de utsedda marknadskontrollmyndigheterna samarbeta och regelbundet utbyta information med de CSIRT-enheter som utsetts till samordnare och Enisa.

5. Marknadskontrollmyndigheterna får be en CSIRT-enhet som utsetts till samordnare eller Enisa att ge tekniska råd i frågor som rör genomförandet och efterlevnaden av denna förordning. Vid genomförandet av en utredning enligt artikel 54 får marknadskontrollmyndigheterna be CSIRT-enheten som utsetts till samordnare eller Enisa att tillhandahålla en analys till stöd för utvärderingar av överensstämmelse för produkter med digitala element.

6. När så är relevant ska marknadskontrollmyndigheterna samarbeta med andra marknadskontrollmyndigheter som utsetts på grundval av annan unionsharmoniseringslagstiftning än denna förordning och regelbundet utbyta information med dessa.

7. Marknadskontrollmyndigheterna ska vid behov samarbeta med de myndigheter som utövar tillsyn över unionens dataskyddsrätt. I detta samarbete ingår att underrätta dessa myndigheter om alla iakttagelser av betydelse för deras fullgörande av sina befogenheter, inbegripet utfärdande av vägledning och råd enligt punkt 10 om vägledningen och råden rör behandling av personuppgifter.

   Myndigheter som utövar tillsyn över unionens dataskyddsrätt ska ha befogenhet att begära och få åtkomst till all dokumentation som skapas eller upprätthålls enligt denna förordning när de behöver åtkomst till sådan dokumentation för att utföra sina uppgifter. De ska underrätta de utsedda marknadskontrollmyndigheterna i den berörda medlemsstaten om varje sådan begäran.

8. Medlemsstaterna ska säkerställa att de utsedda marknadskontrollmyndigheterna har tillräckliga ekonomiska och tekniska resurser, inbegripet vid behov verktyg för automatisk databehandling samt personalresurser med nödvändig cybersäkerhetskompetens för att kunna fullgöra sina uppgifter enligt denna förordning.

9. Kommissionen ska uppmuntra och underlätta utbytet av erfarenhet mellan utsedda marknadskontrollmyndigheter.

10. Marknadskontrollmyndigheterna får ge ekonomiska aktörer vägledning och råd om genomförandet av denna förordning, med stöd av kommissionen och CSIRT-enheter och Enisa när så är lämpligt.

11. Marknadskontrollmyndigheterna ska informera konsumenterna om var klagomål som kan indikera bristande överensstämmelse med denna förordning, i enlighet med artikel 11 i förordning (EU) 2019/1020 lämnas in, och ska informera konsumenterna om var och hur de kan få tillgång till mekanismer för att underlätta rapportering av sårbarheter, incidenter och cyberhot som kan påverka produkter med digitala element.

12. Marknadskontrollmyndigheterna ska när så är lämpligt underlätta samarbetet med berörda parter, inbegripet vetenskapliga organisationer samt forsknings- och konsumentorganisationer.

13. Marknadskontrollmyndigheterna ska årligen rapportera resultaten av relevant marknadskontroll till kommissionen. De utsedda marknadskontrollmyndigheterna ska utan dröjsmål rapportera till kommissionen och berörda nationella konkurrensmyndigheter om all information som framkommit i samband med marknadskontrollen och som kan vara av potentiellt intresse för tillämpningen av unionens konkurrensrätt.

14. För produkter med digitala element som omfattas av denna förordning och som klassificeras som AI-system med hög risk enligt artikel 6 i förordning (EU) 2024/1689 ska de marknadskontrollmyndigheter som utsetts enligt den förordningen vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i den här förordningen. De marknadskontrollmyndigheter som utsetts enligt förordning (EU) 2024/1689 ska vid behov samarbeta med de marknadskontrollmyndigheter som utsetts i enlighet med den här förordningen och, när det gäller tillsyn över genomförandet av rapporteringsskyldigheten enligt artikel 14 i den här förordningen, med de CSIRT-enheter som utsetts till samordnare och Enisa. De marknadskontrollmyndigheter som utsetts enligt förordning (EU) 2024/1689 ska i synnerhet underrätta de marknadskontrollmyndigheter som utsetts enligt den här förordningen om alla iakttagelser av betydelse för fullgörandet av deras uppgifter förbundna med genomförandet av den här förordningen.

15. En Adco-grupp ska inrättas för en enhetlig tillämpning av denna förordning, enligt artikel 30.2 i förordning (EU) 2019/1020. Adco-gruppen ska bestå av företrädare för de utsedda marknadskontrollmyndigheterna och, om så är lämpligt, företrädare för de centrala samordningskontoren. Adco-gruppen ska också behandla särskilda frågor som rör marknadskontroll rörande de skyldigheter som åläggs förvaltare av programvara med fri och öppen källkod.

16. Marknadskontrollmyndigheterna ska övervaka hur tillverkarna har tillämpat de kriterier som avses i artikel 13.8 när de fastställer stödperioden för sina produkter med digitala element.

Adco-gruppen ska i en allmänt tillgänglig och användarvänlig form offentliggöra relevant statistik om kategorier av produkter med digitala element, inbegripet genomsnittliga stödperioder, vilka fastställs av tillverkaren enligt artikel 13.8, samt tillhandahålla vägledning som inbegriper vägledande stödperioder för kategorier av produkter med digitala element.

Om uppgifterna tyder på otillräckliga stödperioder för specifika kategorier av produkter med digitala element får Adco-gruppen utfärda rekommendationer till marknadskontrollmyndigheterna om att inrikta sin verksamhet på sådana kategorier av produkter med digitala element.

Artikel 53

Tillgång till data och dokumentation

När det behövs för att bedöma överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I för produkter med digitala element och de processer som införts av tillverkarna ska marknadskontrollmyndigheterna på motiverad begäran beviljas tillgång, på ett språk som lätt kan förstås av dem, till de data som behövs för att bedöma utformningen, utvecklingen, produktionen och sårbarhetshanteringen av sådana produkter, inbegripet tillhörande intern dokumentation hos den berörda ekonomiska aktören.

Artikel 54

Förfarande på nationell nivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk

1. Om marknadskontrollmyndigheten i en medlemsstat har tillräckliga skäl att anse att en produkt med digitala element, inbegripet dess sårbarhetshantering, utgör en betydande cybersäkerhetsrisk, ska den, utan onödigt dröjsmål och om lämpligt i samarbete med den berörda CSIRT-enheten, göra en utvärdering av den berörda produkten med digitala element med avseende på dess uppfyllande av alla krav som fastställs i denna förordning. De berörda ekonomiska aktörerna ska när så krävs samarbeta med marknadskontrollmyndigheten.

Om marknadskontrollsmyndigheten vid utvärderingen konstaterar att en produkt med digitala element inte uppfyller kraven i denna förordning ska den utan dröjsmål ålägga den berörda ekonomiska aktören att vidta alla lämpliga korrigerande åtgärder för att se till att produkten med digitala element uppfyller dessa krav eller dra tillbaka produkten från marknaden eller återkalla den inom en rimlig tid som marknadskontrollmyndigheten fastställer i förhållande till typen av cybersäkerhetsrisk.

Marknadskontrollmyndigheten ska informera det berörda anmälda organet om detta. Artikel 18 i förordning (EU) 2019/1020 ska tillämpas på de korrigerande åtgärderna.

2. När marknadskontrollmyndigheterna fastställer betydelsen av en cybersäkerhetsrisk som avses i punkt 1 i denna artikel ska de också beakta icke-tekniska riskfaktorer, särskilt de som fastställts till följd av samordnade säkerhetsriskbedömningar av kritiska leveranskedjor på unionsnivå som genomförs i enlighet med artikel 22 i direktiv (EU) 2022/2555. Om en marknadskontrollmyndighet har tillräckliga skäl att anse att en produkt med digitala element utgör en betydande cybersäkerhetsrisk mot bakgrund av icke-tekniska riskfaktorer ska den informera de behöriga myndigheter som utsetts eller inrättats enligt artikel 8 i direktiv (EU) 2022/2555 och när så krävs samarbeta med dessa myndigheter.

3. Om marknadskontrollmyndigheten anser att den bristande överensstämmelsen inte bara gäller det nationella territoriet, ska den informera kommissionen och de andra medlemsstaterna om utvärderingsresultaten och om de åtgärder som den har ålagt den ekonomiska aktören att vidta.

4. Den ekonomiska aktören ska säkerställa att alla lämpliga korrigerande åtgärder vidtas i fråga om alla berörda produkter med digitala element som den har tillhandahållit på unionsmarknaden.

5. Om den ekonomiska aktören inte vidtar lämpliga korrigerande åtgärder inom den period som avses i punkt 1 andra stycket, ska marknadskontrollmyndigheten vidta alla lämpliga provisoriska åtgärder för att förbjuda eller begränsa tillhandahållandet av produkten med digitala element på sin nationella marknad, dra tillbaka produkten från den marknaden eller återkalla den.

   Myndigheten ska utan dröjsmål anmäla dessa åtgärder till kommissionen och de andra medlemsstaterna.

6. I den information som avses i punkt 5 ska alla tillgängliga uppgifter ingå, särskilt de uppgifter som krävs för att kunna identifiera den produkt med digitala element som inte uppfyller kraven, dess ursprung, vilken typ av bristande överensstämmelse som görs gällande och den risk produkten utgör, vilken typ av nationell åtgärd som vidtagits och åtgärdens varaktighet samt den berörda ekonomiska aktörens synpunkter. Marknadskontrollmyndigheten ska särskilt ange om den bristande överensstämmelsen beror på en eller flera av följande orsaker:

   a) Produkten med digitala element eller de processer som införts av tillverkaren uppfyller inte de väsentliga cybersäkerhetskraven i bilaga I.

   b) Det finns brister i de harmoniserade standarder, de europeiska ordningar för cybersäkerhetscertifiering eller de gemensamma specifikationer som avses i artikel 27.

7. Marknadskontrollmyndigheterna i andra medlemsstater än den som inledde förfarandet ska utan dröjsmål informera kommissionen och de andra medlemsstaterna om alla vidtagna åtgärder och eventuella kompletterande uppgifter som de har tillgång till med avseende på bristande överensstämmelse hos den berörda produkten med digitala element samt eventuella invändningar mot den anmälda nationella åtgärden.

8. Åtgärden ska anses vara berättigad om ingen medlemsstat eller kommissionen har gjort invändningar inom tre månader efter mottagandet av den anmälan som avses i punkt 5 i denna artikel mot en provisorisk åtgärd som vidtagits av en medlemsstat. Detta påverkar inte den ekonomiska aktörens processuella rättigheter i enlighet med artikel 18 i förordning (EU) 2019/1020.

9. Marknadskontrollmyndigheterna i alla medlemsstater ska säkerställa att lämpliga begränsande åtgärder vidtas utan dröjsmål med avseende på den berörda produkten med digitala element, till exempel att produkten dras tillbaka från marknaden.

Artikel 55

Unionens förfarande i fråga om skyddsåtgärder

1. Om en medlemsstat inom tre månader efter mottagandet av den anmälan som avses i artikel 54.5 har gjort invändningar mot en åtgärd som vidtagits av en annan medlemsstat, eller om kommissionen anser att åtgärden strider mot unionsrätten, ska kommissionen utan dröjsmål inleda samråd med den berörda medlemsstaten och den eller de ekonomiska aktörerna och ska utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten ska kommissionen besluta om den nationella åtgärden är berättigad eller inte inom nio månader från den anmälan som avses i artikel 54.5 och meddela beslutet till den berörda medlemsstaten.

2. Om den nationella åtgärden anses vara berättigad, ska alla medlemsstater vidta de åtgärder som krävs för att säkerställa att den produkt med digitala element som inte uppfyller kraven dras tillbaka från deras marknader och underrätta kommissionen om detta. Om den nationella åtgärden inte anses vara berättigad ska den berörda medlemsstaten upphäva åtgärden.

3. Om den nationella åtgärden anses vara berättigad och produktens bristande överensstämmelse kan tillskrivas brister i de harmoniserade standarderna ska kommissionen tillämpa det förfarande som föreskrivs i artikel 11 i förordning (EU) nr 1025/2012.

4. Om den nationella åtgärden anses vara berättigad och produktens bristande överensstämmelse kan tillskrivas brister i en europeisk ordning för cybersäkerhetscertifiering som avses i artikel 27, ska kommissionen överväga att ändra eller upphäva eventuella delegerade akter som antagits enligt artikel 27.9 som specificerar presumtionen om överensstämmelse för det certifieringssystemet.

5. Om den nationella åtgärden anses vara berättigad och produktens bristande överensstämmelse kan tillskrivas i de gemensamma specifikationer som avses i artikel 27, ska kommissionen överväga att ändra eller upphäva eventuella genomförandeakter som antagits enligt artikel 27.2 som fastställer dessa gemensamma specifikationer.

Artikel 56

Förfarande på unionsnivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk

1. Om kommissionen har tillräckliga skäl, inbegripet baserat på information från Enisa, att anse att en produkt med digitala element som utgör en betydande cybersäkerhetsrisk inte uppfyller kraven enligt denna förordning ska den informera de berörda marknadskontrollmyndigheterna. Om marknadskontrollmyndigheterna gör en utvärdering av produkten med digitala element som kan utgöra en betydande cybersäkerhetsrisk med avseende på dess överensstämmelse med kraven i denna förordning ska de förfaranden som avses i artiklarna 54 och 55 tillämpas.

2. Om kommissionen har tillräckliga skäl att anse att en produkt med digitala element utgör en betydande cybersäkerhetsrisk mot bakgrund av icke-tekniska riskfaktorer ska den informera de berörda marknadskontrollmyndigheterna och, om så är lämpligt, de behöriga myndigheter som utsetts eller inrättats enligt artikel 8 i direktiv (EU) 2022/2555 och när så krävs samarbeta med dessa myndigheter. Kommissionen ska också beakta relevansen hos de identifierade riskerna för produkten med digitala element med tanke på sina uppgifter avseende de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor på unionsnivå som föreskrivs i artikel 22 i direktiv (EU) 2022/2555, och vid behov samråda med den samarbetsgrupp som inrättats enligt artikel 14 i direktiv (EU) 2022/2555 och Enisa.

3. Vid omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad, och där kommissionen har tillräckliga skäl att anse att den produkt med digitala element som avses i punkt 1 fortfarande inte uppfyller kraven enligt denna förordning och inga effektiva åtgärder har vidtagits av de berörda marknadskontrollmyndigheterna, ska kommissionen göra en utvärdering av överensstämmelsen och får begära att Enisa tillhandahåller en analys för att stödja den. Kommissionen ska underrätta de berörda marknadskontrollmyndigheterna om detta. De berörda ekonomiska aktörerna ska när så krävs samarbeta med Enisa.

4. Baserat på den utvärdering som avses i punkt 3 får kommissionen besluta att en korrigerande eller begränsande åtgärd krävs på unionsnivå. Därför ska kommissionen utan dröjsmål samråda med de berörda medlemsstaterna och berörda ekonomiska aktörer (en eller flera).

5. Baserat på det samråd som avses i punkt 4 i denna artikel får kommissionen anta genomförandeakter för att föreskriva korrigerande eller begränsande åtgärder på unionsnivå, inbegripet krav på att de berörda produkterna med digitala element ska dras tillbaka från marknaden eller återkallas, inom en rimlig tid i förhållande till typen av risk. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

6. Kommissionen ska omedelbart delge berörda ekonomiska aktörer de genomförandeakter som avses i punkt 5. Medlemsstaterna ska genomföra dessa genomförandeakter utan dröjsmål och underrätta kommissionen om detta.

7. Punkterna 3–6 ska vara tillämpliga under den tid som den exceptionella situation som motiverade kommissionens ingripande varar, under förutsättning att den berörda produkten med digitala element inte bringas till överensstämmelse med denna förordning.

Artikel 57

Produkter med digitala element som överensstämmer med kraven men utgör en betydande cybersäkerhetsrisk

1. Marknadskontrollmyndigheten i en medlemsstat ska kräva att en ekonomisk aktör vidtar alla lämpliga åtgärder om den, efter att ha gjort en utvärdering enligt artikel 54, konstaterar att en produkt med digitala element och de processer som införts av tillverkaren överensstämmer med denna förordning, men att de utgör en betydande cybersäkerhetsrisk och en risk för

   a) människors hälsa eller säkerhet,

   b) efterlevnad av skyldigheter enligt unionsrätt eller nationell rätt avsedda att skydda de grundläggande rättigheterna,

c) tillgången till och autenticiteten, riktigheten eller konfidentialiteten för tjänster som de väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555 erbjuder med användning av ett elektroniskt informationssystem, eller

d) andra aspekter av skyddet av allmänintresset.

De åtgärder som avses i första stycket får omfatta åtgärder för att säkerställa att den berörda produkten med digitala element och de processer som införts av tillverkaren inte längre utgör de berörda riskerna när den tillhandahålls på marknaden, tillbakadragande från marknaden av den berörda produkten med digitala element eller återkallande av den, och ska stå i proportion till typen av risker.

2. Tillverkaren eller andra berörda ekonomiska aktörer ska säkerställa att korrigerande åtgärder vidtas i fråga om berörda produkter med digitala element som de har tillhandahållit på marknaden i unionen inom den tidsfrist som fastställts av den marknadskontrollmyndighet i medlemsstaten som avses i punkt 1.

3. Medlemsstaten ska omedelbart underrätta kommissionen och de andra medlemsstaterna om de åtgärder som vidtagits enligt punkt 1. Informationen ska innehålla alla tillgängliga uppgifter, särskilt de uppgifter som krävs för att kunna identifiera den berörda produkten med digitala element, dess ursprung och leveranskedja, vilken typ av risk som produkten utgör samt vilken typ av nationella åtgärder som vidtagits och deras varaktighet.

4. Kommissionen ska utan dröjsmål inleda samråd med medlemsstaterna och den berörda ekonomiska aktören samt utvärdera de nationella åtgärder som vidtagits. På grundval av utvärderingsresultaten ska kommissionen besluta om åtgärden är berättigad eller inte, och vid behov föreslå lämpliga åtgärder.

5. Kommissionen ska rikta det beslut som avses i punkt 4 till medlemsstaterna.

6. Om kommissionen har tillräckliga skäl, däribland baserat på information från Enisa, att anse att en produkt med digitala element som uppfyller kraven i denna förordning ändå utgör de risker som avses i punkt 1 i denna artikel, ska den informera och begära att berörda marknadskontrollmyndigheter (en eller flera) gör en utvärdering och följer de förfaranden som avses i artikel 54 och i punkterna 1, 2 och 3 i denna artikel.

7. Vid omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad, och där kommissionen har tillräckliga skäl att anse att den produkt med digitala element som avses i punkt 6 fortsätter att utgöra de risker som avses i punkt 1 och att inga effektiva åtgärder har vidtagits av de berörda nationella marknadskontrollmyndigheterna, ska kommissionen göra en utvärdering av de risker som produkten med digitala element utgör och får begära att Enisa tillhandahåller en analys för att stödja denna utvärdering och ska underrätta de berörda marknadskontrollmyndigheterna om detta. De berörda ekonomiska aktörerna ska när så krävs samarbeta med Enisa.

8. Baserat på den utvärdering som avses i punkt 7 får kommissionen besluta att en korrigerande eller begränsande åtgärd krävs på unionsnivå. Därför ska kommissionen utan dröjsmål samråda med de berörda medlemsstaterna och berörda ekonomiska aktörer (en eller flera).

9. Baserat på det samråd som avses i punkt 8 i denna artikel får kommissionen anta genomförandeakter för att besluta om korrigerande eller begränsande åtgärder på unionsnivå, inbegripet krav på att de berörda produkterna med digitala element ska dras tillbaka från marknaden eller återkallas, inom en rimlig tid i förhållande till typen av risk. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

10. Kommissionen ska omedelbart delge berörda ekonomiska aktörer de genomförandeakter som avses i punkt 9. Medlemsstaterna ska genomföra dessa genomförandeakter utan dröjsmål och underrätta kommissionen om detta.

11. Punkterna 6–10 ska tillämpas under den tid som den exceptionella situation som motiverade kommissionens ingripande varar och så länge som den berörda produkten med digitala element fortsätter att utgöra de risker som avses i punkt 1.

Artikel 58

Formell bristande överensstämmelse

1. Om marknadskontrollmyndigheten i en medlemsstat konstaterar något av följande ska den ålägga den berörda tillverkaren att åtgärda den bristande överensstämmelsen:

a) CE-märkningen har fästs i strid med artiklarna 29 och 30.

b) CE-märkning saknas.

c) Det har inte upprättats någon EU-försäkran om överensstämmelse.

d) EU-försäkran om överensstämmelse har inte upprättats på ett korrekt sätt.

e) Identifikationsnumret för det anmälda organ som deltar i förfarandet för bedömning av överensstämmelse saknas i tillämpliga fall.

f) Den tekniska dokumentationen är antingen inte tillgänglig eller inte komplett.

2. Om sådan bristande överensstämmelse som avses i punkt 1 kvarstår ska den berörda medlemsstaten vidta lämpliga åtgärder för att begränsa eller förbjuda tillhandahållandet av produkten med digitala element på marknaden eller säkerställa att den återkallas eller dras tillbaka från marknaden.

Artikel 59

Marknadskontrollmyndigheternas gemensamma aktiviteter

1. Marknadskontrollmyndigheter får komma överens med andra berörda myndigheter om att genomföra gemensamma aktiviteter för att säkerställa cybersäkerheten och skyddet av konsumenter med avseende på specifika produkter med digitala element som släpps ut på marknaden eller tillhandahålls på marknaden, i synnerhet produkter med digitala element som ofta befinns utgöra cybersäkerhetsrisker.

2. Kommissionen eller Enisa ska föreslå gemensamma aktiviteter för att kontrollera överensstämmelsen med denna förordning vilka ska genomföras av marknadskontrollmyndigheter baserat på indikationer eller information om potentiell bristande överensstämmelse i flera medlemsstater med kraven i denna förordning när det gäller produkter med digitala element som fastställs i denna förordning.

3. Marknadskontrollmyndigheterna och i tillämpliga fall kommissionen ska säkerställa att överenskommelsen om att genomföra gemensamma aktiviteter inte leder till illojal konkurrens mellan ekonomiska aktörer och inte har någon negativ påverkan på objektiviteten, oberoendet och opartiskheten för parterna i överenskommelsen.

4. En marknadskontrollmyndighet får använda all information som erhållits genom genomförda gemensamma aktiviteter som ett led i utredningar som den gör.

5. Den berörda marknadskontrollmyndigheten och i tillämpliga fall kommissionen ska göra överenskommelsen om gemensamma aktiviteter, inbegripet namnen på de berörda parterna, tillgänglig för allmänheten.

Artikel 60

Samordnade tillsynsåtgärder

1. Marknadskontrollmyndigheterna ska genomföra samtidiga samordnade tillsynsåtgärder (sweeps) för specifika produkter med digitala element eller kategorier av sådana produkter för att kontrollera överensstämmelsen med eller upptäcka överträdelser av denna förordning. Dessa samordnade tillsynsåtgärder får omfatta inspektioner av produkter med digitala element som förvärvats under fingerad identitet.

2. Om inte annat överenskommits mellan de berörda marknadskontrollmyndigheterna ska samordnade tillsynsåtgärder samordnas av kommissionen. Samordnaren av den samordnade tillsynsåtgärden ska, när så är lämpligt, offentliggöra de sammanställda resultaten.

3. Om Enisa vid utförandet av sina uppgifter, däribland baserat på de anmälningar som inkommit enligt artikel 14.1 och 14.3, identifierar kategorier av produkter med digitala element som får omfattas av samordnade tillsynsåtgärder ska Enisa lämna in ett förslag till en samordnad tillsynsåtgärd till den samordnare som avses i punkt 2 i den här artikeln för att övervägas av marknadskontrollmyndigheterna.

4. I samband med samordnade tillsynsåtgärder får marknadskontrollmyndigheterna utnyttja de utredningsbefogenheter som fastställs i artiklarna 52–58 och andra befogenheter som tilldelats dem enligt nationell rätt.

5. Marknadskontrollmyndigheterna får bjuda in kommissionens tjänstemän och andra medföljande personer som bemyndigats av kommissionen att delta i samordnade tillsynsåtgärder.

Kapitel VI

Delegerade befogenheter och kommittéförfarande

Artikel 61

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 2.5 andra stycket, 7.3, 8.1 och 8.2, 13.8 fjärde stycket, 14.9, 25, 27.9, 28.5 och 31.5 ska ges till kommissionen för en period på fem år från och med den … [dagen för denna förordnings ikraftträdande]. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

3. Den delegering av befogenhet som avses i artiklarna 2.5 andra stycket, 7.3, 8.1 och 8.2, 13.8 fjärde stycket, 14.9, 25, 27.9, 28.5 och 31.5 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artiklarna 2.5 andra stycket, 7.3, 8.1 eller 8.2, 13.8 fjärde stycket, 14.9, 25, 27.9, 28.5 eller 31.5 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 62

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

3. Om kommitténs yttrande ska inhämtas genom skriftligt förfarande, ska det förfarandet avslutas utan resultat om kommitténs ordförande, inom tidsfristen för att avge yttrandet, så beslutar eller en kommittéledamot så begär.

Kapitel VII
Konfidentialitet och sanktioner

Artikel 63

Konfidentialitet

1. Alla parter som deltar i tillämpningen av denna förordning ska respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de skyddar följande:

   a) Immateriella rättigheter och en fysisk eller juridisk persons konfidentiella affärsinformation eller företagshemligheter, inbegripet källkod, utom i de fall som avses i artikel 5 i Europaparlamentets och rådets direktiv (EU) 2016/943[37].

   b) Ett ändamålsenligt genomförande av denna förordning, särskilt med avseende på inspektioner, utredningar eller revisioner.

   c) Intressen som rör allmän och nationell säkerhet.

   d) Integriteten i straffrättsliga eller administrativa förfaranden.

[37] Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

2. Utan att det påverkar tillämpningen av punkt 1 får information som utbyts på konfidentiell basis mellan marknadskontrollmyndigheterna och mellan marknadskontrollmyndigheter och kommissionen inte lämnas ut utan föregående samtycke från den marknadskontrollmyndighet som ursprungligen lämnat informationen.

3. Punkterna 1 och 2 påverkar inte kommissionens, medlemsstaternas och de anmälda organens rättigheter och skyldigheter när det gäller att utbyta information och utfärda varningar och inte heller de berörda personernas skyldighet att lämna information enligt medlemsstaternas straffrätt.

4. Kommissionen och medlemsstaterna får vid behov utbyta känslig information med berörda myndigheter i tredjeländer med vilka de har slutit bilaterala eller multilaterala avtal om konfidentialitet som garanterar en tillräcklig skyddsnivå.

Artikel 64

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelser av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder utan dröjsmål samt utan dröjsmål eventuella ändringar som berör dem.

2. Bristande efterlevnad av de väsentliga cybersäkerhetskrav som anges i bilaga I och de skyldigheter som fastställs i artiklarna 13 och 14 ska medföra administrativa sanktionsavgifter på upp till 15 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2,5 % av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

3. Bristande efterlevnad av de skyldigheter som anges i artiklarna 18–23, 28, 30.1-30.4, 31.1-31.4, 32.1, 32.2 och 32.3. Artiklarna 33.5, 39, 41, 47, 49 och 53 ska bli föremål för administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

4. Tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ och marknadskontrollmyndigheter som svar på en begäran ska medföra administrativa sanktionsavgifter på upp till 5 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 1 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

5. Vid beslut om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn ska tas till

   a) överträdelsens art, allvarlighetsgrad och varaktighet samt dess konsekvenser,

   b) huruvida administrativa sanktionsavgifter redan har påförts av samma eller andra marknadskontrollmyndigheter på samma ekonomiska aktör för en liknande överträdelse,

   c) storleken på, särskilt när det gäller mikroföretag, små och medelstora företag, inbegripet uppstartsföretag, och marknadsandelen för den ekonomiska aktör som begått överträdelsen.

6. Marknadskontrollmyndigheter som påför administrativa sanktionsavgifter ska meddela marknadskontrollmyndigheterna i andra medlemsstater detta via det informations- och kommunikationssystem som avses i artikel 34 i förordning (EU) 2019/1020.

7. Varje medlemsstat ska fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och offentliga organ som är inrättade i medlemsstaten.

8. Beroende på medlemsstatens rättssystem kan reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att sanktionsavgifterna utdöms av behöriga nationella domstolar eller andra organ, i enlighet med befogenheter som fastställs på nationell nivå i dessa medlemsstater. Tillämpningen av sådana regler i dessa medlemsstater ska ha motsvarande verkan.

9. Administrativa sanktionsavgifter får, beroende på omständigheterna i det enskilda fallet, påföras utöver eventuella andra korrigerande eller begränsande åtgärder som marknadskontrollmyndigheterna tillämpar på samma överträdelse.

10. Genom undantag från punkterna 3–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:

    a) Tillverkare som klassificeras som mikroföretag eller små företag när det gäller underlåtenhet att iaktta den tidsfrist som avses i artikel 14.2 a eller 14.4 a.

    b) Alla överträdelser av denna förordning som begås av förvaltare av programvara med fri och öppen källkod.

Artikel 65

Grupptalan

Direktiv (EU) 2020/1828 ska tillämpas på grupptalan om ekonomiska aktörers överträdelser av bestämmelserna i denna förordning som skadar eller kan skada konsumenternas kollektiva intressen.

Kapitel VIII

Övergångs- och slutbestämmelser

Artikel 66

Ändring av förordning (EU) 2019/1020

I bilaga I till förordning (EU) 2019/1020 ska följande punkt läggas till:

”XX[+]. Europaparlamentets och rådets förordning (EU) 2024/…*[++].

---

* Europaparlamentets och rådets förordning (EU) 2024/… av den … om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L …, ELI: …).”

[+] EUT: vänligen inför i texten nästa nummer i ordningen i förteckningen i bilaga I till förordning (EU) 2019/1020.

[++] EUT: Vänligen för in nummer på den förordning som finns i dokument PE-CONS 100/23 (2022/0272(COD)) och för in den förordningens nummer, datum och EUT-hänvisning i fotnoten.

Artikel 67

Ändring av direktiv (EU) 2020/1828

I bilaga I till direktiv (EU) 2020/1828 ska följande punkt läggas till:

”XX[+]. Europaparlamentets och rådets förordning (EU) 2024/…[*++].

---

[*] Europaparlamentets och rådets förordning (EU) 2024/… av den … om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L …, ELI: …).”

[+] EUT: vänligen inför i texten nästa nummer i ordningen i förteckningen i bilaga I till direktiv (EU) 2020/1828.

[++] EUT: Vänligen för in nummer på den förordning som finns i dokument PE-CONS 100/23 (2022/0272(COD)) och för in den förordningens nummer, datum och EUT-hänvisning i fotnoten.

Artikel 68

Ändringar av förordning (EU) nr 168/2013

I del C1, i tabellen i bilaga II till Europaparlamentets och rådets förordning (EU) nr 168/2013[38]ska följande post läggas till:

”

XX+	18	Skydd av fordon mot cyberattacker		x	x	x	x	x	x	x	x	x	x	x	x	x	x

”.

[38] Europaparlamentets och rådets förordning (EU) nr 168/2013 av den 15 januari 2013 om godkännande av och marknadskontroll för två- och trehjuliga fordon och fyrhjulingar (EUT L 60, 2.3.2013, s. 52).

+ EUT : vänligen inför i texten nästa nummer i ordningen under del C1 i bilaga II till förordning (EU) nr 168/2013.

Artikel 69

Övergångsbestämmelser

1. EU-typkontrollintyg och beslut om godkännande som utfärdats avseende cybersäkerhetskrav för produkter med digitala element som omfattas av annan unionsharmoniseringslagstiftning än denna förordning ska fortsätta att gälla till och med den … [42 månader från dagen för denna förordnings ikraftträdande], såvida de inte löper ut före den dagen, eller något annat anges i sådan annan unionsharmoniseringslagstiftning, i vilket fall de förblir giltiga enligt den lagstiftningen.

2. Produkter med digitala element som har släppts ut på marknaden före den … [36 månader från dagen för denna förordnings ikraftträdande] ska omfattas av kraven som anges i denna förordning endast om de, från och med den dagen, är föremål för en väsentlig ändring.

3. Som avvikelse från punkt 2 i denna artikel ska de skyldigheter som fastställs i artikel 14 tillämpas på alla produkter med digitala element som omfattas av denna förordnings tillämpningsområde och som har släppts ut på marknaden före den … [36 månader från dagen för denna förordnings ikraftträdande].

Artikel 70

Utvärdering och översyn

1. Kommissionen ska senast den … [72 månader från dagen för denna förordnings ikraftträdande] och därefter vart fjärde år, överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet. Dessa rapporter ska offentliggöras.

2. Senast den … [45 månader från dagen för denna förordnings ikraftträdande] ska kommissionen, efter samråd med Enisa och CSIRT-nätverket, lägga fram en rapport för Europaparlamentet och rådet med en bedömning av ändamålsenligheten hos den gemensamma rapporteringsplattform som anges i artikel 16 samt effekterna av tillämpningen av de cybersäkerhetsrelaterade skäl som avses i artikel 16.2 av de CSIRT-enheter som utsetts till samordnare för den gemensamma rapporteringsplattformens ändamålsenlighet när det gäller att snabbt sprida mottagna anmälningar till andra relevanta CSIRT-enheter.

Artikel 71

Ikraftträdande och tillämpning

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Denna förordning ska tillämpas från och med den … [36 månader från dagen för denna förordnings ikraftträdande].

   Artikel 14 ska dock tillämpas från och med den … [21 månader från dagen för denna förordnings ikraftträdande] och kapitel IV (artiklarna 35–51) ska tillämpas från och med den … [18 månader från dagen för denna förordnings ikraftträdande].

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Strasbourg den …

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

BILAGA I

VÄSENTLIGA CYBERSÄKERHETSKRAV

Del I Cybersäkerhetskrav avseende egenskaper hos produkter med digitala element

1. Produkter med digitala element ska utformas, utvecklas och produceras på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna.

2. På grundval av den bedömning av cybersäkerhetsrisker som avses i artikel 13.2, och i tillämpliga fall, ska produkter med digitala element

   a) tillhandahållas på marknaden utan kända sårbarheter som kan utnyttjas,

   b) tillhandahållas på marknaden med en säker standardkonfiguration, såvida inte tillverkaren och företagsanvändaren kommit överens om något annat med avseende på en skräddarsydd produkt med digitala element, inbegripet möjlighet att återställa produkten till dess ursprungliga skick,

   c) säkerställa att sårbarheter kan åtgärdas genom säkerhetsuppdateringar, inbegripet, i tillämpliga fall, genom automatiska säkerhetsuppdateringar som installeras inom en lämplig tidsram som möjliggörs som standardinställning, med en tydlig och lättanvänd undantagsmekanism, genom att meddela användarna tillgängliga uppdateringar, och möjligheten att tillfälligt skjuta upp dem,

d) säkerställa skydd mot obehörig åtkomst genom lämpliga kontrollmekanismer, inbegripet men inte begränsat till system för autentisering, identitet eller åtkomsthantering, samt rapportera om eventuell obehörig åtkomst,

e) skydda konfidentialiteten för lagrade, överförda eller på annat sätt behandlade uppgifter, personuppgifter eller andra uppgifter, t.ex. genom kryptering av relevanta data i vila eller i transit med hjälp av de senaste metoderna, och med användning av andra tekniska lösningar,

f) skydda riktigheten hos lagrade, överförda eller på annat sätt behandlade uppgifter, personuppgifter eller andra uppgifter, kommandon, program och konfigurationer mot manipulation eller ändringar som inte godkänts av användaren, samt rapportera om datadistorsion,

g) endast behandla personuppgifter eller andra uppgifter som är adekvata, relevanta och begränsade till vad som är nödvändigt i förhållande till det avsedda syftet med produkten med digitala element (”uppgiftsminimering”),

h) skydda tillgången till väsentliga och grundläggande funktioner, även efter en incident, inbegripet genom resiliens- och begränsningsåtgärder mot överbelastningsattacker,

i) minimera de negativa effekterna av produkterna i sig eller av tillhörande tjänster på tillgången till tjänster som tillhandahålls av andra enheter eller nätverk,

j) utformas, utvecklas och produceras för att begränsa attackytor, inbegripet externa gränssnitt,

k) utformas, utvecklas och produceras för att minska effekterna av en incident med hjälp av lämpliga mekanismer och tekniker för att begränsa utnyttjandet,

l) tillhandahålla säkerhetsrelaterad information genom att registrera och övervaka relevant intern verksamhet, inbegripet tillgång till eller ändring av data, tjänster eller funktioner, med en undantagsmekanism för användaren,

m) ge användarna möjlighet att på ett säkert och enkelt sätt permanent ta bort alla data och inställningar och, om sådana data kan överföras till andra produkter eller system, säkerställa att detta görs på ett säkert sätt.

Del II Krav på sårbarhetshantering

Tillverkare av produkter med digitala element ska

1. identifiera och dokumentera sårbarheter och komponenter i produkter med digitala element, bland annat genom att upprätta en programvaruförteckning för material i ett allmänt använt och maskinläsbart format som åtminstone täcker produktens viktigaste (top-level) beroenden,

2. när det gäller riskerna för produkter med digitala element, utan dröjsmål åtgärda och avhjälpa sårbarheter, bland annat genom att tillhandahålla säkerhetsuppdateringar; om det är tekniskt möjligt ska nya säkerhetsuppdateringar tillhandahållas separat från funktionsuppdateringar,

3. tillämpa effektiva och regelbundna provningar och granskningar av säkerheten hos produkten med digitala element,

4. när en uppdatering av säkerheten har gjorts tillgänglig, dela och offentligt redovisa information om åtgärdade sårbarheter, inbegripet en beskrivning av sårbarheterna, information som gör det möjligt för användarna att identifiera den produkt med digitala element som påverkas, sårbarheternas konsekvenser, deras allvarlighetsgrad och tydlig och tillgänglig information som underlättar för användarna att avhjälpa sårbarheterna; i vederbörligen motiverade fall, om tillverkarna anser att säkerhetsriskerna med offentliggörande är större än säkerhetsfördelarna, får de skjuta upp offentliggörandet av information om en åtgärdad sårbarhet till dess att användarna har fått möjlighet att använda den relevanta programfixen,

5. införa och verkställa en policy för samordnad delgivning av information om sårbarheter,

6. vidta åtgärder för att underlätta utbyte av information om potentiella sårbarheter i sin produkt med digitala element och i tredjepartskomponenter som ingår i produkten, inbegripet genom att tillhandahålla en kontaktadress för rapportering av de sårbarheter som upptäckts i produkten med digitala element,

7. tillhandahålla mekanismer för säker distribution av uppdateringar av produkter med digitala element för att säkerställa att sårbarheter åtgärdas eller begränsas i tid och, i tillämpliga fall för säkerhetsuppdateringar, på ett automatiskt sätt,

8. säkerställa att säkerhetsuppdateringar, i de fall då de finns tillgängliga för att hantera identifierade säkerhetsproblem, sprids utan dröjsmål och, såvida inte tillverkaren och företagsanvändaren kommit överens om något annat med avseende på en skräddarsydd produkt med digitala element, kostnadsfritt, åtföljs av rådgivande meddelanden som ger användarna relevant information, inbegripet om eventuella åtgärder som ska vidtas.

BILAGA II

INFORMATION OCH INSTRUKTIONER TILL ANVÄNDAREN

Produkten med digitala element ska åtminstone åtföljas av

1. tillverkarens namn, registrerade firmanamn eller registrerade varumärke samt den postadress, den e-postadress eller andra digitala kontaktuppgifter och, om tillgänglig, den webbplats där tillverkaren kan kontaktas,

2. den gemensamma kontaktpunkt där information om sårbarheter hos produkten med digitala element kan rapporteras och tas emot och där tillverkarens policy för samordnad delgivning av information om sårbarheter kan hittas,

3. namn och typ samt eventuell ytterligare information som möjliggör unik identifiering av produkten med digitala element,

4. det avsedda syftet med produkten med digitala element, inbegripet den säkerhetsmiljö som tillhandahålls av tillverkaren, samt produktens väsentliga funktioner och information om säkerhetsegenskaperna,

5. varje känd eller förutsebar omständighet, som har samband med användningen av produkten med digitala element i enlighet med dess avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning, som kan leda till betydande cybersäkerhetsrisker,

6. i tillämpliga fall, den internetadress där EU-försäkran om överensstämmelse finns tillgänglig,

7. den typ av tekniskt säkerhetsstöd som erbjuds av tillverkaren och slutdatumet för den stödperiod under vilken användarna kan förvänta sig att sårbarheter ska hanteras och få säkerhetsuppdateringar,

8. detaljerade instruktioner eller en internetadress som hänvisar till sådana detaljerade instruktioner och information om

   a) nödvändiga åtgärder under den inledande idrifttagningen och under hela livslängden för produkten med digitala element för att säkerställa en säker användning,

   b) hur ändringar av produkten med digitala element kan påverka datasäkerheten,

   c) hur säkerhetsrelevanta uppdateringar kan installeras,

   d) säker avveckling av produkten med digitala element, inbegripet information om hur användardata kan avlägsnas på ett säkert sätt,

   e) hur standardinställningen som möjliggör automatisk installation av säkerhetsuppdateringar i enlighet med kravet i del I led 2.c i bilaga I kan stängas av,

   f) om produkten med digitala element är avsedd att integreras i andra produkter med digitala element, den information som krävs för att integratorn ska kunna uppfylla de väsentliga cybersäkerhetskrav som anges i bilaga I och dokumentationskraven i bilaga VII,

9. Om tillverkaren beslutar att göra programvaruförteckningen tillgänglig för användaren, information om var programvaruförteckningen kan nås.

BILAGA III

VIKTIGA PRODUKTER MED DIGITALA ELEMENT

Klass I

1. Identitetshanteringssystem och programvara och hårdvara för hantering av privilegierad åtkomst, inbegripet läsare för autentisering och åtkomstkontroll, inbegripet biometriska läsare.

2. Fristående och inbyggda webbläsare.

3. Lösenordshanterare.

4. Programvara som söker efter och avlägsnar skadlig programvara eller sätter den i karantän.

5. Produkter med digitala element som fungerar som virtuella privata nätverk (VPN).

6. System för nätverksförvaltning.

7. System för säkerhetsinformation och händelsehantering (SIEM).

8. Starthanterare.

9. Infrastruktur för kryptering med öppen nyckel (PKI) och programvara för utfärdande av digitala certifikat.

10. Fysiska och virtuella nätverksgränssnitt.

11. Operativsystem.

12. Routrar, modem avsedda för anslutning till internet och dataväxlar.

13. Mikroprocessorer med säkerhetsrelaterade funktioner.

14. Mikrokontroller med säkerhetsrelaterade funktioner.

15. Applikationsspecifika integrerade kretsar (ASIC) och fältprogrammerbara grindmatriser (FPGA) med säkerhetsrelaterade funktioner.

16. Smarta virtuella assistenter för allmänna ändamål.

17. Smarta hemprodukter med säkerhetsfunktioner, inbegripet smarta dörrlås, säkerhetskameror, babyövervakningssystem och larmsystem.

18. Internetanslutna leksaker som omfattas av Europaparlamentets och rådets direktiv 2009/48/EG[1] och som har sociala interaktiva funktioner (t.ex. tal eller filmning) eller som har positionsspårningsfunktioner.

19. Personliga kroppsburna produkter som ska bäras eller placeras på en människokropp och som har ett hälsoövervakningssyfte (t.ex. spårning) och som inte omfattas av förordning (EU) 2017/745 eller (EU) 2017/746, eller personliga kroppsburna produkter som är avsedda att användas av och för barn.

Klass II

1. Hypervisorer och system för körning av programbehållare som stöder virtualiserad exekvering av operativsystem och liknande miljöer.

2. Brandväggar, intrångsdetektions- och intrångsskyddssystem.

3. Manipulationssäkra mikroprocessorer.

4. Manipulationssäkra mikrokontroller.

---

[1] Europaparlamentets och rådets direktiv 2009/48/EG av den 18 juni 2009 om leksakers säkerhet (EUT L 170, 30.6.2009, s. 1).

BILAGA IV

KRITISKA PRODUKTER MED DIGITALA ELEMENT

1. Hårdvaruenheter med säkerhetsboxar.

2. Smarta mätarportar inom smarta mätarsystem enligt definitionen i artikel 2.23 i Europaparlamentets och rådets direktiv (EU) 2019/944[1] och andra enheter för avancerade säkerhetsändamål, inbegripet för säker kryptobehandling.

3. Smartkort eller liknande enheter, inbegripet säkra element.

---

[1] Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125).

BILAGA V

EU-FÖRSÄKRAN OM ÖVERENSSTÄMMELSE

Den EU-försäkran om överensstämmelse som avses i artikel 28 ska innehålla samtliga uppgifter som anges nedan:

1. Namn och typ samt eventuell ytterligare information som möjliggör unik identifiering av produkten med digitala element.

2. Namn och adress till tillverkaren eller tillverkarens representant.

3. En förklaring om att EU-försäkran om överensstämmelse utfärdas på leverantörens eget ansvar.

4. Föremål för försäkran (identifiering av produkten med digitala element så att den kan spåras, vilket vid behov kan inbegripa ett fotografi).

5. En förklaring om att det föremål för försäkran som beskrivs ovan överensstämmer med den relevanta unionsharmoniseringslagstiftningen.

6. Hänvisningar till relevanta harmoniserade standarder som använts eller andra gemensamma specifikationer eller system för cybersäkerhetscertifiering enligt vilka överensstämmelsen försäkras.

7. I tillämpliga fall, det anmälda organets namn och nummer, en beskrivning av det använda förfarandet för bedömning av överensstämmelse och uppgifter om det utfärdade intyget.

8. Ytterligare information:

Undertecknad för:

(ort och datum):

(namn, befattning) (namnteckning):

BILAGA VI

FÖRENKLAD EU-FÖRSÄKRAN OM ÖVERENSSTÄMMELSE

Den förenklade EU-försäkran om överensstämmelse som avses i artikel 13.20 ska utfärdas enligt följande:

Härmed försäkrar ...[tillverkarens namn] att produkten med digitala element ...[beteckning för typ av produkt med digitalt element] uppfyller kraven i (EU) 2024/…[+].

Den fullständiga texten till EU-försäkran om överensstämmelse finns på följande internetadress...:

[+] EUT: Vänligen för in nummer på den förordning som finns i dokument PE-CONS 100/23 (2022/0272(COD)).

BILAGA VII

DEN TEKNISKA DOKUMENTATIONENS INNEHÅLL

Den tekniska dokumentation som avses i artikel 31 ska åtminstone innehålla följande information, beroende på vad som är tillämpligt för den relevanta produkten med digitala element:

1. En allmän beskrivning av produkten med digitala element, inbegripet

   a) dess avsedda ändamål,

   b) versioner av programvara som påverkar överensstämmelsen med de väsentliga cybersäkerhetskraven,

   c) om produkten med digitala element är en hårdvaruprodukt, fotografier eller illustrationer som visar yttre egenskaper, märkning och inre layout,

   d) användarinformation och bruksanvisning enligt bilaga II.

2. En beskrivning av utformningen, utvecklingen och produktionen av produkten med digitala element samt processer för sårbarhetshantering, inbegripet

   a) nödvändig information om utformning och utveckling av produkten med digitala element, i tillämpliga fall inbegripet ritningar och scheman och/eller en beskrivning av systemarkitekturen som förklarar hur programvarukomponenter bygger på eller matas in i varandra och integreras i den övergripande behandlingen,

b) nödvändig information om och specifikationer av de processer för sårbarhetshantering som tillverkaren infört, inbegripet programvaruförteckningen, policyn för samordnad delgivning av information om sårbarheter, bevis på tillhandahållandet av en kontaktadress för rapportering av sårbarheter och en beskrivning av de tekniska lösningar som valts för säker distribution av uppdateringar,

c) nödvändig information om och specifikationer av produktions- och övervakningsprocesser för produkten med digitala element och validering av dessa processer.

3. En bedömning av de cybersäkerhetsrisker mot vilka produkten med digitala element utformas, utvecklas, produceras, levereras och underhålls som fastställs enligt artikel 13, inbegripet hur de väsentliga cybersäkerhetskraven i del I i bilaga I är tillämpliga.

4. Relevant information som beaktades för att fastställa stödperioden enligt artikel 13.8 för produkten med digitala element.

5. En förteckning över de harmoniserade standarder som helt eller delvis har följts och till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, gemensamma specifikationer enligt artikel 27 i denna förordning eller europeiska ordningar för cybersäkerhetscertifiering som antagits enligt förordning (EU) 2019/881 enligt artikel 27.8 i denna förordning, och, om dessa harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering inte har tillämpats, beskrivningar av de lösningar som valts för att uppfylla de väsentliga cybersäkerhetskraven i delarna I och II i bilaga I, inbegripet en förteckning över andra relevanta tekniska specifikationer som tillämpats. När det gäller delvis tillämpade harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering ska det i den tekniska dokumentationen specificeras vilka delar som har tillämpats.

6. Rapporter om de provningar som utförts för att kontrollera att produkten med digitala element och processerna för sårbarhetshantering överensstämmer med de tillämpliga väsentliga cybersäkerhetskraven i delarna I och II i bilaga I.

7. Kopia av EU-försäkran om överensstämmelse.

8. I tillämpliga fall, programvaruförteckningen, efter en motiverad begäran från en marknadskontrollmyndighet, förutsatt att det är nödvändigt för att denna myndighet ska kunna kontrollera överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I.

BILAGA VIII

FÖRFARANDEN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE

Del I Förfarande för bedömning av överensstämmelse som grundar sig på intern kontroll (baserat på modul A)

1. Intern kontroll är det förfarande för bedömning av överensstämmelse genom vilket tillverkaren fullgör skyldigheterna som anges i punkterna 2, 3 och 4 i denna del samt säkerställer och försäkrar på eget ansvar att produkter med digitala element uppfyller alla de väsentliga cybersäkerhetskraven i del I i bilaga I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

2. Tillverkaren ska upprätta den tekniska dokumentation som beskrivs i bilaga VII.

3. Utformning, utveckling, produktion och sårbarhetshantering av produkter med digitala element

   Tillverkaren ska vidta alla åtgärder som krävs för att säkerställa att utformningen, utvecklingen, produktionen samt processerna för sårbarhetshantering och övervakningen av dessa ska leder till att de tillverkade eller utvecklade produkterna med digitala element och de processer som tillverkaren infört överensstämmer med de väsentliga cybersäkerhetskraven i delarna I och II i bilaga I.

4. Märkning om överensstämmelse och försäkran om överensstämmelse

4.1. Tillverkaren ska fästa CE-märkningen på varje enskild produkt med digitala element som uppfyller de tillämpliga kraven som anges i denna förordning.

4.2. Tillverkaren ska upprätta en skriftlig EU-försäkran om överensstämmelse för varje produkt med digitala element i enlighet med artikel 28 och ska kunna uppvisa den tillsammans med den tekniska dokumentationen för de nationella myndigheterna under en period på 10 år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst. I EU-försäkran om överensstämmelse ska det anges för vilken produkt med digitala element den har upprättats. En kopia av EU-försäkran om överensstämmelse ska på begäran göras tillgänglig för de relevanta myndigheterna.

5. Tillverkarens representanter

Tillverkarens representant får fullgöra tillverkarens skyldigheter enligt punkt 4 för dennes räkning och på dennes ansvar, förutsatt att de relevanta skyldigheterna specificeras i fullmakten.

Del II EU-typkontroll (baserat på modul B)

1. EU-typkontroll är den del av ett förfarande för bedömning av överensstämmelse genom vilken ett anmält organ undersöker den tekniska utformningen och utvecklingen hos produkten med digitala element och de processer för sårbarhetshantering som tillverkaren infört och intygar att en produkt med digitala element uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

2. EU-typkontroll ska göras genom bedömning av lämpligheten hos den tekniska utformningen och utvecklingen av produkten med digitala element genom granskningen av den tekniska dokumentation och de underlag som avses i punkt 3 samt undersökningen av provexemplar av en eller flera kritiska delar av produkten (kombination av produktionstyp och utformningstyp).

3. Tillverkaren ska lämna in ansökan om EU-typkontroll till ett valfritt anmält organ.

   Ansökan ska innehålla följande:

   3.1 Tillverkarens namn och adress och, om ansökan lämnas in av tillverkarens representant, även namn och adress för den tillverkarens representant.

3.2 En skriftlig försäkran om att samma ansökan inte har lämnats in till något annat anmält organ.

3.3 Den tekniska dokumentationen, vilken ska göra det möjligt att bedöma överensstämmelsen hos produkten med digitala element med de tillämpliga väsentliga cybersäkerhetskraven i del I i bilaga I och tillverkarens processer för sårbarhetshantering enligt del II i bilaga I, och ska innehålla en tillfredsställande analys och bedömning av riskerna. Den tekniska dokumentationen ska innehålla de tillämpliga kraven och, i den mån det krävs för bedömningen, även en beskrivning av utformningen, tillverkningen och funktionen avseende produkten med digitala element. Den tekniska dokumentationen ska, i tillämpliga fall, innehålla minst de uppgifter som anges i bilaga VII.

3.4 Underlag som visar att de lösningarna för teknisk utformning och utveckling samt processerna för sårbarhetshantering är lämpliga. I underlaget ska anges alla dokument som har använts, särskilt när de relevanta harmoniserade standarderna och/eller de tekniska specifikationerna inte har tillämpats fullt ut. Underlaget ska vid behov innehålla resultaten av provningar som utförts i tillverkarens därtill ägnade laboratorium eller i något annat provningslaboratorium för dennes räkning och under dennes ansvar.

4. Det anmälda organet ska göra följande:

4.1. Granska den tekniska dokumentationen och underlaget för att bedöma om den tekniska utformningen och utvecklingen av produkten med digitala element uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och om de processer för sårbarhetshantering som tillverkaren infört uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

4.2. Kontrollera att provexemplaren har utvecklats eller tillverkats i enlighet med den tekniska dokumentationen och identifiera de delar som har utformats och utvecklats i enlighet med de tillämpliga bestämmelserna i de relevanta harmoniserade standarderna eller de tekniska specifikationerna, liksom de delar som har utformats och utvecklats utan att de tillämpliga bestämmelserna i dessa standarder har följts.

4.3. Utföra eller låta utföra lämpliga undersökningar och provningar för att, i de fall där tillverkaren har valt att tillämpa lösningarna i de relevanta harmoniserade standarderna eller de tekniska specifikationerna för de krav som anges i bilaga I, kontrollera att de lösningarna har tillämpats på rätt sätt.

4.4. Utföra eller låta utföra lämpliga undersökningar och provningar för att, i de fall där lösningarna i relevanta harmoniserade standarder eller tekniska specifikationer för de krav som anges i bilaga I inte har tillämpats, kontrollera om de lösningar som tillverkaren använt uppfyller de väsentliga cybersäkerhetskraven.

4.5. Komma överens med tillverkaren om var undersökningarna och provningarna ska utföras.

5. Det anmälda organet ska utarbeta en bedömningsrapport i vilken de åtgärder som utförts i enlighet med punkt 4 och resultatet av dem redovisas. Utan att det påverkar det anmälda organets skyldigheter gentemot de anmälande myndigheterna får organet endast offentliggöra hela eller delar av innehållet i rapporten med tillverkarens samtycke.

6. Om typen och processerna för sårbarhetshantering uppfyller de väsentliga cybersäkerhetskraven i bilaga I ska det anmälda organet utfärda ett EU-typintyg till tillverkaren. Intyget ska innehålla tillverkarens namn och adress, slutsatserna av undersökningen, eventuella giltighetsvillkor och de uppgifter som krävs för identifiering av den godkända typen och processerna för sårbarhetshantering. Intyget kan ha en eller flera bilagor.

Intyget och bilagorna ska innehålla all information som behövs för att bedöma om de tillverkade eller utvecklade produkterna med digitala element överensstämmer med den undersökta typen och processerna för sårbarhetshantering och för att kontrollera produkter i bruk.

Om typen och processerna för sårbarhetshantering inte uppfyller de tillämpliga väsentliga cybersäkerhetskraven i bilaga I ska det anmälda organet avslå ansökan om EU-typintyg och informera sökanden om detta samt utförligt motivera avslaget.

7. Det anmälda organet ska följa med i den tekniska utvecklingen, och om denna tyder på att den godkända typen och processerna för sårbarhetshantering inte längre uppfyller de tillämpliga väsentliga cybersäkerhetskraven i bilaga I ska organet fastställa om det krävs ytterligare undersökningar. Om så är fallet ska det anmälda organet underrätta tillverkaren om detta.

Tillverkaren ska underrätta det anmälda organ som innehar den tekniska dokumentationen för EU-typintyget om alla ändringar av den godkända typen och processerna för sårbarhetshantering som kan påverka överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I eller villkoren för intygets giltighet. För sådana ändringar krävs ytterligare godkännande i form av ett tillägg till det ursprungliga EU-typintyget.

8. Det anmälda organet ska regelbundet genomföra revisioner för att säkerställa att processerna för sårbarhetshantering enligt del II i bilaga I genomförs på ett tillfredsställande sätt.

9. Varje anmält organ ska underrätta sina anmälande myndigheter om de EU-typintyg och tillägg till dessa som det har utfärdat eller återkallat, och det ska periodiskt återkommande eller på begäran ge de anmälande myndigheterna tillgång till förteckningen över de intyg och eventuella tillägg till dessa som det har avslagit, tillfälligt återkallat eller på annat sätt belagt med restriktioner.

Varje anmält organ ska underrätta de övriga anmälda organen om de EU-typintyg och eventuella tillägg till dessa som det har vägrat utfärda, slutgiltigt eller tillfälligt återkallat eller på annat sätt belagt med restriktioner och, på begäran, om de intyg och tillägg till dessa som det har utfärdat.

Kommissionen, medlemsstaterna och de övriga anmälda organen har rätt att på begäran få en kopia av EU-typkontrollintyget och alla tillägg till det. Kommissionen och medlemsstaterna har rätt att på begäran få en kopia av den tekniska dokumentationen och av resultaten från de undersökningar som utförts av det anmälda organet. Det anmälda organet ska spara en kopia av EU-typintyget med bilagor och tillägg samt av den tekniska dokumentationen, inklusive dokumentation från tillverkaren, så länge som intyget är giltigt.

10. Tillverkaren ska för de nationella myndigheterna kunna uppvisa en kopia av EU-typintyget med bilagor och tillägg tillsammans med den tekniska dokumentationen under tio år efter det att produkten med digitala element släpptes ut på marknaden eller under stödperioden, beroende på vilken period som är längst.

11. Tillverkarens representant får lämna in den ansökan som avses i punkt 3 och fullgöra skyldigheterna enligt punkterna 7 och 10, förutsatt att de relevanta skyldigheterna specificeras i fullmakten.

Del III Överensstämmelse med typ som grundar sig på intern tillverkningskontroll (baserat på modul C)

1. Överensstämmelse med typ som grundar sig på intern tillverkningskontroll är den del av ett förfarande för bedömning av överensstämmelse genom vilken tillverkaren fullgör skyldigheterna som anges i punkterna 2 och 3 i denna del samt säkerställer och försäkrar att de berörda produkterna med digitala element överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

2. Produktion

Tillverkaren ska vidta alla nödvändiga åtgärder för att produktionen och övervakningen av den ska leda till att de tillverkade produkterna med digitala element överensstämmer med den godkända typen enligt beskrivningen i EU-typintyget och med de väsentliga cybersäkerhetskraven i del I i bilaga I och säkerställer att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

3. Märkning om överensstämmelse och försäkran om överensstämmelse

3.1. Tillverkaren ska fästa CE-märkningen på varje enskild produkt med digitala element som överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de tillämpliga kraven som anges i denna förordning.

3.2. Tillverkaren ska upprätta en skriftlig försäkran om överensstämmelse för en produktmodell och kunna uppvisa den för de nationella myndigheterna under en period på tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst. I försäkran om överensstämmelse ska det anges för vilken produktmodell den har upprättats. En kopia av försäkran om överensstämmelse ska på begäran göras tillgänglig för de behöriga myndigheterna.

4. Tillverkarens representant

Tillverkarens representant får fullgöra tillverkarens skyldigheter enligt punkt 3 för dennes räkning och på dennes ansvar, förutsatt att de relevanta skyldigheterna specificeras i fullmakten.

Del IV Överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H)

1. Överensstämmelse som grundar sig på fullständig kvalitetssäkring är det förfarande för bedömning av överensstämmelse genom vilket tillverkaren fullgör skyldigheterna som anges i punkterna 2 och 5 i denna del samt säkerställer och försäkrar på eget ansvar att de berörda produkterna med digitala element eller produktkategorierna uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att de processer för sårbarhetshantering som tillverkaren infört uppfyller kraven i del II i bilaga I.

2. Utformning, utveckling, produktion och sårbarhetshantering av produkter med digitala element

Tillverkaren ska tillämpa ett godkänt kvalitetssystem enligt punkt 3 för utformning, utveckling, slutlig produktkontroll och provning av de berörda produkterna med digitala element och för hantering av sårbarheter, upprätthålla dess effektivitet under hela stödperioden och ska stå under övervakning i enlighet med punkt 4.

3. Kvalitetssystem

3.1. Tillverkaren ska hos ett valfritt anmält organ ansöka om att få sitt kvalitetssystem för de berörda produkterna med digitala element bedömt.

Ansökan ska innehålla följande:

a) Tillverkarens namn och adress och, om ansökan lämnas in av tillverkarens representant, namn och adress för den tillverkarens representant.

b) Den tekniska dokumentationen för en modell av varje kategori av produkter med digitala element som är tänkt att tillverkas eller utvecklas. Den tekniska dokumentationen ska, i tillämpliga fall, innehålla de uppgifter som anges i bilaga VII.

c) Dokumentation av kvalitetssystemet.

d) En skriftlig försäkran om att samma ansökan inte har lämnats till något annat anmält organ.

3.2. Kvalitetssystemet ska säkerställa att produkterna med digitala element uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att de processer för sårbarhetshantering som tillverkaren infört uppfyller kraven i del II i bilaga I.

Alla de faktorer, krav och bestämmelser som tillverkaren tagit hänsyn till ska dokumenteras på ett systematiskt och överskådligt sätt i form av skriftliga riktlinjer, förfaranden och anvisningar. Denna dokumentation av kvalitetssystemet ska möjliggöra en enhetlig tolkning av rutiner och kvalitetsåtgärder, såsom program, planer, manualer och protokoll.

Den ska framför allt innehålla en fullgod beskrivning av

a) kvalitetsmålen och organisationsstruktur samt ledningens ansvar och befogenheter när det gäller utformning, utveckling, produktkvalitet och sårbarhetshantering,

b) de tekniska specifikationer för utformning och utveckling, inbegripet standarder, som ska tillämpas och, när de relevanta harmoniserade standarderna eller de tekniska föreskrifterna inte tillämpas fullt ut, de medel som används för att säkerställa att de väsentliga cybersäkerhetskraven i del I i bilaga I som är tillämpliga för produkterna med digitala element uppfylls,

c) de tekniska specifikationer för förfaranden, inklusive standarder, som ska tillämpas och, när de relevanta harmoniserade standarderna eller de tekniska föreskrifterna inte tillämpas fullt ut, de medel som används för att säkerställa att de väsentliga cybersäkerhetskraven i del II i bilaga I som är tillämpliga för tillverkaren uppfylls,

d) kontrollen av utformning och utveckling, samt de metoder, processer och systematiska förfaranden för verifikation av utformning och utveckling som ska användas vid utformning och utveckling av produkter med digitala element inom den berörda kategorin,

e) de motsvarande metoder, processer och systematiska åtgärder för produktion, kvalitetskontroll och kvalitetssäkring som ska användas,

f) de undersökningar och provningar som kommer att utföras före, under och efter produktionen, och hur ofta de kommer att utföras,

g) kvalitetsdokumenten, t.ex. kontrollrapporter, provningsresultat, kalibreringsresultat och redogörelser för den berörda personalens kvalifikationer.

h) metoderna för övervakning av att den erforderliga utformnings- och produktkvaliteten uppnås och att kvalitetssystemet fungerar effektivt.

3.3. Det anmälda organet ska bedöma kvalitetssystemet för att avgöra det uppfyller kraven i punkt 3.2.

Det ska förutsätta att kraven är uppfyllda i fråga om de delar av kvalitetssäkringssystemet som uppfyller motsvarande specifikationer i den nationella standard genom vilken den relevanta harmoniserade standarden eller de tekniska specifikationerna genomförs.

Utöver erfarenhet av kvalitetsledningssystem ska minst en av revisionsgruppens deltagare ha erfarenhet av bedömning av det aktuella produktområdet och den berörda produkttekniken, och känna till de tillämpliga kraven som anges i denna förordning. Revisionen ska även omfatta ett bedömningsbesök i tillverkarens anläggning, om en sådan anläggning finns. Revisionsgruppen ska granska den tekniska dokumentation som avses i punkt 3.1 b för att kontrollera att tillverkaren känner till de tillämpliga kraven som anges i denna förordning och kan utföra de undersökningar som krävs för att säkerställa att produkten med digitala element överensstämmer med kraven.

Tillverkaren eller tillverkarens representant ska meddelas beslutet.

Meddelandet ska innehålla slutsatserna från revisionen och det motiverade bedömningsbeslutet.

3.4. Tillverkaren ska åta sig att fullgöra de skyldigheter som är förenade med det godkända kvalitetssystemet och att upprätthålla det så att det förblir ändamålsenligt och effektivt.

3.5. Tillverkaren ska informera det anmälda organ som har godkänt kvalitetssystemet om alla planerade ändringar av systemet.

Det anmälda organet ska bedöma de föreslagna ändringarna och avgöra om ett ändrat kvalitetssystem fortfarande uppfyller de krav som avses i punkt 3.2 eller om en ny bedömning är nödvändig.

Det ska meddela tillverkaren sitt beslut. Meddelandet ska innehålla slutsatserna från undersökningen och det motiverade bedömningsbeslutet.

4. Övervakning under det anmälda organets ansvar

4.1. Syftet med övervakningen är att säkerställa att tillverkaren fullgör de skyldigheter som är förenade med det godkända kvalitetssystemet.

4.2. För att möjliggöra en bedömning ska tillverkaren ge det anmälda organet tillträde till lokaler för utformning, utveckling, produktion, kontroll, provning och lagring och tillhandahålla all nödvändig information, särskilt i fråga om

a) dokumentationen av kvalitetssystemet,

b) de dokument som anges i kvalitetssystemets utformningsdel, t.ex. resultat från analyser, beräkningar och provningar,

c) de dokument som anges i kvalitetssystemets tillverkningsdel, t.ex. kontrollrapporter, provningsresultat, kalibreringsresultat och redogörelser för den berörda personalens kvalifikationer.

4.3. Det anmälda organet ska regelbundet genomföra revisioner för att säkerställa att tillverkaren vidmakthåller och tillämpar kvalitetssystemet, samt överlämna en revisionsrapport till tillverkaren.

5. Märkning om överensstämmelse och försäkran om överensstämmelse

5.1. Tillverkaren ska fästa CE-märkningen och, under ansvar av det anmälda organ som avses i punkt 3.1, organets identifikationsnummer på varje enskild produkt med digitala element som uppfyller kraven i del I i bilaga I.

5.2. Tillverkaren ska upprätta en skriftlig försäkran om överensstämmelse för en produktmodell och kunna uppvisa den för de nationella myndigheterna under en period på tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst. I försäkran om överensstämmelse ska det anges för vilken produktmodell den har upprättats.

En kopia av försäkran om överensstämmelse ska på begäran göras tillgänglig för de behöriga myndigheterna.

6. Tillverkaren ska under en period på minst tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst, kunna uppvisa följande för de nationella myndigheterna:

   a) Den tekniska dokumentation som avses i punkt 3.1.

   b) Sådan dokumentation av kvalitetssystemet som avses i punkt 3.1.

   c) Godkända ändringar som avses i punkt 3.5.

   d) De beslut och rapporter från det anmälda organet som avses i punkterna 3.5 och 4.3.

7. Varje anmält organ ska underrätta sina anmälande myndigheter om de godkännanden av kvalitetssystem som det har utfärdat eller återkallat och ska regelbundet eller på begäran ge de anmälande myndigheterna tillgång till förteckningen över godkännanden som det har vägrat att utfärda, tillfälligt återkallat eller på annat sätt belagt med restriktioner.

   Varje anmält organ ska underrätta de övriga anmälda organen om de godkännanden av kvalitetssystem som det har vägrat utfärda eller tillfälligt eller slutgiltigt återkallat och, på begäran, om de godkännanden av kvalitetssystem som det har utfärdat.

8. Tillverkarens representant

Tillverkarens skyldigheter enligt punkterna 3.1, 3.5, 5 och 6 får fullgöras, för dennes räkning och på dennes ansvar, av tillverkarens representant, förutsatt att de relevanta skyldigheterna specificeras i fullmakten.

Ett uttalande har gjorts om denna akt och återges i [EUT ska tillhandahålla följande: EUT C, XXX, XX.XX.2024, s. XX] och på följande webbadress: [EUT: vänligen för in webbadressen för uttalandet]