2024/2847

20.11.2024

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2024/2847

af 23. oktober 2024

om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed)

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([1]),

efter høring af Regionsudvalget,

efter den almindelige lovgivningsprocedure ([2]), og

ud fra følgende betragtninger:

(1) Cybersikkerhed er en af de største udfordringer for Unionen. Antallet og mangfoldigheden af forbundne enheder vil stige eksponentielt i de kommende år. Cyberangreb udgør et område af offentlig interesse, eftersom de har en kritisk indvirkning ikke blot på Unionens økonomi, men også på demokratiet og forbrugernes sikkerhed og sundhed. Det er derfor nødvendigt at styrke Unionens tilgang til cybersikkerhed, tage cyberrobusthed op på EU-plan og forbedre det indre markeds funktion ved at fastlægge en ensartet retlig ramme for væsentlige cybersikkerhedskrav til produkter med digitale elementer, der bringes i omsætning på EU-markedet. Der bør tages fat på to store problemer, som øger omkostningerne for brugerne og samfundet: et lavt cybersikkerhedsniveau for produkter med digitale elementer, der afspejles i udbredte sårbarheder og utilstrækkelig og inkonsekvent levering af sikkerhedsopdateringer til håndtering heraf, og brugernes utilstrækkelige forståelse af og adgang til oplysninger, hvilket forhindrer dem i at vælge produkter med tilstrækkelige cybersikkerhedsegenskaber eller at anvende dem på en sikker måde.

(2) Denne forordning har til formål at fastsætte rammebetingelserne for udvikling af sikre produkter med digitale elementer ved at sikre, at hardware- og softwareprodukter bringes i omsætning med færre sårbarheder, og at fabrikanterne tager sikkerheden alvorligt i hele et produkts livscyklus. Den har også til formål at skabe betingelser, der gør det muligt for brugerne at tage hensyn til cybersikkerhed, når de udvælger og anvender produkter med digitale elementer, f.eks. ved at øge gennemsigtigheden med hensyn til supportperioden for produkter med digitale elementer, der bringes i omsætning.

(3) Relevant gældende EU-ret omfatter flere sæt horisontale regler, der omhandler visse cybersikkerhedsaspekter fra forskellige vinkler, herunder foranstaltninger til forbedring af sikkerheden i den digitale forsyningskæde. Eksisterende EU-ret vedrørende cybersikkerhed, herunder Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([3]) og Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([4]), omfatter imidlertid ikke direkte obligatoriske krav til sikkerheden af produkter med digitale elementer.

([1]) EUT C 100 af 16.3.2023, s. 101.
([2]) Europa-Parlamentets holdning af 12.3.2024 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 10.10.2024.
([3]) Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).
([4]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

(4) Selv om eksisterende EU-ret finder anvendelse på visse produkter med digitale elementer, er der ingen horisontal EU-lovramme, der fastsætter omfattende cybersikkerhedskrav for alle produkter med digitale elementer. De forskellige retsakter og initiativer, der indtil videre er truffet på EU-plan og nationalt plan, løser kun delvist de identificerede cybersikkerhedsrelaterede problemer og risici og skaber et lovgivningsmæssigt kludetæppe i det indre marked, øger retsusikkerheden for både fabrikanter og brugere af disse produkter og pålægger virksomheder og organisationer unødvendige byrder forbundet med opfyldelsen af en række krav og forpligtelser for lignende produkttyper. Cybersikkerheden for disse produkter har en særlig stærk grænseoverskridende dimension, da produkter med digitale elementer fremstillet i én medlemsstat eller ét tredjeland ofte anvendes af organisationer og forbrugere i hele det indre marked. Dette gør det nødvendigt at regulere området på EU-plan for at sikre harmoniserede lovgivningsmæssige rammer og retssikkerhed for brugere, organisationer og virksomheder, herunder mikrovirksomheder og små og mellemstore virksomheder som defineret i bilaget til Kommissionens henstilling 2003/361/EF ([5]). Unionens lovgivningsmæssige landskab bør harmoniseres ved at indføre horisontale cybersikkerhedskrav for produkter med digitale elementer. Der bør desuden i hele Unionen sikres større retssikkerhed for erhvervsdrivende og brugere samt en bedre harmonisering af det indre marked og proportionalitet for mikrovirksomheder og små og mellemstore virksomheder, og dermed mere levedygtige vilkår for erhvervsdrivende, der ønsker at komme ind på dette marked.

(5) For så vidt angår mikrovirksomheder og små og mellemstore virksomheder bør bestemmelserne i bilaget til henstilling 2003/361/EF anvendes i deres helhed ved fastlæggelsen af, hvilken kategori en virksomhed falder ind under. Ved beregningen af antal beskæftigede og finansielle tærskler til afgrænsning af virksomhedskategorierne, bør bestemmelserne i artikel 6 i bilaget til henstilling 2003/361/EF om fastsættelse af oplysninger om virksomheden under hensyntagen til specifikke typer virksomheder, f.eks. partnervirksomheder eller tilknyttede virksomheder, derfor også finde anvendelse.

(6) Kommissionen bør yde vejledning for at bistå erhvervsdrivende, navnlig mikrovirksomheder og små og mellemstore virksomheder, med anvendelsen af denne forordning. Sådan vejledning bør bl.a. omfatte denne forordnings anvendelsesområde, navnlig fjerndatabehandling og dens konsekvenser for udviklere af gratis open source-software, anvendelsen af kriterier til at fastsætte supportperioder for produkter med digitale elementer, samspillet mellem denne forordning og anden EU-ret, og begrebet væsentlig ændring.

(7) På EU-plan er der i forskellige program- og politikdokumenter såsom den fælles meddelelse fra Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik af 16. december 2020 med titlen »EU's strategi for cybersikkerhed for det digitale årti«, Rådets konklusioner af 2. december 2020 om cybersikkerheden ved forbundet udstyr og af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition og Europa-Parlamentets beslutning af 10. juni 2021 om EU's strategi for cybersikkerhed for det digitale årti ([6]), opfordret til specifikke EU-cybersikkerhedskrav til produkter med digitale elementer, og en række tredjelande har indført foranstaltninger til at løse dette problem på eget initiativ. I den endelige rapport fra konferencen om Europas fremtid opfordrede borgerne Unionen til at spille en stærkere rolle i bekæmpelsen af cybersikkerhedstrusler. Hvis Unionen skal spille en førende international rolle på området cybersikkerhed, er det vigtigt at fastlægge ambitiøse overordnede lovgivningsmæssige rammer.

(8) For at øge det samlede cybersikkerhedsniveau for alle produkter med digitale elementer, der bringes i omsætning i det indre marked, er det nødvendigt at indføre objektive og teknologineutrale væsentlige cybersikkerhedskrav til disse produkter, der gælder horisontalt.

(9) Under visse omstændigheder kan alle produkter med digitale elementer, der er integreret i eller forbundet med et større elektronisk informationssystem, fungere som angrebsvektor for ondsindede aktører. Som følge heraf kan selv hardware og software, der anses som mindre kritisk, lette den indledende kompromittering af en enhed eller et netværk, der gør det muligt for ondsindede aktører at få privilegeret adgang til et system eller bevæge sig sideværts på tværs af systemer. Fabrikanterne bør derfor sikre, at alle produkter med digitale elementer, der kan forbindes, designes og udvikles i overensstemmelse med de væsentlige cybersikkerhedskrav, der er fastsat i denne forordning. Denne forpligtelse vedrører både produkter, der kan forbindes fysisk via hardwaregrænseflader, og produkter, der er logisk forbundne, såsom via netstikdåser, rør, filer, applikationsprogrammeringsgrænseflader eller andre typer softwaregrænseflader. Da cybertrusler kan udbredes gennem forskellige produkter med digitale elementer, inden de når et bestemt mål, f.eks. ved at sammenkæde flere sårbarheder, bør fabrikanterne også sikre cybersikkerheden i de produkter, der kun er indirekte forbundet med andre enheder eller netværk.

([5]) Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

([6]) EUT C 67 af 8.2.2022, s. 81.

(10) Ved at fastsætte cybersikkerhedskrav til produkter med digitale elementer, der bringes i omsætning, er hensigten, at disse produkters cybersikkerhed bliver forbedret for både forbrugere og virksomheder. Disse krav vil desuden sikre, at der tages hensyn til cybersikkerheden hele vejen igennem forsyningskæderne, og dermed gøre endelige produkter med digitale elementer og deres komponenter mere sikre. Dette omfatter også krav til produkter med digitale elementer beregnet til sårbare forbrugere, f.eks. legetøj og systemer til overvågning af spædbørn, der bringes i omsætning. Forbrugerprodukter med digitale elementer, der i denne forordning kategoriseres som vigtige produkter med digitale elementer, udgør en højere cybersikkerhedsrisiko ved at udføre en funktion, der indebærer en betydelig risiko for negative virkninger med hensyn til dens intensitet og evne til at skade sådanne produkters brugeres sundhed, sikkerhed eller tryghed, og de bør underkastes en strengere overensstemmelsesvurderingsprocedure. Dette gælder for sådanne produkter som produkter til intelligente bygninger med sikkerhedsfunktioner, herunder intelligente dørlåse, systemer til overvågning af spædbørn og alarmsystemer, internetforbundet legetøj og personlig wearable-sundhedsteknologi. Derudover vil de strengere overensstemmelsesvurderingsprocedurer, som andre produkter med digitale elementer, der i denne forordning kategoriseres som vigtige eller kritiske produkter med digitale elementer, skal gennemgå, bidrage til at forebygge potentielle negative virkninger for forbrugerne af udnyttelsen af sårbarheder.

(11) Formålet med denne forordning er at sikre et højt cybersikkerhedsniveau for produkter med digitale elementer og deres integrerede fjerndatabehandlingsløsninger. Sådanne fjerndatabehandlingsløsninger bør defineres som databehandling på afstand, til hvilken softwaren er designet og udviklet af eller på vegne af fabrikanten af det pågældende produkt med digitale elementer, og hvis fravær ville forhindre produktet med digitale elementer i at udføre en af sine funktioner. Denne tilgang sikrer, at sådanne produkter er tilstrækkeligt sikret i deres helhed af deres fabrikanter, uanset om data behandles eller lagres lokalt på brugerens enhed eller på afstand af fabrikanten. Samtidig er behandling eller lagring på afstand kun omfattet af denne forordnings anvendelsesområde, i det omfang det er nødvendigt, for at et produkt med digitale elementer kan udføre sine funktioner. En sådan behandling eller lagring på afstand omfatter den situation, hvor en mobilapplikation kræver adgang til en applikationsprogrammeringsgrænseflade eller til en database, der leveres ved hjælp af en tjeneste udviklet af fabrikanten. I så fald er tjenesten omfattet af denne forordnings anvendelsesområde som en fjerndatabehandlingsløsning. Kravene vedrørende fjerndatabehandlingsløsninger, der er omfattet af denne forordnings anvendelsesområde, omfatter derfor ikke tekniske, operationelle eller organisatoriske foranstaltninger, der har til formål at styre de risici, der er forbundet med sikkerheden i en fabrikants net- og informationssystemer som helhed.

(12) Cloudløsninger udgør kun fjerndatabehandlingsløsninger i den i denne forordning anvendte betydning, hvis de opfylder definitionen i denne forordning. For eksempel bør cloudaktiverede funktioner, der stilles til rådighed af fabrikanter af enheder til intelligente bygninger, og som gør det muligt for brugerne at kontrollere enheden på afstand, være omfattet af denne forordnings anvendelsesområde. På den anden side er websteder, der ikke understøtter funktionaliteten af et produkt med digitale elementer, eller cloudtjenester, der er designet og udviklet uden for en fabrikants ansvar for et produkt med digitale elementer, ikke omfattet af denne forordnings anvendelsesområde. Direktiv (EU) 2022/2555 finder anvendelse på cloud computing-tjenester og modeller for cloudtjenester såsom software som en service (SaaS), platform som en service (PaaS) eller infrastruktur som en service (IaaS). Enheder, der udbyder cloud computing-tjenester i Unionen, og som er mellemstore virksomheder i henhold til artikel 2 i bilaget til henstilling 2003/361/EF, eller som overskrider de lofter for mellemstore virksomheder, der er fastsat i nævnte artikels stk. 1, er omfattet af nævnte direktivs anvendelsesområde.

(13) I overensstemmelse med denne forordnings mål om at fjerne hindringerne for den frie bevægelighed for produkter med digitale elementer, må medlemsstaterne ikke hindre tilgængeliggørelse på markedet af produkter med digitale elementer, der opfylder kravene i denne forordning, for så vidt angår spørgsmål, der er omfattet af denne forordning. For så vidt angår spørgsmål, der harmoniseres ved denne forordning, kan medlemsstaterne derfor ikke pålægge yderligere cybersikkerhedskrav for tilgængeliggørelse på markedet af produkter med digitale elementer. Enhver offentlig eller privat enhed kan imidlertid fastsætte yderligere krav ud over dem, der er fastsat i denne forordning, for udbud eller anvendelse af produkter med digitale elementer til vedkommendes specifikke formål og kan derfor vælge at anvende produkter med digitale elementer, der opfylder strengere eller mere specifikke cybersikkerhedskrav end dem, der gælder for tilgængeliggørelse på markedet i henhold til denne forordning. Uden at det berører Europa-Parlamentets og Rådets direktiv 2014/24/EU ([7]) og 2014/25/EU ([8]), bør medlemsstaterne, når de indkøber produkter med digitale elementer, som skal opfylde de væsentlige cybersikkerhedskrav, der er fastsat i denne forordning, herunder dem, der vedrører håndtering af sårbarheder, sikre, at der tages hensyn til sådanne krav

([7]) Europa-Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (EUT L 94 af 28.3.2014, s. 65).

([8]) Europa-Parlamentets og Rådets direktiv 2014/25/EU af 26. februar 2014 om fremgangsmåderne ved indgåelse af kontrakter inden for vand- og energiforsyning, transport samt posttjenester og om ophævelse af direktiv 2004/17/EF (EUT L 94 af 28.3.2014, s. 243).

i udbudsprocessen, og at der også tages hensyn til fabrikanternes evne til effektivt at anvende cybersikkerheds-foranstaltninger og håndtere cybertrusler. Derudover fastsætter direktiv (EU) 2022/2555 foranstaltninger til styring af cybersikkerhedsrisici for væsentlige og vigtige enheder, der er omhandlet i nævnte direktivs artikel 3, som kunne indebære sikkerhedsforanstaltninger i forsyningskæden, der kræver, at sådanne enheder anvender produkter med digitale elementer, der opfylder strengere cybersikkerhedskrav end dem, der er fastsat i denne forordning. I overensstemmelse med direktiv (EU) 2022/2555 og med dets princip om minimumsharmonisering kan medlemsstaterne derfor pålægge yderligere cybersikkerhedskrav for væsentlige eller vigtige enheders brug af informations- og kommunikationsteknologiprodukter (IKT-produkter) i henhold til nævnte direktiv for at sikre et højere cybersikkerhedsniveau, forudsat at sådanne krav er i overensstemmelse med medlemsstaternes forpligtelser i henhold til EU-retten. Spørgsmål, der ikke er omfattet af denne forordning, kan omfatte ikketekniske faktorer vedrørende produkter med digitale elementer og fabrikanterne heraf. Medlemsstaterne kan derfor fastsætte nationale foranstaltninger, herunder restriktioner for produkter med digitale elementer eller leverandører af sådanne produkter, der tager hensyn til ikketekniske faktorer. Det er en forpligtelse, at nationale foranstaltninger vedrørende sådanne faktorer er i overensstemmelse med EU-retten.

(14) Denne forordning bør ikke berøre medlemsstaternes ansvar for beskyttelse af den nationale sikkerhed i overensstemmelse med EU-retten. Medlemsstaterne bør kunne underlægge produkter med digitale elementer, der indkøbes eller anvendes til nationale sikkerheds- eller forsvarsformål, yderligere foranstaltninger, forudsat at sådanne foranstaltninger er i overensstemmelse med medlemsstaternes forpligtelser, der er fastsat i EU-retten.

(15) Denne forordning finder kun anvendelse på erhvervsdrivende i forbindelse med produkter med digitale elementer, der gøres tilgængelige på markedet og dermed leveres med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed. Levering som led i erhvervsvirksomhed kan være kendetegnet ikke blot ved opkrævning af en pris for et produkt med digitale elementer, men også ved opkrævning af en pris for tekniske supporttjenester, hvor dette ikke blot tjener til dækning af de reelle omkostninger, ved et formål om at tjene penge, f. eks. ved tilrådighedsstillelse af en softwareplatform, hvorigennem fabrikanten tjener penge på andre tjenester, ved at kræve behandling af personoplysninger til andre formål end blot at forbedre softwarens sikkerhed, kompatibilitet eller interoperabilitet som forudsætning for anvendelsen, eller ved at modtage donationer, der overstiger de omkostninger, der er forbundet med design, udvikling og levering af et produkt med digitale elementer. Modtagelse af donationer uden gevinst for øje bør ikke anses som værende erhvervsvirksomhed.

(16) Produkter med digitale elementer, der leveres som en del af leveringen af en tjeneste, for hvilken der opkræves et gebyr udelukkende for at dække de faktiske omkostninger, der er direkte forbundet med driften af denne tjeneste, således som det kan være tilfældet for visse produkter med digitale elementer, der leveres af offentlige forvaltningsenheder, bør af disse grunde ikke i sig selv anses for at være erhvervsvirksomhed for så vidt angår denne forordning. Derudover bør produkter med digitale elementer, som udvikles eller ændres af en offentlig forvaltningsenhed udelukkende til eget brug, ikke anses for at være gjort tilgængelige på markedet i den i denne forordning anvendte betydning.

(17) Software og data, der deles åbent, og hvor brugerne frit kan få adgang til, bruge, ændre og videredistribuere dem eller ændrede versioner heraf, kan bidrage til forskning og innovation på markedet. For at fremme udviklingen og udbredelsen af gratis open source-software, navnlig af mikrovirksomheder og små og mellemstore virksomheder, herunder nyetablerede virksomheder, enkeltpersoner, nonprofitorganisationer og akademiske forskningsorganisationer, bør der ved anvendelsen af denne forordning på produkter med digitale elementer, der kan betegnes som gratis open source-software, der leveres med henblik på distribution eller anvendelse som led i erhvervsvirksomhed, tages hensyn til, at der findes forskellige udviklingsmodeller for software, der distribueres og udvikles under gratis open source software-licenser.

(18) Ved gratis open source-software forstås software, hvis kildekode deles åbent, og hvis licensering giver alle rettigheder til, at den kan deles åbent og er frit tilgængelig, anvendelig, redigerbar og redistribuerbar. Gratis open source-software udvikles, opdateres og distribueres åbent, herunder via onlineplatforme. For så vidt angår erhvervsdrivende, der er omfattet af denne forordnings anvendelsesområde, bør kun gratis open source-software, der stilles til rådighed på markedet og derfor leveres med henblik på distribution eller anvendelse som led i erhvervsvirksomhed, være omfattet af denne forordnings anvendelsesområde. De omstændigheder, hvorunder produktet er blevet udviklet, eller hvordan udviklingen er blevet finansieret, bør derfor ikke i sig selv tages i betragtning ved fastlæggelsen af den pågældende aktivitets kommercielle eller ikkekommercielle karakter. Mere specifikt bør levering af produkter med digitale elementer, der kan betegnes som gratis open source-software, som fabrikanterne ikke tjener penge på, ikke anses som værende erhvervsvirksomhed for så vidt angår denne forordning

og i forhold til de erhvervsdrivende, der er underlagt dens anvendelsesområde, for at sikre, at der skelnes klart mellem udviklings- og forsyningsfaserne. Desuden bør levering af produkter med digitale elementer, der kan betegnes som gratis open source software-komponenter, og som er beregnet til, at andre fabrikanter kan integrere dem i deres egne produkter med digitale elementer, kun anses som at være tilgængeliggørelse på markedet, hvis den oprindelige fabrikant tjener penge på komponenten. F.eks. bør den blotte omstændighed, at et open source software-produkt med digitale elementer modtager finansiel støtte fra fabrikanter, eller at fabrikanterne bidrager til udviklingen af et sådant produkt, ikke i sig selv være afgørende for, at der er tale om erhvervsvirksomhed. Desuden bør den blotte tilstedeværelse af regelmæssige udgivelser ikke i sig selv føre til den konklusion, at et produkt med digitale elementer leveres som led i erhvervsvirksomhed. Endelig bør nonprofitorganisationers udvikling af produkter med digitale elementer, der kan betegnes som gratis open source-software, med henblik på denne forordning ikke anses som værende erhvervsvirksomhed, forudsat at organisationen er oprettet på en sådan måde, at det sikres, at al indtjening efter fradrag af omkostninger anvendes til at nå almennyttige mål. Denne forordning finder ikke anvendelse på fysiske eller juridiske personer, der bidrager med kildekode til produkter med digitale elementer, der kan betegnes som gratis open source-software, som ikke er deres ansvar.

(19) I betragtning af hvilken betydning mange produkter med digitale elementer, der kan betegnes som gratis open source-software, og som offentliggøres, men ikke gøres tilgængelige på markedet i den i denne forordning anvendte betydning, spiller for cybersikkerheden, bør juridiske personer, der på vedvarende basis yder støtte til udvikling af sådanne produkter, der er beregnet til kommercielle aktiviteter, og som spiller en vigtig rolle med hensyn til at sikre disse produkters levedygtighed (open source software-forvaltere), være omfattet af en lempelig og skræddersyet reguleringsordning. Open source software-forvaltere omfatter visse fonde samt enheder, der udvikler og offentliggør gratis open source-software i en forretningssammenhæng, herunder almennyttige enheder. Reguleringsordningen bør tage hensyn til deres særlige karakter og forenelighed med den type forpligtelser, der pålægges. Den bør kun omfatte produkter med digitale elementer, der kan betegnes som gratis open source-software, såfremt disse i sidste ende er beregnet til erhvervsvirksomhed såsom integration i kommercielle tjenester eller i produkter med digitale elementer, som der tjenes penge på. For så vidt angår denne reguleringsordning omfatter en hensigt om integration i produkter med digitale elementer, som der tjenes penge på, tilfælde, hvor fabrikanter, der integrerer en komponent i deres egne produkter med digitale elementer, enten bidrager regelmæssigt til udviklingen af den pågældende komponent eller yder regelmæssig finansiel bistand for at sikre kontinuiteten af et softwareprodukt. Vedvarende støtte til udvikling af et produkt med digitale elementer omfatter, men er ikke begrænset til, hosting og forvaltning af samarbejdsplatforme for softwareudvikling, hosting af kildekode eller software, styring eller forvaltning af produkter med digitale elementer, der kan betegnes som gratis open source-software, samt styring af udviklingen af sådanne produkter. Eftersom den lempelige og skræddersyede reguleringsordning ikke pålægger dem, der optræder som open source software-forvaltere, de samme forpligtelser som dem, der optræder som fabrikanter i henhold til denne forordning, bør de ikke have lov til at anbringe CE-mærkningen på produkter med digitale elementer, hvis udvikling de yder støtte til.

(20) Den blotte handling at hoste free and open source software i åbne databaser, herunder via pakkestyringssystemer eller på samarbejdsplatforme, udgør ikke i sig selv tilgængeliggørelse på markedet af et produkt med digitale elementer. Leverandører af sådanne tjenester bør kun anses som værende distributører, hvis de gør den pågældende software tilgængelig på markedet og dermed leverer den med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed.

(21) For at støtte og lette due diligence hos fabrikanter, der integrerer gratis open source software-komponenter, der ikke er omfattet af de væsentlige cybersikkerhedskrav, der er fastsat i denne forordning, i deres produkter med digitale elementer, bør Kommissionen kunne oprette frivillige sikkerhedscertificeringsprogrammer, enten ved en delegeret retsakt, der supplerer denne forordning, eller ved at anmode om en europæisk cybersikkerhedscertificeringsordning i henhold til artikel 48 i forordning (EU) 2019/881, som tager hensyn til de særlige forhold, der gør sig gældende for gratis open source software-udviklingsmodeller. Sikkerhedscertificeringsprogrammerne bør udformes på en sådan måde, at ikke blot fysiske eller juridiske personer, der udvikler eller bidrager til udviklingen af et produkt med digitale elementer, der kan betegnes som gratis open source-software, kan iværksætte eller finansiere en sikkerhedsattestering, men også tredjeparter såsom fabrikanter, der integrerer sådanne produkter i deres egne produkter med digitale elementer, brugere eller Unionens og de nationale offentlige forvaltninger.

(22) I lyset af denne forordnings mål vedrørende offentlig cybersikkerhed og for at forbedre medlemsstaternes situationsbevidsthed med hensyn til Unionens afhængighed af softwarekomponenter og navnlig af potentielle gratis open source software-komponenter bør en særlig administrativ samarbejdsgruppe (ADCO), der nedsættes ved denne forordning, kunne beslutte i fællesskab at foretage en EU-afhængighedsvurdering. Markedsovervågningsmyndighederne bør kunne anmode fabrikanter af kategorier af produkter med digitale elementer, der er opstillet af ADCO, om at indsende de softwarekomponentlister, som de har genereret i henhold til denne forordning. For at beskytte fortroligheden af softwarestyklisterne bør markedsovervågningsmyndighederne indsende relevante oplysninger om afhængighedsforhold til ADCO på en anonymiseret og aggregeret måde.

(23) Effektiviteten af gennemførelsen af denne forordning vil også afhænge af tilgængeligheden af tilstrækkelige cybersikkerhedsfærdigheder. På EU-plan anerkendte forskellige program- og politikdokumenter såsom Kommissionens meddelelse af 18. april 2023 med titlen »Opbygning af cybersikkerhedskompetencer skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed« og Rådets konklusioner af 22. maj 2023 om EU's cyberforsvarspolitik manglen på cybersikkerhedskompetencer i Unionen og behovet for at prioritere håndteringen af sådanne udfordringer i både den offentlige og den private sektor. Med henblik på at sikre en effektiv gennemførelse af denne forordning bør medlemsstaterne sikre, at der er tilstrækkelige ressourcer til rådighed til, at markedsovervågningsmyndighederne og overensstemmelsesvurderingsorganerne kan udføre deres opgaver som fastsat i denne forordning. Disse foranstaltninger bør øge arbejdskraftens mobilitet på cybersikkerhedsområdet og de dermed forbundne karriereveje. De bør også bidrage til at gøre cybersikkerhedsarbejdsstyrken mere modstandsdygtig og inklusiv, også med hensyn til køn. Medlemsstaterne bør derfor træffe foranstaltninger til at sikre, at disse opgaver udføres af tilstrækkeligt uddannede fagfolk med de nødvendige cybersikkerhedskompetencer. Fabrikanterne bør ligeledes sikre, at deres personale har de nødvendige færdigheder til at opfylde deres forpligtelser som fastlagt i denne forordning. Medlemsstaterne og Kommissionen bør i overensstemmelse med deres prærogativer og kompetencer og de specifikke opgaver, som denne forordning pålægger dem, træffe foranstaltninger til at støtte fabrikanter og navnlig mikrovirksomheder og små og mellemstore virksomheder, herunder nyetablerede virksomheder, også på områder såsom kompetenceudvikling, med henblik på at opfylde deres forpligtelser som fastlagt i denne forordning. Da direktiv (EU) 2022/2555 desuden kræver, at medlemsstaterne vedtager politikker, der fremmer og udvikler uddannelse i cybersikkerhed og cybersikkerhedsfærdigheder som led i deres nationale cybersikkerhedsstrategier, kan medlemsstaterne, når de vedtager sådanne strategier, også overveje at imødekomme de behov for cybersikkerhedsfærdigheder, der følger af denne forordning, herunder dem, der vedrører omskoling og opkvalificering.

(24) Et sikkert internet er uundværligt for kritiske infrastrukturers funktion og for samfundet som helhed. Direktiv (EU) 2022/2555 har til formål at sikre et højt cybersikkerhedsniveau for tjenester, der leveres af væsentlige og vigtige enheder som omhandlet i nævnte direktivs artikel 3, herunder udbydere af digital infrastruktur, der understøtter centrale funktioner i det åbne internet og sikrer internetadgang og leverer internettjenester. Det er derfor vigtigt, at produkter med digitale elementer, der er nødvendige for, at udbydere af digital infrastruktur kan sikre, at internettet fungerer, udvikles på en sikker måde, og at de overholder veletablerede standarder for internetsikkerhed. Denne forordning, som finder anvendelse på alle hardware- og softwareprodukter, der kan forbindes, har også til formål at gøre det lettere for udbydere af digital infrastruktur at overholde kravene i forsyningskæden i henhold til direktiv (EU) 2022/2555 ved at sikre, at de produkter med digitale elementer, som de anvender i forbindelse med leveringen af deres tjenester, udvikles på en sikker måde, og at de har adgang til rettidige sikkerhedsopdateringer for sådanne produkter.

(25) Europa-Parlamentets og Rådets forordning (EU) 2017/745 ([9]) fastsætter regler om medicinsk udstyr, og Europa-Parlamentets og Rådets forordning (EU) 2017/746 ([10]) fastsætter regler om medicinsk udstyr til in vitro-diagnostik. Nævnte forordninger omhandler cybersikkerhedsrisici og følger særlige tilgange, der også behandles i nærværende forordning. Mere specifikt fastsætter forordning (EU) 2017/745 og (EU) 2017/746 væsentlige krav til medicinsk udstyr, der fungerer via et elektronisk system, eller som selv er software. Visse former for ikkeindlejret software og livscyklustilgangen behandles også i nævnte forordninger. Disse krav giver fabrikanterne mandat til at udvikle og bygge deres produkter ved at anvende risikostyringsprincipper og ved at fastsætte krav vedrørende IT-sikkerhedsforanstaltninger samt tilsvarende overensstemmelsesvurderingsprocedurer. Derudover blev der i december 2019 indført specifik vejledning om cybersikkerhed for medicinsk udstyr, som giver fabrikanter af medicinsk udstyr, herunder udstyr til in vitro-diagnostik, vejledning i, hvordan de opfylder alle de relevante væsentlige krav i bilag I til nævnte forordninger for så vidt angår cybersikkerhed. Produkter med digitale elementer, som en af nævnte forordninger finder anvendelse på, bør derfor ikke være omfattet af nærværende forordning.

(26) Produkter med digitale elementer, der udelukkende udvikles eller ændres til nationale sikkerheds- eller forsvarsformål, eller produkter, som er specifikt designet til behandling af fortrolige oplysninger, er ikke omfattet af denne forordnings anvendelsesområde. Medlemsstaterne opfordres til at sikre det samme eller et højere niveau af beskyttelse af disse produkter som af de produkter, der er omfattet af denne forordnings anvendelsesområde.

([9]) Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, om ændring af direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om ophævelse af Rådets direktiv 90/385/EØF og 93/42/EØF (EUT L 117 af 5.5.2017, s. 1).

([10]) Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik og om ophævelse af direktiv 98/79/EF og Kommissionens afgørelse 2010/227/EU (EUT L 117 af 5.5.2017, s. 176).

(27) Ved Europa-Parlamentets og Rådets forordning (EU) 2019/2144 ([11]) fastsættes krav til typegodkendelse af køretøjer og deres systemer og komponenter, idet der indføres en række cybersikkerhedskrav, herunder vedrørende drift af et certificeret cybersikkerhedsstyringssystem og softwareopdateringer, der dækker organisationers politikker og processer for styring af cybersikkerhedsrisici i hele livscyklussen for køretøjer, udstyr og tjenester under overholdelse af de gældende FN-regulativer om tekniske specifikationer og cybersikkerhed, navnlig FN-regulativ nr. 155 — Ensartede forskrifter for godkendelse af køretøjer for så vidt angår cybersikkerhed og systemer til forvaltning af cybersikkerhed ([12]), og der indføres specifikke overensstemmelsesvurderingsprocedurer. På luftfartsområdet er hovedformålet med Europa-Parlamentets og Rådets forordning (EU) 2018/1139 ([13]) at fastlægge og opretholde et højt og ensartet sikkerhedsniveau for den civile luftfart i Unionen. Den skaber en ramme for væsentlige krav til luftdygtighed for luftfartøjsmateriel, dele og udstyr, herunder software, der omfatter forpligtelser til at beskytte mod trusler mod informationssikkerheden. Certificeringsprocessen i henhold til forordning (EU) 2018/1139 sikrer det samme beskyttelsesniveau som det, der er fastsat i nærværende forordning. Produkter med digitale elementer, som forordning (EU) 2019/2144 finder anvendelse på, og produkter, der er certificeret i overensstemmelse med forordning (EU) 2018/1139, bør derfor ikke være omfattet af de væsentlige cybersikkerhedskrav og overensstemmelsesvurderingsprocedurerne i nærværende forordning.

(28) I denne forordning fastsættes horisontale cybersikkerhedsregler, som ikke er specifikke for sektorer eller visse produkter med digitale elementer. Der kan imidlertid indføres sektor- eller produktspecifikke EU-forskrifter, der fastlægger krav vedrørende alle eller nogle af de risici, der er omfattet af de væsentlige cybersikkerhedskrav i denne forordning. I sådanne tilfælde kan anvendelsen af denne forordning på produkter med digitale elementer, som er omfattet af andre EU-forskrifter, der fastlægger krav vedrørende alle eller nogle af de risici, som er omfattet af de væsentlige cybersikkerhedskrav i denne forordning, begrænses eller udelukkes, hvor en sådan begrænsning eller udelukkelse er i overensstemmelse med den overordnede lovgivningsmæssige ramme, der gælder for disse produkter, og hvor de sektorspecifikke regler sikrer mindst samme beskyttelsesniveau som det, der er fastsat i denne forordning. Kommissionen bør tillægges beføjelser til at vedtage delegerede retsakter for at supplere denne forordning ved at identificere sådanne produkter og forskrifter. For eksisterende EU-ret, hvor sådanne begrænsninger eller udelukkelser bør finde anvendelse, indeholder denne forordning specifikke bestemmelser for at præcisere dens sammenhæng med den pågældende EU-ret.

(29) For at sikre, at produkter med digitale elementer, der gøres tilgængelige på markedet, kan repareres effektivt, og at deres holdbarhed kan forlænges, bør der fastsættes en undtagelse for reservedele. Denne undtagelse bør omfatte både reservedele, der har til formål at reparere ældre produkter, som er gjort tilgængelige før anvendelsesdatoen for denne forordning, og for reservedele, der allerede har gennemgået en overensstemmelsesvurderingsprocedure i henhold til denne forordning.

(30) I Kommissionens delegerede forordning (EU) 2022/30 ([14]) præciseres det, at en række væsentlige krav i artikel 3, stk. 3, litra d), e) og f), i Europa-Parlamentets og Rådets direktiv 2014/53/EU ([15]) vedrørende skade på nettet og misbrug af netressourcer, personoplysninger og privatlivets fred samt svig finder anvendelse på visse typer radioudstyr. I Kommissionens gennemførelsesafgørelse C(2022)5637 af 5. august 2022 om en standardiseringsanmodning til Den Europæiske Standardiseringsorganisation og Den Europæiske Komité for Elektroteknisk Standardisering fastsættes krav til udviklingen af specifikke standarder med nærmere angivelse af, hvordan disse væsentlige krav bør håndteres. De væsentlige cybersikkerhedskrav i nærværende forordning omfatter alle elementerne i de væsentlige krav, der er omhandlet i artikel 3, stk. 3, litra d), e) og f), i direktiv 2014/53/EU.

([11]) Europa-Parlamentets og Rådets forordning (EU) 2019/2144 af 27. november 2019 om krav til typegodkendelse af motorkøretøjer og påhængskøretøjer dertil samt systemer, komponenter og separate tekniske enheder til sådanne køretøjer for så vidt angår deres generelle sikkerhed og beskyttelsen af køretøjspassagerer og bløde trafikanter og om ændring af Europa-Parlamentets og Rådets forordning (EU) 2018/858 og ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 78/2009, forordning (EF) nr. 79/2009 og forordning (EF) nr. 661/2009 og Kommissionens forordning (EF) 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 og (EU) 2015/166 (EUT L 325 af 16.12.2019, s. 1).

([12]) EUT L 82 af 9.3.2021, s. 30.

([13]) Europa-Parlamentets og Rådets forordning (EU) 2018/1139 af 4. juli 2018 om fælles regler for civil luftfart og oprettelse af Den Europæiske Unions Luftfartssikkerhedsagentur og om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og direktiv 2014/30/EU og 2014/53/EU og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 552/2004 og (EF) nr. 216/2008 og Rådets forordning (EØF) nr. 3922/91 (EUT L 212 af 22.8.2018, s. 1).

([14]) Kommissionens delegerede forordning (EU) 2022/30 af 29. oktober 2021 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2014/53/EU for så vidt angår anvendelsen af de væsentlige krav, der er omhandlet i nævnte direktivs artikel 3, stk. 3, litra d), e) og f) (EUT L 7 af 12.1.2022, s. 6).

([15]) Europa-Parlamentets og Rådets direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet og om ophævelse af direktiv 1999/5/EF (EUT L 153 af 22.5.2014, s. 62).

Endvidere er de væsentlige cybersikkerhedskrav i nærværende forordning i overensstemmelse med målene for kravene til specifikke standarder, der er omfattet af denne standardiseringsanmodning. Når Kommissionen ophæver eller ændrer delegeret forordning (EU) 2022/30 med den konsekvens, at den ophører med at finde anvendelse på visse produkter, der er omfattet af nærværende forordning, bør Kommissionen og de europæiske standardiseringsorganisationer derfor tage hensyn til det standardiseringsarbejde, der er udført i forbindelse med gennemførelsesafgørelse C(2022)5637, ved udarbejdelsen og udviklingen af harmoniserede standarder for at lette gennemførelsen af nærværende forordning. I overgangsperioden for anvendelsen af nærværende forordning bør Kommissionen yde vejledning til fabrikanter omfattet af nærværende forordning, som også er omfattet af delegeret forordning (EU) 2022/30, for at lette påvisningen af overensstemmelse med de to forordninger.

(31) Europa-Parlamentets og Rådets direktiv (EU) 2024/2853 ([16]) supplerer denne forordning. Nævnte direktiv fastsætter regler om produktansvar, således at skadelidte kan kræve erstatning for skade forårsaget af defekte produkter. Det fastsætter princippet om, at fabrikanten af et produkt er ansvarlig for skader forårsaget af produktets manglende sikkerhed uanset fejl (»objektivt ansvar«). Hvis en sådan mangel på sikkerhed består i manglende sikkerhedsopdateringer, efter at produktet er bragt i omsætning, og dette forårsager skade, kan fabrikantens ansvar udløses. Fabrikanternes forpligtelser vedrørende levering af sådanne sikkerhedsopdateringer bør fastsættes i denne forordning.

(32) Denne forordning bør ikke berøre Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([17]), herunder bestemmelser vedrørende fastlæggelse af certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og databehandleres behandlingsaktiviteter overholder nævnte forordning. Sådanne aktiviteter kan indlejres i et produkt med digitale elementer. Databeskyttelse gennem design og gennem standardindstillinger samt cybersikkerhed generelt er centrale elementer i forordning (EU) 2016/679. Ved at beskytte forbrugere og organisationer mod cybersikkerhedsrisici skal de væsentlige cybersikkerhedskrav i nærværende forordning også bidrage til at forbedre beskyttelsen af personoplysninger og privatlivets fred for enkeltpersoner. Synergier med hensyn til både standardisering og certificering af cybersikkerhedsaspekter bør overvejes inden for rammerne af samarbejdet mellem Kommissionen, de europæiske standardiseringsorganisationer, Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), Det Europæiske Databeskyttelsesråd, der er oprettet ved forordning (EU) 2016/679, og de nationale databeskyttelsestilsynsmyndigheder. Der bør også skabes synergier mellem nærværende forordning og EU-databeskyttelsesretten inden for markedsovervågning og håndhævelse. Med henblik herpå bør nationale markedsovervågningsmyndigheder udpeget i henhold til nærværende forordning samarbejde med myndigheder, der fører tilsyn med anvendelsen af EU-databeskyttelsesretten. Sidstnævnte myndigheder bør også have adgang til oplysninger, der er relevante for udførelsen af deres opgaver.

(33) I det omfang deres produkter er omfattet af denne forordnings anvendelsesområde, bør leverandører af europæiske digitale identitetstegnebøger som omhandlet i artikel 5a, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([18]) opfylde både de horisontale væsentlige cybersikkerhedskrav, der er fastsat i nærværende forordning, og de specifikke sikkerhedskrav, der er fastsat i artikel 5a i forordning (EU) nr. 910/2014. For at lette overholdelsen bør udbydere af tegnebøger kunne påvise, at europæiske digitale identitetstegnebøger opfylder de krav, der er fastsat henholdsvis i nærværende forordning og i forordning (EU) nr. 910/2014, ved at certificere deres produkter i henhold til en europæisk cybersikkerhedscertificeringsordning, der er oprettet i henhold til forordning (EU) 2019/881, og for hvilken Kommissionen har angivet ved hjælp af delegerede retsakter, at den kan danne grundlag for formodning om overensstemmelse med nærværende forordning, såfremt attesten eller dele heraf dækker disse krav.

(34) Når fabrikanter integrerer komponenter fra tredjeparter i produkter med digitale elementer under design- og udviklingsfasen, bør de for at sikre, at produkterne designes, udvikles og produceres i overensstemmelse med de væsentlige cybersikkerhedskrav i denne forordning, foretage due diligence med hensyn til disse komponenter, herunder gratis open-source software-komponenter, der ikke er gjort tilgængelige på markedet. Det passende niveau

([16]) Europa-Parlamentets og Rådets direktiv (EU) 2024/2853 af 23. oktober 2024 om produktansvar og om ophævelse af Rådets direktiv 85/374/EØF (EUT L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

([18]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

af due diligence afhænger af en given komponents art og det niveau af cybersikkerhedsrisiko, som en given komponent anses for at have, og bør med dette for øje tage en eller flere af følgende tiltag i betragtning: kontrol af, at fabrikanten af en komponent har påvist overensstemmelse med denne forordning, herunder ved at kontrollere, om komponenten allerede er forsynet med CE-mærkning, i det omfang dette er relevant; kontrol af, at en komponent modtager regelmæssige sikkerhedsopdateringer såsom ved at kontrollere dens sikkerhedshistorik; kontrol af, at en komponent er fri for sårbarheder registreret i den europæiske sårbarhedsdatabase, der er oprettet i henhold til artikel 12, stk. 2, i direktiv (EU) 2022/2555, eller andre offentligt tilgængelige sårbarhedsdatabaser; eller gennemførelse af yderligere sikkerhedsafprøvninger. De forpligtelser vedrørende sårbarhedshåndtering, der er fastsat i denne forordning, og som fabrikanterne skal overholde, når de bringer et produkt med digitale elementer i omsætning og i supportperioden, finder anvendelse på produkter med digitale elementer i deres helhed, herunder alle integrerede komponenter. Hvor fabrikanten af produktet i forbindelse med foretagelsen af due diligence identificerer en sårbarhed i en komponent, herunder i en gratis open source-komponent, bør fabrikanten underrette den person eller enhed, der udvikler eller vedligeholder komponenten, tage hånd om og afhjælpe sårbarheden og, i givet fald, stille den anvendte sikkerhedsløsning til rådighed for personen eller enheden.

(35) Umiddelbart efter overgangsperioden for anvendelsen af denne forordning er en fabrikant af et produkt med digitale elementer, der integrerer en eller flere komponenter fra tredjeparter, som også er omfattet af denne forordning, muligvis ikke i stand til som led i sin due diligence-forpligtelse at kontrollere, at fabrikanterne af disse komponenter har påvist overensstemmelse med denne forordning, ved f.eks. at kontrollere, om komponenterne allerede er forsynet med CE-mærkning. Dette kan være tilfældet, hvis komponenterne er blevet integreret, før denne forordning finder anvendelse på fabrikanterne af de pågældende komponenter. I så fald bør en fabrikant, der integrerer sådanne komponenter, foretage due diligence ved hjælp af andre midler.

(36) Produkter med digitale elementer bør være forsynet med CE-mærkning for synligt, læseligt og uudsletteligt at vise, at de er i overensstemmelse med denne forordning, således at de kan bevæge sig frit på det indre marked. Medlemsstaterne bør ikke skabe uberettigede hindringer for omsætning af produkter med digitale elementer, der opfylder kravene i denne forordning, og som er forsynet med CE-mærkning. Endvidere bør medlemsstaterne ikke forhindre, at der på messer og udstillinger samt ved demonstrationer eller lignende begivenheder præsenteres eller anvendes et produkt med digitale elementer, der ikke er i overensstemmelse med denne forordning, herunder prototyper heraf, forudsat at produktet præsenteres med et synlig skilt, hvoraf det tydeligt fremgår, at det ikke overholder denne forordning og ikke må gøres tilgængeligt på markedet, før det gør det.

(37) For at sikre, at fabrikanterne kan frigive software til afprøvningsformål, inden deres produkter med digitale elementer underkastes en overensstemmelsesvurdering, bør medlemsstaterne ikke forhindre, at ufærdig software såsom alfaversioner, betaversioner eller versioner, som er klar til frigivelse, stilles til rådighed, forudsat at den ufærdige software kun stilles til rådighed i det tidsrum, der er nødvendigt for at afprøve den og indsamle feedback. Fabrikanterne bør sikre, at software, der stilles til rådighed under disse betingelser, først frigives efter en risikovurdering, og at den i videst muligt omfang opfylder de sikkerhedskrav vedrørende egenskaberne ved produkter med digitale elementer, der er fastsat i denne forordning. Fabrikanterne bør også gennemføre kravene til håndtering af sårbarheder i videst muligt omfang. Fabrikanterne bør ikke tvinge brugerne til at opgradere til versioner, der kun frigives til afprøvningsformål.

(38) For at sikre, at produkter med digitale elementer, når de bringes i omsætning, ikke indebærer cybersikkerhedsrisici for personer og organisationer, bør der fastsættes væsentlige cybersikkerhedskrav til sådanne produkter. Disse væsentlige cybersikkerhedskrav, herunder krav til håndtering af sårbarheder, finder anvendelse på hvert enkelt produkt med digitale elementer, når det bringes i omsætning, uanset om produktet med digitale elementer fremstilles som en individuel enhed eller i serier. For en produkttype bør hvert enkelt produkt med digitale elementer f.eks. have modtaget alle sikkerhedsrettelser eller opdateringer, der er tilgængelige til at håndtere relevante sikkerhedsproblemer, når den bringes i omsætning. Hvor produkter med digitale elementer efterfølgende ændres fysisk eller digitalt på en måde, som fabrikanten ikke har forudset i den indledende risikovurdering, og som kan indebære, at de ikke længere opfylder de relevante væsentlige cybersikkerhedskrav, bør ændringen anses som værende væsentlig. reparationer kunne f.eks. sammenlignes med vedligeholdelse, såfremt de ikke ændrer et produkt med digitale elementer, der allerede er bragt i omsætning, på en sådan måde, at det påvirker overholdelsen af de gældende krav, eller såfremt det tilsigtede formål, som produktet vurderes med henblik på, kan ændres.

(39) Som det er tilfældet med fysiske reparationer eller ændringer, bør et produkt med digitale elementer anses for at være væsentligt ændret ved en softwareændring, hvor softwareopdateringen ændrer produktets tilsigtede formål, og disse ændringer ikke var forudset af fabrikanten i den indledende risikovurdering, eller hvor farens art har ændret sig, eller

cybersikkerhedsrisikoniveauet er forøget som følge af softwareopdateringen, og den opdaterede version af produktet gøres tilgængeligt på markedet. Hvor en sikkerhedsopdatering, der er udformet med henblik på at mindske cybersikkerhedsrisikoen ved et produkt med digitale elementer, ikke ændrer det tilsigtede formål med et produkt med digitale elementer, anses den ikke som værende en væsentlig ændring. Dette omfatter normalt situationer, hvor en sikkerhedsopdatering kun medfører mindre justeringer af kildekoden. Dette kunne f.eks. være tilfældet, hvor en sikkerhedsopdatering retter op på en kendt sårbarhed, herunder ved at ændre funktioner eller ydeevne for et produkt med digitale elementer med det ene formål at mindske cybersikkerhedsrisikoniveauet. På samme måde bør en mindre funktionalitetsopdatering såsom en visuelle forbedring eller tilføjelse af nye piktogrammer eller sprog til brugergrænsefladen generelt ikke anses som værende en væsentlig ændring. Hvis en funktionsopdatering derimod ændrer de oprindelige tilsigtede funktioner eller typen eller ydeevnen af et produkt med digitale elementer og opfylder ovennævnte kriterier, bør den anses som værende en væsentlig ændring, da tilføjelsen af nye funktioner typisk fører til en bredere angrebsflade og dermed øger cybersikkerhedsrisikoen. Dette kunne f.eks. være tilfældet, hvis der tilføjes et nyt inputelement til en applikation, der kræver, at fabrikanten sikrer tilstrækkelig inputvalidering. Ved vurderingen af, hvorvidt en funktionsopdatering anses som værende en væsentlig ændring, er det ikke relevant, om den leveres som en separat opdatering eller i kombination med en sikkerhedsopdatering. Kommissionen bør yde vejledning for, hvordan det fastslås, hvad der udgør en væsentlig ændring.

(40) Under hensyntagen til softwareudviklings iterative karakter bør fabrikanter, der har bragt efterfølgende versioner af et softwareprodukt i omsætning som følge af en efterfølgende væsentlig ændring af det pågældende produkt, kun skulle være i stand til at levere sikkerhedsopdateringer i supportperioden for den version af softwareproduktet, som de senest har bragt i omsætning. De bør kun skulle være i stand til at gøre dette, hvis brugerne af de relevante tidligere produktversioner har gratis adgang til den produktversion, der senest er bragt i omsætning, og ikke pådrager sig yderligere omkostninger til tilpasning af det hardware- eller softwaremiljø, som de anvender produktet i. Dette kunne f.eks. være tilfældet, hvor en opgradering af et desktopoperativsystem ikke kræver ny hardware såsom en hurtigere central databehandlingsenhed eller mere hukommelse. Ikke desto mindre bør fabrikanten i supportperioden fortsat overholde andre krav til sårbarhedshåndtering såsom at have en politik for koordineret offentliggørelse af sårbarheder eller foranstaltninger på plads til at lette udvekslingen af oplysninger om potentielle sårbarheder for alle efterfølgende væsentligt ændrede versioner af det softwareprodukt, der bringes i omsætning. Fabrikanter bør kun skulle være i stand til at levere mindre sikkerheds- eller funktionalitetsopdateringer, der ikke udgør en væsentlig ændring, til den seneste version eller underversion af et softwareprodukt, der ikke er blevet væsentligt ændret. Hvor et hardwareprodukt såsom en smartphone ikke er kompatibelt med den seneste version af operativsystemet, som det oprindeligt blev leveret sammen med, bør fabrikanten samtidig fortsat levere sikkerhedsopdateringer som minimum til den seneste kompatible version af operativsystemet i supportperioden.

(41) I overensstemmelse med det almindeligt anerkendte begreb væsentlig ændring for produkter, der er reguleret ved EU-harmoniseringslovgivning, er det hensigtsmæssigt, at det verificeres, om et produkt med digitale elementer overholder kravene, og i givet fald underkastes en ny overensstemmelsesvurdering, hvor der sker en væsentlig ændring, som kan påvirke produktets overensstemmelse med denne forordning, eller når produktets tilsigtede formål ændres. Hvis fabrikanten foretager en overensstemmelsesvurdering, der involverer en tredjepart, bør tredjeparten i givet fald underrettes om en ændring, der kunne føre til en væsentlig ændring.

(42) Hvor et produkt med digitale elementer er genstand for »istandsættelse«, »vedligeholdelse« og »reparation« som defineret i artikel 2, nr. 18), 19) og 20), i Europa-Parlamentets og Rådets forordning (EU) 2024/1781 ([19]), fører dette ikke nødvendigvis til en væsentlig ændring af produktet, f.eks. hvis det tilsigtede formål og den tilsigtede funktionalitet ikke ændres, og risikoniveauet ikke påvirkes. En fabrikants opgradering af et produkt med digitale elementer kan imidlertid føre til ændringer i det pågældende produkts design og udvikling og kan derfor påvirke dets tilsigtede formål og opfyldelse af kravene i nærværende forordning.

(43) Produkter med digitale elementer bør anses som værende vigtige, hvis den negative indvirkning af udnyttelsen af potentielle cybersikkerhedssårbarheder i produktet kan være alvorlig, bl.a. på grund af den cybersikkerhedsrelaterede funktionalitet eller en funktion, der indebærer en betydelig risiko for negative virkninger med hensyn til intensitet og evne til at afbryde, kontrollere eller forvolde skade på et stort antal andre produkter med digitale elementer eller på dets brugeres sundhed, sikkerhed eller tryghed gennem direkte manipulation såsom en central systemfunktion, herunder netværksstyring, konfigurationskontrol, virtualisering eller behandling af personoplysninger. Sårbarheder i produkter med digitale elementer, der har en cybersikkerhedsrelateret funktionalitet, såsom boot managers kan navnlig skabe en lang række sikkerhedsproblemer i hele forsyningskæden. Indvirkningen af en hændelse kan også

([19]) Europa-Parlamentets og Rådets forordning (EU) 2024/1781 af 13. juni 2024 om fastlæggelse af en ramme for fastsættelse af krav til miljøvenligt design for bæredygtige produkter, om ændring af direktiv (EU) 2020/1828 og forordning (EU) 2023/1542 og om ophævelse af direktiv 2009/125/EF (EUT L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

blive mere alvorlig, hvor produktet primært udfører en central systemfunktion, herunder netværksstyring, konfigurationskontrol, virtualisering eller behandling af personoplysninger.

(44) Visse kategorier af produkter med digitale elementer bør være underlagt strengere overensstemmelsesvurderingsprocedurer, samtidig med at der sikres en forholdsmæssig tilgang. Med henblik herpå bør vigtige produkter med digitale elementer inddeles i to klasser, der afspejler cybersikkerhedsrisikoniveauet for disse produktkategorier. En hændelse, der involverer vigtige produkter med digitale elementer, der er omfattet af klasse II, kan have større negative virkninger end en hændelse, der involverer vigtige produkter med digitale elementer, der er omfattet af klasse I, f.eks. på grund af arten af deres cybersikkerhedsrelaterede funktion eller udførelsen af en anden funktion, som indebærer en betydelig risiko for negative virkninger. Som en indikation af sådanne større negative virkninger kan produkter med digitale elementer, der er omfattet af klasse II, enten udføre en cybersikkerhedsrelateret funktionalitet eller en anden funktion, der indebærer en betydelig risiko for negative virkninger, der er højere end for dem, der er opført i klasse I, eller opfylde begge ovennævnte kriterier. Vigtige produkter med digitale elementer, der henhører under klasse II, bør derfor underkastes en strengere overensstemmelsesvurderingsprocedure.

(45) Vigtige produkter med digitale elementer som omhandlet i denne forordning bør forstås som de produkter, hvis væsentligste funktionalitet henhører under en kategori af vigtige produkter med digitale elementer, der er fastsat i denne forordning. F.eks. fastsætter denne forordning kategorier af vigtige produkter med digitale elementer, der defineres ud fra deres væsentligste funktionalitet som firewalls eller systemer til opdagelse eller forebyggelse af indtrængen i klasse II. Som følge heraf er firewalls eller systemer til opdagelse eller forebyggelse af indtrængen underkastet obligatorisk tredjepartsoverensstemmelsesvurdering. Dette er ikke tilfældet for andre produkter med digitale elementer, der ikke kategoriseres som vigtige produkter med digitale elementer, og som kan integrere firewalls eller systemer til opdagelse eller forebyggelse af indtrængen. Kommissionen bør vedtage en gennemførelsesretsakt for at præcisere den tekniske beskrivelse af de kategorier af vigtige produkter med digitale elementer, der falder ind under kategori I og II som fastsat i denne forordning.

(46) De kategorier af kritiske produkter med digitale elementer, der er fastsat i denne forordning, har en cybersikkerhedsrelateret funktionalitet og udfører en funktionalitet, der indebærer en betydelig risiko for negative virkninger med hensyn til intensitet og evne til at afbryde, kontrollere eller forvolde skade på et stort antal andre produkter med digitale elementer gennem direkte manipulation. Derudover anses disse kategorier af produkter med digitale elementer for at udgøre kritiske afhængighedsforhold for væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555. De kategorier af kritiske produkter med digitale elementer, der er fastsat i et bilag til denne forordning, anvender allerede i betragtning af deres kritikalitet i vid udstrækning forskellige former for certificering og er også omfattet af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC), der er fastsat i Kommissionens gennemførelsesforordning (EU) 2024/482 ([20]). For at sikre en fælles tilstrækkelig cybersikkerhedsbeskyttelse af kritiske produkter med digitale elementer i Unionen kunne det derfor være hensigtsmæssigt og forholdsmæssigt ved hjælp af en delegeret retsakt at underkaste sådanne produktkategorier en obligatorisk europæisk cybersikkerhedscertificering, hvor der allerede findes en relevant europæisk cybersikkerhedscertificeringsordning, der dækker disse produkter, og Kommissionen har foretaget en vurdering af den potentielle indvirkning på markedet af den påtænkte obligatoriske certificering. Denne vurdering bør tage hensyn til både udbuds- og efterspørgselssiden, herunder om der er tilstrækkelig efterspørgsel efter produkter med de pågældende digitale elementer fra både medlemsstater og brugere til, at der kræves europæisk cybersikkerhedscertificering, samt de formål, hvortil produkter med digitale elementer skal anvendes, herunder at der er en kritisk afhængighed af dem hos væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555. Vurderingen bør også analysere de potentielle virkninger af den obligatoriske certificering på tilgængeligheden af disse produkter på det indre marked og medlemsstaternes kapacitet og parathed til at gennemføre de relevante europæiske cybersikkerhedscertificeringsordninger.

(47) Delegerede retsakter, der kræver obligatorisk europæisk cybersikkerhedscertificering, bør fastlægge de produkter med digitale elementer, hvis væsentligste funktionalitet henhører under en kategori af kritiske produkter med digitale elementer, der er fastsat i denne forordning, og som skal være underlagt obligatorisk certificering, samt det krævede tillidsniveau, der som minimum bør være »betydeligt«. Det krævede tillidsniveau bør stå i et rimeligt forhold til det cybersikkerhedsrisikoniveau, der er forbundet med produktet med digitale elementer. Hvor et produkt med digitale elementer, hvis væsentligste funktionalitet henhører under en kategori af kritiske produkter med digitale elementer,

([20]) Kommissionens gennemførelsesforordning (EU) 2024/482 af 31. januar 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

der er fastsat i denne forordning, f.eks. er beregnet til anvendelse i et følsomt eller kritisk miljø såsom produkter beregnet til anvendelse af væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555 kan det kræve det højeste tillidsniveau.

(48) For at sikre en fælles tilstrækkelig cybersikkerhedsbeskyttelse i Unionen af produkter med digitale elementer, hvis væsentligste funktionalitet henhører under en kategori af kritiske produkter med digitale elementer, der er fastsat i denne forordning, bør Kommissionen også tillægges beføjelse til at vedtage delegerede retsakter med henblik på at ændre denne forordning ved at tilføje eller fjerne kategorier af kritiske produkter med digitale elementer, for hvilke fabrikanterne kan pålægges at indhente en europæisk cybersikkerhedsattest i henhold til en europæisk cybersikkerhedscertificeringsordning i henhold til forordning (EU) 2019/881 for at påvise overensstemmelse med nærværende forordning. En ny kategori af kritiske produkter med digitale elementer kan tilføjes til disse kategorier, hvis der er en kritisk afhængighed af dem hos væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555, eller, hvis dette, såfremt de påvirkes af hændelser, eller når de indeholder udnyttede sårbarheder, kan føre til forstyrrelser af kritiske forsyningskæder. Ved vurderingen af behovet for at tilføje eller fjerne kategorier af kritiske produkter med digitale elementer ved hjælp af en delegeret retsakt bør Kommissionen kunne tage hensyn til, om medlemsstaterne på nationalt plan har identificeret produkter med digitale elementer, der har en kritisk rolle for modstandsdygtigheden af de væsentlige enheder, der er omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555, og som i stigende grad udsættes for cyberangreb i forsyningskæden med potentielle alvorlige forstyrrende virkninger. Endvidere bør Kommissionen kunne tage hensyn til resultaterne af koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan, der foretages i overensstemmelse med artikel 22 i direktiv (EU) 2022/2555.

(49) Kommissionen bør sikre, at en bred vifte af relevante interessenter høres på en struktureret og regelmæssig måde, når der udarbejdes foranstaltninger til gennemførelse af denne forordning. Dette bør navnlig være tilfældet, hvor Kommissionen vurderer behovet for potentielle ajourføringer af listerne over kategorier af vigtige eller kritiske produkter med digitale elementer, hvor relevante fabrikanter bør høres og deres synspunkter tages i betragtning med henblik på at analysere cybersikkerhedsrisiciene samt balancen mellem omkostninger og fordele ved at udpege sådanne kategorier af produkter som vigtige eller kritiske.

(50) Denne forordning har en målrettet tilgang til cybersikkerhedsrisici. Produkter med digitale elementer kan imidlertid indebære andre sikkerhedsrisici, som ikke altid vedrører cybersikkerhed, men som kan være en konsekvens af et sikkerhedsbrud. Disse risici bør fortsat reguleres ved anden relevant EU-harmoniseringslovgivning end denne forordning. Hvis ingen anden EU-harmoniseringslovgivning end denne forordning finder anvendelse, bør de være omfattet af Europa-Parlamentets og Rådets forordning (EU) 2023/988 ([21]). Uanset artikel 2, stk. 1, tredje afsnit, litra b), i forordning (EU) 2023/988 bør kapitel III, afdeling 1, kapitel V og VII og kapitel IX-XI i forordning (EU) 2023/988 i lyset af nærværende forordnings målrettede karakter derfor finde anvendelse på produkter med digitale elementer for så vidt angår sikkerhedsrisici, der ikke er omfattet af nærværende forordning, hvis disse produkter ikke er omfattet af specifikke krav i anden EU-harmoniseringslovgivning end nærværende forordning i den i artikel 3, nr. 27), i forordning (EU) 2023/988 anvendte betydning.

(51) Produkter med digitale elementer, der er klassificeret som højrisiko-AI-systemer i henhold til artikel 6 i Europa-Parlamentets og Rådets forordning (EU) 2024/1689 ([22]), og som er omfattet af nærværende forordnings anvendelsesområde, bør opfylde de væsentlige cybersikkerhedskrav, der er fastsat i nærværende forordning. Hvor disse højrisiko-AI-systemer opfylder de væsentlige cybersikkerhedskrav i nærværende forordning, bør de anses for at opfylde cybersikkerhedskravene i artikel 15 i forordning (EU) 2024/1689, for så vidt som disse krav er omfattet af EU-overensstemmelseserklæringen eller dele heraf udstedt i henhold til nærværende forordning. Med henblik herpå bør vurderingen af de cybersikkerhedsrisici, der er forbundet med et produkt med digitale elementer, der er klassificeret som et højrisiko-AI-system i henhold til forordning (EU) 2024/1689, som skal tages i betragtning i forbindelse med planlægnings-, design-, udviklings-, produktions-, leverings- og vedligeholdelsesfaserne for et sådant produkt som krævet i nærværende forordning, tage hensyn til risici for et AI-systems cyberrobusthed for så vidt angår uautoriserede tredjeparters forsøg på at ændre dets anvendelse, adfærd eller ydeevne, herunder

([21]) Europa-Parlamentets og Rådets forordning (EU) 2023/988 af 10. maj 2023 om produktsikkerhed i almindelighed, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 og Europa-Parlamentets og Rådets direktiv (EU) 2020/1828 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2001/95/EF og Rådets direktiv 87/357/EØF (EUT L 135 af 23.5.2023, s. 1).

([22]) Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

AI-specifikke sårbarheder såsom dataforgiftning eller fjendtlige angreb, samt, alt efter hvad der er relevant, risici for de grundlæggende rettigheder, i overensstemmelse med forordning (EU) 2024/1689. For så vidt angår overensstemmelsesvurderingsprocedurerne vedrørende de væsentlige cybersikkerhedskrav til et produkt med digitale elementer, der er omfattet af nærværende forordnings anvendelsesområde og klassificeret som et højrisiko-AI-system, bør artikel 43 i forordning (EU) 2024/1689 som hovedregel finde anvendelse i stedet for de relevante bestemmelser i nærværende forordning. Denne regel bør dog ikke resultere i en begrænsning af den nødvendige grad af sikkerhed for vigtige eller kritiske produkter med digitale elementer som omhandlet i nærværende forordning. Uanset denne regel bør højrisiko-AI-systemer, der er omfattet af anvendelsesområdet for forordning (EU) 2024/1689 og også betragtes som vigtige eller kritiske produkter med digitale elementer som omhandlet i nærværende forordning, og som overensstemmelsesvurderingsproceduren baseret på intern kontrol som omhandlet i bilag VI til forordning (EU) 2024/1689 finder anvendelse på, derfor være omfattet af procedurerne for overensstemmelsesvurdering i nærværende forordning for så vidt angår de væsentlige cybersikkerhedskrav i nærværende forordning. I sådan et tilfælde bør de relevante bestemmelser om overensstemmelsesvurdering på grundlag af intern kontrol, der er fastsat i bilag VI til forordning (EU) 2024/1689, finde anvendelse på alle andre aspekter, der er omfattet af nævnte forordning.

(52) For at forbedre sikkerheden af produkter med digitale elementer, der bringes i omsætning i det indre marked, er det nødvendigt at fastsætte væsentlige cybersikkerhedskrav, der gælder for sådanne produkter. Disse væsentlige cybersikkerhedskrav bør ikke berøre de koordinere sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan, der fremgår af artikel 22 i direktiv (EU) 2022/2555, hvor der tages hensyn til både tekniske og, hvor det er relevant, ikketekniske risikofaktorer såsom et tredjelands utilbørlige indflydelse på leverandører. De bør desuden ikke berøre medlemsstaternes beføjelser til at fastsætte yderligere krav, der tager hensyn til ikketekniske faktorer med henblik på at sikre et højt niveau af modstandsdygtighed, herunder dem, der er defineret i Kommissionens henstilling (EU) 2019/534 ([23]), i den EU-koordinerede risikovurdering af cybersikkerheden af 5G-net og i EU-værktøjskassen til 5G-cybersikkerhed, som samarbejdsgruppen, der er nedsat i medfør af artikel 14 i direktiv (EU) 2022/2555, er nået til enighed om.

(53) Fabrikanter af produkter, der er omfattet af anvendelsesområdet for Europa-Parlamentets og Rådets forordning (EU) 2023/1230 ([24]), der også er produkter med digitale elementer som defineret i nærværende forordning, bør opfylde både de væsentlige cybersikkerhedskrav, der er fastsat i nærværende forordning, og de væsentlige sundheds- og sikkerhedskrav, der er fastsat i forordning (EU) 2023/1230. De væsentlige cybersikkerhedskrav, der er fastsat i nærværende forordning, og visse væsentlige krav, der er fastsat i forordning (EU) 2023/1230, kan være rettet mod ensartede cybersikkerhedsrisici. Derfor kan overholdelsen af de væsentlige cybersikkerhedskrav, der er fastsat i nærværende forordning, lette overholdelsen af de væsentlige krav, der også omfatter visse cybersikkerhedsrisici som fastsat i forordning (EU) 2023/1230, og navnlig kravene vedrørende beskyttelse mod korruption og kontrolsystemers sikkerhed og pålidelighed, der er fastsat i afsnit 1.1.9 og 1.2.1 i bilag III til nævnte forordning. Sådanne synergier skal påvises af fabrikanten, f.eks. ved, hvor sådanne foreligger, at anvende harmoniserede standarder eller andre tekniske specifikationer, der dækker relevante væsentlige cybersikkerhedskrav, efter en risikovurdering, der dækker disse cybersikkerhedsrisici. Fabrikanten bør også følge de gældende overensstemmelsesvurderingsprocedurer, der er fastsat i nærværende forordning og i forordning (EU) 2023/1230. Kommissionen og de europæiske standardiseringsorganisationer bør i det forberedende arbejde til støtte for gennemførelsen af nærværende forordning og forordning (EU) 2023/1230 og de tilknyttede standardiseringsprocesser fremme konsistens i, hvordan cybersikkerhedsrisiciene skal vurderes, og hvordan disse risici skal dækkes af harmoniserede standarder med hensyn til de relevante væsentlige krav. Kommissionen og de europæiske standardiseringsorganisationer bør navnlig tage hensyn til nærværende forordning i forbindelse med udarbejdelsen og udviklingen af harmoniserede standarder til at lette gennemførelsen af forordning (EU) 2023/1230 for så vidt angår navnlig cybersikkerhedsaspekter i forbindelse med beskyttelse mod korruption og kontrolsystemers sikkerhed og pålidelighed, der er fastsat i afsnit 1.1.9 og 1.2.1 i bilag III til nævnte forordning. Kommissionen bør yde vejledning for at støtte fabrikanter, der er omfattet af nærværende forordning, og som også er omfattet af forordning (EU) 2023/1230, navnlig for at lette påvisningen af overensstemmelse med de relevante væsentlige krav i nærværende forordning og i forordning (EU) 2023/1230.

(54) For at sikre, at produkter med digitale elementer er sikre både på det tidspunkt, hvor de bringes i omsætning, og i den periode, hvor produktet med digitale elementer forventes at være i brug, er det nødvendigt at fastsætte væsentlige cybersikkerhedskrav til sårbarhedshåndtering og væsentlige cybersikkerhedskrav vedrørende egenskaberne ved produkter med digitale elementer. Mens fabrikanterne bør opfylde alle væsentlige cybersikkerhedskrav

([23]) Kommissionens henstilling (EU) 2019/534 af 26. marts 2019 Cybersikkerheden i forbindelse med 5G-net (EUT L 88 af 29.3.2019, s. 42).

([24]) Europa-Parlamentets og Rådets forordning (EU) 2023/1230 af 14. juni 2023 om maskiner og om ophævelse af Europa-Parlamentets og Rådets direktiv 2006/42/EF og af Rådets direktiv 73/361/EØF (EUT L 165 af 29.6.2023, s. 1).

vedrørende håndtering af sårbarheder i hele supportperioden, bør de afgøre, hvilke andre væsentlige cybersikkerhedskrav vedrørende produktegenskaberne der er relevante for den pågældende produkttype med digitale elementer. Med henblik herpå bør fabrikanterne foretage en vurdering af de cybersikkerhedsrisici, der er forbundet med et produkt med digitale elementer, for at identificere relevante risici og relevante væsentlige cybersikkerhedskrav og for at stille deres produkter med digitale elementer til rådighed uden kendte sårbarheder, der kan udnyttes, og som kan have en indvirkning på de pågældende produkters sikkerhed, og for på passende vis at anvende relevante harmoniserede standarder, fælles specifikationer eller europæiske eller internationale standarder.

(55) Hvor visse væsentlige cybersikkerhedskrav ikke finder anvendelse på et produkt med digitale elementer, bør fabrikanten medtage en klar begrundelse i cybersikkerhedsrisikovurderingen, som er inkluderet i den tekniske dokumentation. Dette kunne være tilfældet, hvis et væsentligt cybersikkerhedskrav er uforeneligt med karakteren af et produkt med digitale elementer. For eksempel kan det tilsigtede formål med et produkt med digitale elementer kræve, at fabrikanten følger bredt anerkendte interoperabilitetsstandarder, selv om dets sikkerhedsfunktioner ikke længere anses for at være på det aktuelle tekniske niveau. På samme måde kræver anden EU-ret, at fabrikanterne anvender specifikke interoperabilitetskrav. Hvor et væsentligt cybersikkerhedskrav ikke finder anvendelse på et produkt med digitale elementer, men fabrikanten har identificeret cybersikkerhedsrisici i forbindelse med dette væsentlige cybersikkerhedskrav, bør fabrikanten træffe foranstaltninger til at imødegå disse risici på anden vis, f.eks. ved at begrænse produktets tilsigtede formål til pålidelige miljøer eller ved at informere brugerne om de pågældende risici.

(56) En af de vigtigste foranstaltninger, som brugerne skal træffe for at beskytte deres produkter med digitale elementer mod cyberangreb, er at installere de seneste tilgængelige sikkerhedsopdateringer så hurtigt som muligt. Fabrikanterne bør derfor udforme deres produkter og indføre processer for at sikre, at produkter med digitale elementer omfatter funktioner, der muliggør automatisk anmeldelse, distribution, download og installation af sikkerhedsopdateringer, navnlig i forbindelse med forbrugerprodukter. De bør også give mulighed for at godkende download og installation af sikkerhedsopdateringer som et sidste skridt. Brugerne bør bevare muligheden for at deaktivere automatiske opdateringer med en klar og brugervenlig mekanisme understøttet af klare instrukser i, hvordan brugerne kan fravælge dem. Kravene vedrørende automatiske opdateringer som fastsat i et bilag til denne forordning finder ikke anvendelse på produkter med digitale elementer, der primært er beregnet til at blive integreret som komponenter i andre produkter. De finder heller ikke anvendelse på produkter med digitale elementer, for hvilke brugerne ikke med rimelighed kan forvente automatiske opdateringer, herunder produkter med digitale elementer, der er beregnet til at blive anvendt i professionelle IKT-netværk, og navnlig i kritiske og industrielle miljøer, hvor en automatisk opdatering kunne forårsage forstyrrelser i driften. Uanset om et produkt med digitale elementer er designet til at modtage automatiske opdateringer eller ej, bør dets fabrikant informere brugerne om sårbarheder og straks stille sikkerhedsopdateringer til rådighed. Hvis et produkt med digitale elementer har en brugergrænseflade eller lignende tekniske midler, der muliggør direkte interaktion med dets brugere, bør fabrikanten gøre brug af sådanne funktioner til at informere brugerne om, at deres produkt med digitale elementer har nået udgangen af supportperioden. Underretninger bør begrænses til, hvad der er nødvendigt for at sikre en effektiv modtagelse af disse oplysninger, og bør ikke have en negativ indvirkning på brugeroplevelsen af produktet med digitale elementer.

(57) For at forbedre gennemsigtigheden af sårbarhedshåndteringsprocesser og for at sikre, at brugerne ikke er forpligtet til at installere nye funktionalitetsopdateringer udelukkende med henblik på at modtage de seneste sikkerhedsopdateringer, bør fabrikanterne, hvor det er teknisk muligt, sikre, at nye sikkerhedsopdateringer leveres adskilt fra funktionalitetsopdateringer.

(58) I den fælles meddelelse fra Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik af 20. juni 2023 med titlen »En europæisk økonomisk sikkerhedsstrategi« fastslås det, at Unionen er nødt til at maksimere fordelene ved sin økonomiske åbenhed og samtidig minimere risiciene fra økonomisk afhængighed af højrisikoleverandører gennem en fælles strategisk ramme for Unionens økonomiske sikkerhed. Afhængighed af højrisikoleverandører af kritiske produkter med digitale elementer udgør en strategisk risiko, som bør håndteres på EU-plan, navnlig hvor de kritiske produkter med digitale elementer er beregnet til brug af væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555. Sådanne risici kan være knyttet til, men er ikke begrænset til, den jurisdiktion, der gælder for fabrikanten, egenskaberne ved ejerskabsforholdene i fabrikantens virksomhed og kontrolrelationerne med en regering i et tredjeland, hvor den er etableret, navnlig hvor et tredjeland er involveret i økonomisk spionage eller uforsvarlig statslig adfærd, og dets lovgivning tillader vilkårlig adgang til enhver form for virksomhedsaktiviteter eller -data, herunder kommercielt følsomme data, og kan pålægge forpligtelser til efterretningsformål uden demokratiske kontrolforanstaltninger, tilsynsmekanismer, en retfærdig procedure eller retten til at klage til en uafhængig domstol. Ved fastlæggelsen af væsentligheden af en cybersikkerhedsrisiko i den i denne forordning anvendte betydning bør Kommissionen og markedsovervågningsmyndighederne i overensstemmelse med deres ansvar som fastsat i denne forordning også tage hensyn til

ikketekniske risikofaktorer, navnlig dem, der er fastsat som følge af koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan foretaget i overensstemmelse med artikel 22 i direktiv (EU) 2022/2555.

(59) Med henblik på at garantere sikkerheden af produkter med digitale elementer, efter at de er bragt i omsætning, bør fabrikanterne fastsætte supportperioder, som bør afspejle den periode, hvor produktet med digitale elementer forventes at være i brug. Ved fastsættelsen af en supportperiode bør en fabrikant navnlig tage hensyn til rimelige brugerforventninger, produktets art samt relevant EU-ret, der fastsætter levetiden for produkter med digitale elementer. Fabrikanter bør også kunne tage hensyn til andre relevante faktorer. Kriterierne bør anvendes på en måde, der sikrer proportionalitet ved fastsættelsen af supportperioden. På anmodning bør en fabrikant give markedsovervågningsmyndighederne de oplysninger, der blev taget i betragtning med henblik på at fastlægge supportperioden for et produkt med digitale elementer.

(60) Den supportperiode, hvor fabrikanten sikrer effektiv håndtering af sårbarheder, bør være på mindst fem år, medmindre levetiden for produktet med digitale elementer er mindre end fem år, i hvilket tilfælde fabrikanten bør sikre sårbarhedshåndteringen i den pågældende levetid. Hvis den periode, hvor produktet med digitale elementer med rimelighed forventes at være i brug, er længere end fem år, som det ofte er tilfældet for hardwarekomponenter såsom motherboards eller mikroprocessorer, netværksenheder såsom routere, modemmer eller switches samt software såsom operativsystemer eller videoredigeringsværktøjer, bør fabrikanterne i overensstemmelse hermed sikre længere supportperioder. Navnlig produkter med digitale elementer, der er beregnet til anvendelse i industrielle miljøer, såsom industrielle kontrolsystemer, anvendes ofte i betydeligt længere tid. En fabrikant bør kun kunne definere en supportperiode på mindre end fem år, hvis dette er begrundet i arten af det pågældende produkt med digitale elementer, og hvis produktet forventes at være i brug i mindre end fem år, i hvilket tilfælde supportperioden bør svare til den forventede anvendelsestid. F.eks. kunne levetiden for en kontaktopsporingsapplikation, der er beregnet til brug under en pandemi, begrænses til pandemiens varighed. Desuden kan visse softwareapplikationer i sagens natur kun stilles til rådighed på grundlag af en abonnementsmodel, navnlig hvis applikationen bliver utilgængelig for brugeren og derfor ikke længere er i brug, når abonnementet udløber.

(61) Når produkter med digitale elementer når udgangen af deres supportperioder, bør fabrikanterne for at sikre, at sårbarheder kan håndteres efter udløbet af supportperioden, overveje at frigive kildekoden for sådanne produkter med digitale elementer enten til andre virksomheder, der forpligter sig til at udvide leveringen af sårbarhedshåndteringstjenester, eller til offentligheden. Hvis fabrikanterne frigiver kildekoden til andre virksomheder, bør de være i stand til at beskytte ejerskabet af produktet med digitale elementer og forhindre udbredelse af kildekoden til offentligheden, f.eks. gennem kontraktlige ordninger.

(62) For at sikre, at fabrikanter i hele Unionen fastsætter ensartede supportperioder for sammenlignelige produkter med digitale elementer, bør ADCO offentliggøre statistikker over de gennemsnitlige supportperioder, som fabrikanterne har fastsat for kategorier af produkter med digitale elementer, og udstede retningslinjer med angivelse af passende supportperioder for sådanne kategorier. Med henblik på at sikre en harmoniseret tilgang i hele det indre marked bør Kommissionen derudover kunne vedtage delegerede retsakter for at fastsætte minimumssupportperioder for specifikke produktkategorier, hvor data fra markedsovervågningsmyndighederne tyder på, at de supportperioder, som fabrikanterne fastsætter, enten systematisk ikke er i overensstemmelse med kriterierne for fastsættelse af supportperioder som fastsat i denne forordning, eller at fabrikanter i forskellige medlemsstater uberettiget fastsætter forskellige supportperioder.

(63) Fabrikanter bør oprette et centralt kontaktpunkt, der gør det muligt for brugere let at kommunikere med dem, herunder med henblik på at indberette og modtage oplysninger om sårbarhederne i produktet med et digitalt element. De bør gøre det centrale kontaktpunkt let tilgængeligt for brugerne og klart angive, hvornår det er tilgængeligt, og holde disse oplysninger ajour. Hvor fabrikanter vælger at tilbyde automatiserede værktøjer, f.eks. chatbokse, bør de også tilbyde et telefonnummer eller andre digitale kontaktmidler såsom en e-mailadresse eller en kontaktformular. Det centrale kontaktpunkt bør ikke udelukkende benytte automatiserede værktøjer.

(64) Fabrikanter bør gøre deres produkter med digitale elementer tilgængelige på markedet med en sikker konfiguration som standard og gratis levere sikkerhedsopdateringer til brugerne. Fabrikanter bør kun kunne afvige fra de væsentlige cybersikkerhedskrav i forbindelse med skræddersyede produkter, der er udformet til et bestemt formål for en bestemt erhvervsbruger, og hvor både fabrikanten og brugeren udtrykkeligt har aftalt et andet sæt kontraktvilkår.

(65) Fabrikanterne bør via den fælles indberetningsplatform samtidig underrette både den enhed, der håndterer IT-sikkerhedshændelser (CSIRT), der er udpeget som koordinator, og ENISA om aktivt udnyttede sårbarheder i produkter med digitale elementer samt alvorlige hændelser, der har indvirkning på disse produkters sikkerhed. Underretningerne bør indgives via adgangspunkter for elektronisk underretning i en CSIRT, der er udpeget som koordinator, og bør samtidig være tilgængelige for ENISA.

(66) Fabrikanterne bør underrette om aktivt udnyttede sårbarheder for at sikre, at de CSIRT'er, der er udpeget som koordinatorer, og ENISA har et passende overblik over sådanne sårbarheder og får de oplysninger, der er nødvendige for, at de kan udføre deres opgaver som fastsat i direktiv (EU) 2022/2555, og øge det overordnede cybersikkerhedsniveau for væsentlige og vigtige enheder som omhandlet i nævnte direktivs artikel 3, samt for at sikre, at markedsovervågningsmyndighederne fungerer effektivt. Da de fleste produkter med digitale elementer markedsføres i hele det indre marked, bør enhver udnyttet sårbarhed i et produkt med digitale elementer anses som værende en trussel mod det indre markeds funktion. ENISA bør i samarbejde med fabrikanterne offentliggøre afhjulpne sårbarheder i den europæiske sårbarhedsdatabase, der er oprettet i henhold til artikel 12, stk. 2, i direktiv (EU) 2022/2555. Den europæiske sårbarhedsdatabase vil hjælpe fabrikanterne til at opdage kendte sårbarheder, der kan udnyttes, i deres produkter, med henblik på at sørge for, at der bringes sikre produkter i omsætning.

(67) Fabrikanterne bør også give underretning om enhver alvorlig hændelse, der indvirker på sikkerheden af produktet med digitale elementer til den CSIRT, der er udpeget som koordinator, og til ENISA. For at sikre, at brugerne kan reagere hurtigt på alvorlige hændelser, der har indvirkning på sikkerheden af deres produkter med digitale elementer, bør fabrikanterne også underrette deres brugere om en sådan hændelse og, i givet fald, om eventuelle korrigerende foranstaltninger, som brugerne kan træffe for at afbøde virkningen af hændelsen, f.eks. ved at offentliggøre relevante oplysninger på deres websteder eller, hvor fabrikanten har mulighed for at kontakte brugerne og hvor cybersikkerhedsrisiciene berettiger dertil, ved at kontakte brugerne direkte.

(68) Aktivt udnyttede sårbarheder vedrører tilfælde, hvor en fabrikant konstaterer, at et brud på sikkerheden, der påvirker dens brugere eller andre fysiske eller juridiske personer, skyldes, at en ondsindet aktør udnytter en fejl i et af produkterne med digitale elementer, som fabrikanten har gjort tilgængelige på markedet. Eksempler på sådanne sårbarheder kan være svagheder i et produkts identifikations- og autentifikationsfunktioner. Sårbarheder, der opdages uden ondsindede hensigter, men med det formål i god tro at afprøve, undersøge, korrigere eller offentliggøre med henblik på at fremme systemejerens og dennes brugeres sikkerhed, bør ikke være omfattet af obligatoriske underretninger. Alvorlige hændelser, der har en indvirkning på sikkerheden af produktet med digitale elementer, vedrører derimod situationer, hvor en cybersikkerhedshændelse påvirker fabrikantens udviklings-, produktions- eller vedligeholdelsesprocesser på en sådan måde, at det kan resultere i en øget cybersikkerhedsrisiko for brugere eller andre personer. En sådan alvorlig hændelse kan omfatte en situation, hvor en angriber på vellykket vis har indført ondsindet kode i den frigivelseskanal, hvorigennem fabrikanten frigiver sikkerhedsopdateringer til brugere.

(69) For at sikre, at underretninger hurtigt kan formidles til alle relevante CSIRT'er, der er udpeget som koordinatorer, og for at gøre det muligt for fabrikanterne at sende en enkelt underretning på hvert trin i underretningsproceduren, bør ENISA oprette en fælles indberetningsplatform med nationale elektroniske adgangspunkter for underretning. Den fælles indberetningsplatforms daglige drift bør forvaltes og opretholdes af ENISA. De CSIRT'er, der er udpeget som koordinatorer, bør informere deres respektive markedsovervågningsmyndigheder om anmeldte sårbarheder eller hændelser. Den fælles indberetningsplatform bør udformes på en sådan måde, at den sikrer fortroligheden af underretninger, navnlig for så vidt angår sårbarheder, for hvilke en sikkerhedsopdatering endnu ikke er tilgængelig. ENISA bør desuden indføre procedurer for behandling af oplysninger på en sikker og fortrolig måde. På grundlag af de oplysninger, som ENISA indsamler, bør det hvert andet år udarbejde en teknisk rapport om nye tendenser med hensyn til cybersikkerhedsrisici forbundet med produkter med digitale elementer og forelægge den for den samarbejdsgruppe, der er oprettet i henhold til artikel 14 i direktiv (EU) 2022/2555.

(70) Under ekstraordinære omstændigheder og navnlig efter anmodning fra fabrikanten bør den CSIRT, der er udpeget som koordinator, og som indledningsvist modtager en underretning, kunne beslutte at udsætte formidlingen heraf til de andre relevante CSIRT'er, der er udpeget som koordinatorer, via den fælles indberetningsplatform, hvis dette kan berettiges på grundlag af cybersikkerhedsrelaterede årsager og i en periode, der er strengt nødvendig. Den CSIRT, der er udpeget som koordinator, bør omgående underrette ENISA om afgørelsen om udsættelse og om årsagerne hertil samt om, hvornår den agter at videreformidle underretningen. Kommissionen bør gennem en delegeret retsakt udarbejde specifikationer for vilkår og betingelser for, hvornår de cybersikkerhedsrelaterede årsager kunne finde anvendelse, og bør samarbejde med CSIRT-netværket, der er oprettet i henhold til artikel 15 i direktiv (EU) 2022/2555, og ENISA om udarbejdelsen af udkastet til delegeret retsakt. Eksempler på cybersikkerhedsrelaterede årsager omfatter en igangværende procedure for koordineret offentliggørelse af sårbarheder eller situationer, hvor en fabrikant forventes at træffe en afbødende foranstaltning i løbet af kort tid, og cybersikkerhedsrisiciene ved en øjeblikkelig formidling via den fælles indberetningsplatform opvejer fordelene herved. Hvis den CSIRT, der er

udpeget som koordinator, anmoder herom, bør ENISA kunne støtte den pågældende CSIRT med henvisning til de cybersikkerhedsrelaterede årsager i forbindelse med udsættelsen af formidlingen af underretningen på grundlag af de oplysninger, som ENISA har modtaget fra den pågældende CSIRT om afgørelsen om at tilbageholde en underretning af disse cybersikkerhedsrelaterede årsager. Endvidere bør ENISA under særlig ekstraordinære omstændigheder ikke modtage alle detaljerne vedrørende en aktivt udnyttet sårbarhed samtidig. Dette vil være tilfældet, når fabrikanten i sin underretning anfører, at den anmeldte sårbarhed er blevet udnyttet aktivt af en ondsindet aktør, og at den ifølge de foreliggende oplysninger ikke er blevet udnyttet i nogen anden medlemsstat end den, hvor den CSIRT, der er udpeget som koordinator, og til hvem fabrikanten har anmeldt sårbarheden, befinder sig, når en øjeblikkelig videreformidling af den anmeldte sårbarhed sandsynligvis vil føre til levering af oplysninger, hvis offentliggørelse vil stride mod den pågældende medlemsstats væsentlige interesser, eller når den anmeldte sårbarhed udgør en overhængende høj cybersikkerhedsrisiko som følge af videreformidlingen. I sådanne tilfælde vil ENISA kun få samtidig adgang til oplysningerne om, at fabrikanten har foretaget en underretning, generelle oplysninger om det pågældende produkt med digitale elementer, oplysninger om den generelle karakter af udnyttelsen og oplysninger om, at fabrikanten har gjort disse sikkerhedsgrunde gældende, og at underretningens fulde indhold derfor tilbageholdes. Den fuldstændige underretning bør derefter stilles til rådighed for ENISA og andre relevante CSIRT'er, der er udpeget som koordinatorer, når den CSIRT, der er udpeget som koordinator, og som indledningsvist modtog underretningen, finder, at disse sikkerhedsgrunde, der udgør særlig ekstraordinære omstændigheder som fastsat i denne forordning, ikke længere foreligger. Hvor ENISA på grundlag af de tilgængelige oplysninger finder, at der er tale om en systemisk risiko, der indvirker på sikkerheden i det indre marked, bør ENISA anbefale den modtagende CSIRT at formidle den fuldstændige underretning til de andre CSIRT'er, der er udpeget som koordinatorer, og til ENISA selv.

(71) Når fabrikanter underretter om en aktivt udnyttet sårbarhed eller en alvorlig hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer, bør de angive, hvor følsomme de anser de indberettede oplysninger for at være. Den CSIRT, der er udpeget som den koordinator, der oprindeligt modtager underretningen, bør tage hensyn til disse oplysninger, når den vurderer, om underretningen giver anledning til ekstraordinære omstændigheder, der berettiger en udsættelse af formidlingen af underretningen til de andre relevante CSIRT'er, der er udpeget som koordinatorer, på grundlag af begrundede cybersikkerhedsrelaterede årsager. Den bør også tage hensyn til disse oplysninger, når den vurderer, om underretningen om en aktivt udnyttet sårbarhed giver anledning til særlige ekstraordinære omstændigheder, der berettiger, at den fuldstændige underretning ikke samtidig stilles til rådighed for ENISA. Endelig bør CSIRT'er, der er udpeget som koordinatorer, kunne tage hensyn til disse oplysninger, når de træffer passende foranstaltninger til at afbøde de risici, der følger af sådanne sårbarheder og hændelser.

(72) For at forenkle indberetningen af de oplysninger, der kræves i henhold til denne forordning, i betragtning af andre supplerende indberetningskrav, der er fastsat i EU-retten, såsom forordning (EU) 2016/679, Europa-Parlamentets og Rådets forordning (EU) 2022/2554 ([25]), Europa-Parlamentets og Rådets direktiv 2002/58/EF ([26]) og direktiv (EU) 2022/2555, samt for at mindske den administrative byrde for enhederne, opfordres medlemsstaterne til at overveje at oprette centrale indgangspunkter på nationalt plan for sådanne indberetningskrav. Anvendelsen af sådanne nationale fælles indgangspunkter til indberetning af sikkerhedshændelser i henhold til forordning (EU) 2016/679 og direktiv 2002/58/EF bør ikke berøre anvendelsen af bestemmelserne i forordning (EU) 2016/679 og direktiv 2002/58/EF, navnlig bestemmelserne vedrørende uafhængigheden af de deri omhandlede myndigheder. Ved oprettelsen af den fælles indberetningsplatform, der er omhandlet i nærværende forordning, bør ENISA tage hensyn til muligheden for, at de nationale adgangspunkter for elektronisk underretning, der er omhandlet i nærværende forordning, integreres i nationale centrale indgangspunkter, som også kan integrere andre underretninger, der kræves i henhold til EU-retten.

(73) Ved oprettelsen af den fælles indberetningsplatform, der er omhandlet i denne forordning, og for at drage fordel af tidligere erfaringer bør ENISA konsultere andre EU-institutioner eller -agenturer, der forvalter platforme eller databaser, der er underlagt strenge sikkerhedskrav, såsom Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA). ENISA bør også analysere mulig komplementaritet med den europæiske sårbarhedsdatabase, som er oprettet i henhold til artikel 12, stk. 2, i direktiv (EU) 2022/2555.

(74) Fabrikanter og andre fysiske og juridiske personer bør på frivillig basis kunne underrette en CSIRT, der er udpeget som koordinator, eller ENISA om enhver sårbarhed i et produkt med digitale elementer, cybertrusler, der kunne

([25]) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1).

([26]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

påvirke risikoprofilen for et produkt med digitale elementer, enhver hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer, samt nærvedhændelser, der kunne have resulteret i en sådan hændelse.

(75) Medlemsstaterne bør så vidt muligt tackle de udfordringer, som sårbarhedsforskere står over for, herunder deres potentielle strafansvar, i overensstemmelse med national ret. Eftersom fysiske og juridiske personer, der forsker i sårbarheder, i nogle medlemsstater vil kunne blive udsat for strafferetligt og civilretligt ansvar, opfordres medlemsstaterne til at vedtage retningslinjer for ikke-retsforfølgelse af informationssikkerhedsforskere og en fritagelse for civilretligt ansvar for deres aktiviteter.

(76) Fabrikanter af produkter med digitale elementer bør indføre koordinerede politikker for offentliggørelse af sårbarheder for at gøre det lettere for enkeltpersoner eller enheder at indberette sårbarheder, enten direkte til fabrikanten eller indirekte, og efter der er anmodning om at gøre dette anonymt, via CSIRT'er, der er udpeget som koordinatorer med henblik på koordineret offentliggørelse af sårbarheder i overensstemmelse med artikel 12, stk. 1, i direktiv (EU) 2022/2555. Fabrikanters politik for koordineret offentliggørelse af sårbarheder bør angive en struktureret proces, hvorigennem sårbarheder indberettes til en fabrikant på en måde, der gør det muligt for fabrikanten at diagnosticere sådanne sårbarheder, inden detaljerede sårbarhedsoplysninger videregives til tredjeparter eller offentligheden. Derudover bør fabrikanter også overveje at offentliggøre deres sikkerhedspolitikker i maskinlæsbart format. Da oplysninger om sårbarheder, der kan udnyttes i almindeligt anvendte produkter med digitale elementer, kan sælges til høje priser på det sorte marked, bør fabrikanter af sådanne produkter som led i deres koordinerede politikker for offentliggørelse af sårbarheder kunne anvende programmer, der tilskynder til indberetning af sårbarheder, ved at sikre, at enkeltpersoner eller enheder modtager anerkendelse og kompensation for deres indsats. Dette henviser til såkaldte »bug bounty-programmer«.

(77) For at lette sårbarhedsanalysen bør fabrikanterne identificere og dokumentere komponenter i produkter med digitale elementer, herunder ved at udarbejde en softwarekomponentliste. En softwarekomponentliste kan give fabrikanter, købere og brugere af software oplysninger, som øger deres forståelse af forsyningskæden, hvilket har mange fordele, navnlig at den hjælper fabrikanter og brugere med at spore kendte nyligt opståede sårbarheder og cybersikkerhedsrisici. Det er særlig vigtigt, at fabrikanterne sikrer, at deres produkter med digitale elementer ikke indeholder sårbare komponenter udviklet af tredjeparter. Fabrikanterne bør ikke være forpligtet til at offentliggøre softwarekomponentlisten.

(78) En virksomhed, der opererer online, kan inden for de nye, komplekse forretningsmodeller, der er knyttet til onlinesalg, levere en række forskellige tjenesteydelser. Afhængigt af arten af de tjenester, der leveres i forbindelse med et givet produkt med digitale elementer, kan den samme enhed falde ind under forskellige kategorier af forretningsmodeller eller kategorier af erhvervsdrivende. Hvis en enhed kun leverer onlineformidlingstjenester for et givet produkt med digitale elementer og blot er udbyder af en onlinemarkedsplads som defineret i artikel 3, nr. 14), i Europa-Parlamentets og Rådets forordning (EU) 2023/988, betragtes den ikke som en erhvervsdrivende som defineret i nærværende forordning. Hvor den samme enhed er en udbyder af en onlinemarkedsplads og også fungerer som en erhvervsdrivende som defineret i nærværende forordning i forbindelse med salg af produkter med digitale elementer, bør den være omfattet af de forpligtelser i nærværende forordning, der er fastsat for denne type af erhvervsdrivende. Hvis udbyderen af en onlinemarkedsplads f.eks. også håndterer distribution af et produkt med digitale elementer, vil den med hensyn til salget af dette produkt blive anses som værende en distributør. Tilsvarende vil den pågældende enhed, hvis den sælger sine egne mærkevarer med digitale elementer, betragtes som en fabrikant og vil dermed skulle opfylde de gældende krav til fabrikanter. Nogle enheder kan også betragtes som udbydere af distributionstjenester som defineret i artikel 3, nr. 11), i Europa-Parlamentets og Rådets forordning (EU) 2019/1020 ([27]), hvis de tilbyder sådanne tjenester. Sådanne forhold vil skulle vurderes fra sag til sag. I betragtning af den fremtrædende rolle, som onlinemarkedspladser spiller med hensyn til at muliggøre elektronisk handel, bør de bestræbe sig på at samarbejde med medlemsstaternes markedsovervågningsmyndigheder for at hjælpe med at sikre, at produkter med digitale elementer, der købes via onlinemarkedspladser, opfylder de cybersikkerhedskrav, der er fastsat i nærværende forordning.

(79) For at lette vurderingen af overensstemmelsen med kravene i denne forordning bør der være en formodning om overensstemmelse for produkter med digitale elementer, som er i overensstemmelse med harmoniserede standarder, der omsætter de væsentlige cybersikkerhedskrav i denne forordning til detaljerede tekniske specifikationer og er

([27]) Europa-Parlamentets og Rådets forordning (EU) 2019/1020 af 20. juni 2019 om markedsovervågning og produktoverensstemmelse og om ændring af direktiv 2004/42/EF og forordning (EF) nr. 765/2008 og (EU) nr. 305/2011 (EUT L 169 af 25.6.2019, s. 1).

vedtaget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 ([28]). Nævnte forordning fastsætter bestemmelser om en procedure for indsigelse mod harmoniserede standarder i tilfælde, hvor disse standarder ikke fuldt ud opfylder kravene i nærværende forordning. Standardiseringsprocessen bør sikre en afbalanceret repræsentation af interesser og effektiv deltagelse af interesserede parter fra civilsamfundet, herunder forbrugerorganisationer. Der bør også tages hensyn til internationale standarder, der er i overensstemmelse med det cybersikkerhedsniveau, der tilstræbes med de væsentlige cybersikkerhedskrav i nærværende forordning, for at lette udviklingen af harmoniserede standarder og gennemførelsen af nærværende forordning samt for at lette overholdelsen for virksomheder, navnlig mikrovirksomheder og små og mellemstore virksomheder og dem, der opererer globalt.

(80) Rettidig udvikling af harmoniserede standarder i overgangsperioden for anvendelsen af denne forordning og deres tilgængelighed inden anvendelsesdatoen for denne forordning vil være særlig vigtig for dens effektive gennemførelse. Dette er navnlig tilfældet for vigtige produkter med digitale elementer, som er omfattet af klasse I. Tilgængeligheden af harmoniserede standarder vil gøre det muligt for fabrikanter af sådanne produkter at udføre overensstemmelsesvurderingerne via proceduren for intern kontrol og kan derfor undgå flaskehalse og forsinkelser i overensstemmelsesvurderingsorganers aktiviteter.

(81) Ved forordning (EU) 2019/881 oprettes en frivillig europæisk ramme for cybersikkerhedscertificering af IKT-produkter, IKT-processer og IKT-tjenester. Europæiske cybersikkerhedscertificeringsordninger giver brugere en fælles tillidsramme, så de kan anvende produkter med digitale elementer, der er omfattet af nærværende forordning. Nærværende forordning bør følgelig skabe synergier med forordning (EU) 2019/881. For at lette vurderingen af overensstemmelsen med kravene i nærværende forordning formodes produkter med digitale elementer, der er certificeret, eller for hvilke der er udstedt en overensstemmelseserklæring i henhold til en europæisk cybersikkerhedsordning i henhold til forordning (EU) 2019/881, som Kommissionen har identificeret i en gennemførelsesretsakt, at være i overensstemmelse med de væsentlige cybersikkerhedskrav, der er fastsat i nærværende forordning, såfremt den europæiske cybersikkerhedsattest eller overensstemmelseserklæring eller dele heraf dækker disse krav. Behovet for nye europæiske cybersikkerhedscertificeringsordninger for produkter med digitale elementer bør vurderes i lyset af nærværende forordning, herunder ved udarbejdelse af Unionens rullende arbejdsprogram i overensstemmelse med forordning (EU) 2019/881. Hvis der er behov for en ny ordning, der omfatter produkter med digitale elementer, herunder for at lette overholdelsen af nærværende forordning, kan Kommissionen anmode ENISA om at udarbejde forslag til ordninger i overensstemmelse med artikel 48 i forordning (EU) 2019/881. I sådanne fremtidige europæiske cybersikkerhedscertificeringsordninger, der dækker produkter med digitale elementer, bør der tages hensyn til de væsentlige cybersikkerhedskrav og procedurerne for overensstemmelsesvurderinger som fastsat i nærværende forordning, og de bør lette overholdelsen af nærværende forordning. For europæiske cybersikkerhedscertificeringsordninger, der træder i kraft inden nærværende forordnings ikrafttræden, kan der være behov for yderligere specifikationer af detaljerede aspekter af, hvordan en formodning om overensstemmelse kan finde anvendelse. Kommissionen bør ved hjælp af delegerede retsakter tillægges beføjelser til at præcisere de betingelser, hvorunder de europæiske cybersikkerhedscertificeringsordninger kan anvendes til at påvise overensstemmelse med de væsentlige cybersikkerhedskrav i nærværende forordning. For at undgå unødige administrative byrder bør der derudover ikke være en forpligtelse for fabrikanter til at foretage en tredjepartsoverensstemmelsesvurdering vedrørende tilsvarende krav som omhandlet i nærværende forordning, hvor en europæisk cybersikkerhedsattest er udstedt i henhold til sådanne europæiske cybersikkerhedscertificeringsordninger på et tillidsniveau, der som minimum er »betydeligt«.

(82) Ved ikrafttræden af gennemførelsesforordning (EU) 2024/482, der vedrører produkter, der er omfattet af nærværende forordnings anvendelsesområde, såsom hardwaresikkerhedsmoduler og mikroprocessorer, bør Kommissionen ved hjælp af en delegeret retsakt kunne præcisere, hvordan EUCC giver en formodning om overensstemmelse med de væsentlige cybersikkerhedskrav som fastsat i bilag I til nærværende forordning eller dele heraf. Derudover kan en sådan delegeret retsakt præcisere, hvordan en attest udstedt i henhold til EUCC fritager fabrikanterne fra forpligtelsen til at lade foretage en tredjepartsvurdering som krævet i henhold til nærværende forordning for tilsvarende krav.

(83) Den nuværende europæiske standardiseringsramme, som er baseret på principperne om en ny metode i medfør af Rådets resolution af 7. maj 1985 om en ny metode i forbindelse med teknisk harmonisering og standarder og på forordning (EU) nr. 1025/2012, udgør som standard rammen for udarbejdelse af standarder, der giver formodning om overensstemmelse med de relevante væsentlige cybersikkerhedskrav i nærværende forordning. Europæiske standarder bør være markedsdrevne, tage hensyn til den offentlige interesse samt de politiske mål, der klart fremgår af Kommissionens anmodning til en eller flere europæiske standardiseringsorganisationer om at udarbejde harmoniserede standarder inden for en fastsat frist, og være konsensusbaseret. I mangel af relevante henvisninger til harmoniserede standarder bør Kommissionen imidlertid kunne vedtage gennemførelsesretsakter, der fastsætter fælles

([28]) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).

specifikationer for de væsentlige cybersikkerhedskrav i nærværende forordning, forudsat at den i den forbindelse behørigt respekterer europæiske standardiseringsorganisationers rolle og funktioner, som en ekstraordinær nødløsning for at lette fabrikanters forpligtelse til at overholde disse væsentlige cybersikkerhedskrav, hvor standardiseringsprocessen blokeres, eller når der er forsinkelser i udarbejdelsen af passende harmoniserede standarder. Hvis en sådan forsinkelse skyldes den pågældende standards tekniske kompleksitet, bør Kommissionen tage dette i betragtning, inden den overvejer, om der skal udarbejdes fælles specifikationer.

(84) Med henblik på at udarbejde fælles specifikationer, der dækker de væsentlige cybersikkerhedskrav i denne forordning, på den mest effektive måde, bør Kommissionen inddrage relevante interessenter i processen.

(85) For så vidt angår offentliggørelsen af en henvisning til harmoniserede standarder i *Den Europæiske Unions Tidende* i overensstemmelse med forordning (EU) nr. 1025/2012 skal der ved »en rimelig tidsfrist« forstås en periode, i hvilken der forventes offentliggørelse i *Den Europæiske Unions Tidende* af referencen til standarden, berigtigelsen heraf eller ændringen heraf, og som ikke bør overstige ét år efter fristen for udarbejdelse af en europæisk standard, der er fastsat i overensstemmelse med forordning (EU) nr. 1025/2012.

(86) Med henblik på at gøre det lettere at vurdere overensstemmelsen med de væsentlige cybersikkerhedskrav i denne forordning bør der være en formodning om overensstemmelse for produkter med digitale elementer, som er i overensstemmelse med de fælles specifikationer, der er vedtaget af Kommissionen i henhold til denne forordning med henblik på detaljerede tekniske specifikationer af disse krav.

(87) Anvendelsen af harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger vedtaget i henhold til forordning (EU) 2019/881, der giver formodning om overensstemmelse med de væsentlige cybersikkerhedskrav, der gælder for produkter med digitale elementer, vil gøre det lettere for fabrikanterne at vurdere overensstemmelsen. Hvis fabrikanten vælger ikke at anvende sådanne midler for visse krav, skal denne i sin tekniske dokumentation angive, hvordan der ellers opnås overensstemmelse. Desuden vil anvendelsen af harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til forordning (EU) 2019/881, og som giver fabrikanterne overensstemmelsesformodning, gøre det lettere for markedsovervågningsmyndighederne at kontrollere overholdelse af kravene for så vidt angår produkter med digitale elementer. Fabrikanter af produkter med digitale elementer opfordres derfor til at anvende sådanne harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger.

(88) Fabrikanterne bør udfærdige en EU-overensstemmelseserklæring for at afgive de i henhold til denne forordning krævede oplysninger om overensstemmelsen af produkter med digitale elementer med de væsentlige cybersikkerhedskrav, der er fastsat i denne forordning og, i givet fald, med anden relevant EU-harmoniseringslovgivning, som produktet med digitale elementer er omfattet af. Fabrikanter kan også blive pålagt at udarbejde en EU-overensstemmelseserklæring i henhold til andre EU-retsakter. For at sikre effektiv adgang til oplysninger med henblik på markedsovervågning bør der udarbejdes en enkelt EU-overensstemmelseserklæring for overholdelse af alle relevante EU-retsakter. For at mindske de administrative byrder for de erhvervsdrivende bør det være muligt for denne enkelte EU-overensstemmelseserklæring at tage form af et dossier bestående af relevante individuelle overensstemmelseserklæringer.

(89) CE-mærkningen er et udtryk for et produkts overensstemmelse med kravene og det synlige resultat af en omfattende proces med overensstemmelsesvurdering i bred forstand. De generelle principper for CE-mærkning er fastsat i Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 ([29]). Der bør i nærværende forordning fastsættes bestemmelser vedrørende anbringelsen af CE-mærkningen på produkter med digitale elementer. CE-mærkningen bør være den eneste mærkning, der garanterer, at produkter med digitale elementer opfylder kravene i nærværende forordning.

(90) For at gøre det muligt for erhvervsdrivende at påvise overensstemmelse med de væsentlige cybersikkerhedskrav i denne forordning og gøre det muligt for markedsovervågningsmyndighederne at sikre, at produkter med digitale elementer, der gøres tilgængelige på markedet, opfylder disse krav, er det nødvendigt at fastsætte overensstemmelsesvurderingsprocedurer. Europa-Parlamentets og Rådets afgørelse 768/2008/EF ([30]) fastsætter moduler for

([29]) Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og om ophævelse af forordning (EØF) nr. 339/93 (EUT L 218 af 13.8.2008, s. 30).

([30]) Europa-Parlamentets og Rådets afgørelse nr. 768/2008/EF af 9. juli 2008 om fælles rammer for markedsføring af produkter og om ophævelse af Rådets afgørelse 93/465/EØF (EUT L 218 af 13.8.2008, s. 82).

overensstemmelsesvurderingsprocedurer alt efter risikoniveauet og det krævede sikkerhedsniveau. For at sikre kohærens mellem de forskellige sektorer og undgå ad hoc-varianter bør overensstemmelsesvurderingsprocedurer, der er tilstrækkelige til kontrol af, om produkter med digitale elementer er i overensstemmelse med de væsentlige cybersikkerhedskrav i denne forordning, være baseret på disse moduler. Overensstemmelsesvurderingsprocedurerne bør omfatte en undersøgelse og kontrol af både produkt- og procesrelaterede krav, der dækker hele livscyklussen for produkter med digitale elementer, herunder planlægning, design, udvikling eller produktion, afprøvning og vedligeholdelse af produktet med digitale elementer.

(91) Overensstemmelsesvurderingen af produkter med digitale elementer, der ikke er opført som væsentlige eller kritiske produkter med digitale elementer i denne forordning, kan foretages af fabrikanten på eget ansvar i henhold til den interne kontrolprocedure baseret på modul A i afgørelse 768/2008/EF i overensstemmelse med denne forordning. Dette gælder også i tilfælde, hvor en fabrikant vælger helt eller delvist ikke at anvende en gældende harmoniseret standard, en fælles specifikation eller den europæiske cybersikkerhedscertificeringsordning. Fabrikanten har fleksibilitet til at vælge en strengere overensstemmelsesvurderingsprocedure, der involverer en tredjepart. Under proceduren for intern kontrol sikrer og erklærer fabrikanten på eget eksklusive ansvar, at produktet med digitale elementer og fabrikantens processer opfylder de gældende væsentlige cybersikkerhedskrav i denne forordning. Hvis et vigtigt produkt med digitale elementer er omfattet af klasse I, kræves der yderligere sikkerhed for at påvise overensstemmelse med de væsentlige cybersikkerhedskrav i denne forordning. Fabrikanten bør anvende harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger vedtaget i henhold til forordning (EU) 2019/881, som Kommissionen har identificeret i en gennemførelsesretsakt, hvis fabrikanten ønsker at foretage overensstemmelsesvurderingen på eget ansvar (modul A). Hvis fabrikanten ikke anvender sådanne harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger, bør fabrikanten lade foretage en overensstemmelsesvurdering af tredjepart (baseret på modul B og C eller H). Under hensyntagen til fabrikanternes administrative byrde og det forhold, at cybersikkerhed spiller en vigtig rolle i design- og udviklingsfasen for materielle og immaterielle produkter med digitale elementer, er overensstemmelsesvurderingsprocedurer baseret på modul B og C eller modul H i afgørelse nr. 768/2008/EF blevet valgt som værende mest hensigtsmæssige til at vurdere overensstemmelsen af vigtige produkter med digitale elementer på en forholdsmæssig og effektiv måde. Den fabrikant, der foretager tredjepartsoverensstemmelsesvurderingen, kan vælge den procedure, der passer bedst til fabrikantens design- og produktionsproces. I betragtning af den endnu større cybersikkerhedsrisiko, der er forbundet med anvendelsen af vigtige produkter med digitale elementer, der er omfattet af klasse II, bør overensstemmelsesvurderingen altid involvere en tredjepart, selv når produktet helt eller delvist overholder harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger. Fabrikanter af vigtige produkter med digitale elementer, der kan betegnes som gratis open source-software, bør kunne følge den interne kontrolprocedure baseret på modul A, forudsat at de stiller den tekniske dokumentation til rådighed for offentligheden.

(92) Selv om fremstillingen af håndgribelige produkter med digitale elementer normalt kræver, at fabrikanterne gør en betydelig indsats i hele design-, udviklings- og produktionsfasen, er der ved fremstillingen af produkter med digitale elementer i form af software næsten udelukkende fokus på design og udvikling, mens produktionsfasen spiller en mindre rolle. I mange tilfælde skal softwareprodukter dog stadig først samles, bygges, pakkes, gøres tilgængelige for download eller kopieres på fysiske medier, inden de bringes i omsætning. Disse aktiviteter bør anses som aktiviteter, der svarer til produktion, når de relevante overensstemmelsesvurderingsmoduler anvendes til at verificere produktets overensstemmelse med de væsentlige cybersikkerhedskrav i denne forordning i hele design-, udviklings- og produktionsfasen.

(93) For så vidt angår mikrovirksomheder og små virksomheder er det for at sikre proportionalitet hensigtsmæssigt at mindske de administrative omkostninger uden at påvirke graden af cybersikkerhedsbeskyttelse for produkter med digitale elementer, der er omfattet af denne forordnings anvendelsesområde, eller de lige konkurrencevilkår for fabrikanter. Det er derfor hensigtsmæssigt, at Kommissionen udarbejder en forenklet teknisk dokumentationsformular, der er målrettet mikrovirksomheders og små virksomheders behov. Den forenklede tekniske dokumentationsformular, som Kommissionen har vedtaget, bør omfatte alle de relevante elementer vedrørende den tekniske dokumentation, der er fastsat i denne forordning, og præcisere, hvordan en mikrovirksomhed eller en lille virksomhed kan levere de ønskede elementer på en koncis måde, såsom beskrivelsen af designet, udviklingen og produktionen af produktet med digitale elementer. I den forbindelse vil formularen bidrage til at lette den administrative byrde i forbindelse med overensstemmelse ved at give de berørte virksomheder retssikkerhed med hensyn til omfanget og detaljeringsgraden af de oplysninger, der skal gives. Mikrovirksomheder og små virksomheder bør kunne vælge at fremlægge de relevante elementer vedrørende teknisk dokumentation i omfattende form og ikke drage fordel af den forenklede tekniske form, der er til rådighed for dem.

(94) For at fremme og beskytte innovation er det vigtigt, at der tages særligt hensyn til interesserne hos fabrikanter, der er mikrovirksomheder eller små eller mellemstore virksomheder, navnlig mikrovirksomheder og små virksomheder, herunder nyetablerede virksomheder. Med henblik herpå kan medlemsstaterne udvikle initiativer, der er rettet mod fabrikanter, der er mikrovirksomheder eller små virksomheder, herunder for så vidt angår aktiviteter vedrørende uddannelse, bevidstgørelse, kommunikation af oplysninger, afprøvning og tredjepartsoverensstemmelsesvurdering samt oprettelse af sandkasser. Udgifter til oversættelse i forbindelse med obligatorisk dokumentation såsom den tekniske dokumentation og de oplysninger og anvisninger til brugeren, der kræves i henhold til denne forordning, og kommunikation med myndighederne kan udgøre en betydelig omkostning for fabrikanterne, herunder fabrikanter af mindre størrelse. Medlemsstaterne bør derfor kunne bestemme, at et af de sprog, som de bestemmer sig for og accepterer til de relevante fabrikanters dokumentation og til kommunikation med fabrikanter, er et sprog, der forstås bredt af det størst mulige antal brugere.

(95) For at sikre en gnidningsløs anvendelse af denne forordning bør medlemsstaterne sikre, at der inden datoen for denne forordnings anvendelse er et tilstrækkeligt antal bemyndigede organer tilgængelige til at udføre tredjepartsoverensstemmelsesvurderinger. Kommissionen bør bistå medlemsstaterne og andre relevante parter med disse bestræbelser for at undgå flaskehalse og hindringer for fabrikanters markedsadgang. Målrettede uddannelsesaktiviteter under ledelse af medlemsstaterne, herunder, hvor det er hensigtsmæssigt, med støtte fra Kommissionen, kan bidrage til tilgængeligheden af kvalificerede fagfolk, herunder til støtte for bemyndigede organers aktiviteter i henhold til denne forordning. I betragtning af de omkostninger, som tredjepartsoverensstemmelsesvurderinger kan medføre, bør det desuden overvejes at finansiere initiativer på EU-plan og nationalt plan, der har til formål at lette sådanne omkostninger for mikrovirksomheder og små virksomheder.

(96) For at sikre proportionalitet bør overensstemmelsesvurderingsorganer, når de fastsætter gebyrerne for overensstemmelsesvurderingsprocedurer, tage hensyn til mikrovirksomheders og små og mellemstore virksomheders, herunder nyetablerede virksomheders, særlige interesser og behov. Overensstemmelsesvurderingsorganerne bør navnlig kun anvende den relevante undersøgelsesprocedure og de relevante afprøvninger, der er fastsat i denne forordning, hvor det er relevant og efter en risikobaseret tilgang.

(97) Formålet med reguleringsmæssige sandkasser bør være at fremme innovation og konkurrenceevne for virksomheder ved at etablere kontrollerede afprøvningsmiljøer, inden produkter med digitale elementer bringes i omsætning. Reguleringsmæssige sandkasser bør bidrage til at forbedre retssikkerheden for alle aktører, der er omfattet af denne forordnings anvendelsesområde, og lette og fremskynde adgangen til EU-markedet for produkter med digitale elementer, navnlig når de leveres af mikrovirksomheder og små virksomheder, herunder nyetablerede virksomheder.

(98) Med henblik på foretagelse af tredjepartsoverensstemmelsesvurderinger af produkter med digitale elementer bør de nationale bemyndigende myndigheder notificere overensstemmelsesvurderingsorganer til Kommissionen og de øvrige medlemsstater, forudsat at de opfylder en række krav, navnlig med hensyn til uafhængighed, kompetencer og fravær af interessekonflikter.

(99) For at sikre et ensartet kvalitetsniveau ved overensstemmelsesvurderingen af produkter med digitale elementer er det også nødvendigt at fastsætte krav til bemyndigende myndigheder og andre organer, som er involveret i vurdering, bemyndigelse og overvågning af bemyndigede organer. Den ordning, der fastsættes ved denne forordning, bør suppleres af akkrediteringsordningen som omhandlet i forordning (EF) nr. 765/2008. Da akkreditering er et vigtigt middel til at efterprøve overensstemmelsesvurderingsorganers kompetence, bør det også anvendes med henblik på bemyndigelse.

(100) Overensstemmelsesvurderingsorganer, der er akkrediteret og bemyndiget i henhold til EU-retten, der fastsætter krav svarende til dem, der er fastsat i denne forordning, såsom et overensstemmelsesvurderingsorgan, der er bemyndiget til en europæisk cybersikkerhedscertificeringsordning vedtaget i henhold til forordning (EU) 2019/881 eller bemyndiget i henhold til delegeret forordning (EU) 2022/30, bør vurderes og bemyndiges på ny i henhold til nærværende forordning. De relevante myndigheder kan dog definere synergier med hensyn til overlappende krav for at undgå unødvendige finansielle og administrative byrder og for at sikre en gnidningsløs og rettidig bemyndigelsesprocedure.

(101) De nationale offentlige myndigheder i hele Unionen bør betragte gennemsigtig akkreditering som foreskrevet i forordning (EF) nr. 765/2008, der sikrer den fornødne tillid til overensstemmelsesattester, som værende det foretrukne middel til dokumentation af overensstemmelsesvurderingsorganers tekniske kompetence. De nationale myndigheder kan imidlertid finde, at de selv har passende midler til at foretage denne evaluering. I så fald bør de for at sikre et passende troværdighedsniveau for evalueringer, der foretages af andre nationale myndigheder, forelægge Kommissionen og de øvrige medlemsstater den nødvendige dokumentation for, at de evaluerede overensstemmelsesvurderingsorganer overholder de relevante forskriftsmæssige krav.

(102) Overensstemmelsesvurderingsorganer giver ofte dele af deres aktiviteter i forbindelse med overensstemmelsesvurdering til underleverandører eller benytter sig af en dattervirksomhed. For at sikre det krævede beskyttelsesniveau for et produkt med digitale elementer, der skal bringes i omsætning, er det afgørende, at de pågældende underleverandører og dattervirksomheder opfylder de samme krav som bemyndigede organer hvad angår udførelse af overensstemmelsesvurderingsopgaver.

(103) Den bemyndigende myndighed bør fremsende underretningen om bemyndigelsen af et overensstemmelsesvurderingsorgan til Kommissionen og de øvrige medlemsstater via NANDO-informationssystemet (New Approach Notified and Designated Organisations). NANDO-informationssystemet er det elektroniske notifikationsværktøj, som Kommissionen har udviklet og administrerer, og det indeholder en liste over alle bemyndigede organer.

(104) Eftersom bemyndigede organer kan tilbyde deres tjenester i hele Unionen, er det hensigtsmæssigt at give de øvrige medlemsstater og Kommissionen mulighed for at kunne gøre indsigelse mod et bemyndiget organ. Det er derfor vigtigt, at der fastsættes en periode, inden for hvilken eventuel tvivl eller usikkerhed om overensstemmelsesvurderingsorganers kompetence kan afklares, før de påbegynder deres aktiviteter som bemyndigede organer.

(105) Af konkurrencehensyn er det afgørende, at bemyndigede organer anvender overensstemmelsesvurderingsprocedurerne uden at skabe unødvendige byrder for de erhvervsdrivende. Af samme grund og for at sikre, at de erhvervsdrivende behandles ens, er det nødvendigt at sikre, at den tekniske anvendelse af overensstemmelsesvurderingsprocedurerne er ensartet. Dette kan bedst opnås gennem hensigtsmæssig koordinering og samarbejde mellem de bemyndigede organer.

(106) Markedsovervågning er et væsentligt instrument til at sikre en korrekt og ensartet anvendelse af EU-retten. Det er derfor hensigtsmæssigt at skabe juridiske rammer, inden for hvilke markedsovervågningen kan foretages på en passende måde. Reglerne om EU-markedsovervågning og kontrol af produkter, der indføres på EU-markedet, i forordning (EU) 2019/1020 finder anvendelse på produkter med digitale elementer, der er omfattet af nærværende forordnings anvendelsesområde.

(107) I overensstemmelse med forordning (EU) 2019/1020 udfører en markedsovervågningsmyndighed markedsovervågning på området for den medlemsstat, som udpeger den. Nærværende forordning bør ikke forhindre medlemsstater i at vælge de kompetente myndigheder, der skal udføre markedsovervågningsopgaver. Hver medlemsstat bør udpege en eller flere markedsovervågningsmyndigheder på dens område. Medlemsstaterne bør kunne vælge at udpege enhver eksisterende eller ny myndighed som markedsovervågningsmyndighed, herunder kompetente myndigheder udpeget eller etableret i henhold til artikel 8 i direktiv (EU) 2022/2555, nationale cybersikkerhedscertificeringsmyndigheder udpeget i henhold til artikel 58 i forordning (EU) 2019/881 eller markedsovervågningsmyndigheder udpeget med henblik på direktiv 2014/53/EU. Erhvervsdrivende bør samarbejde fuldt ud med markedsovervågningsmyndigheder og andre kompetente myndigheder. Hver medlemsstat bør underrette Kommissionen samt de øvrige medlemsstater om sine markedsovervågningsmyndigheder og kompetenceområderne for hver af disse myndigheder og bør sikre de nødvendige ressourcer og færdigheder til at udføre markedsovervågningsopgaverne vedrørende nærværende forordning. I henhold til artikel 10, stk. 2 og 3, i forordning (EU) 2019/1020 bør hver medlemsstat udpege et centralt forbindelseskontor, der bl.a. er ansvarligt for at repræsentere den koordinerede holdning blandt markedsovervågningsmyndighederne og bidrage til samarbejdet mellem markedsovervågningsmyndighederne i forskellige medlemsstater.

(108) Der bør oprettes en særlig ADCO for cyberrobustheden af produkter med digitale elementer med henblik på ensartet gennemførelse af denne forordning i henhold til artikel 30, stk. 2, i forordning (EU) 2019/1020. ADCO bør bestå af repræsentanter fra de udpegede markedsovervågningsmyndigheder og, hvis det er relevant, repræsentanter fra de centrale forbindelseskontorer. Kommissionen bør støtte og tilskynde til samarbejde mellem markedsovervågningsmyndigheder gennem EU-netværket for produktoverensstemmelse, der er oprettet i henhold til artikel 29 i forordning (EU) 2019/1020 og består af repræsentanter for hver medlemsstat, herunder en repræsentant for hvert centralt forbindelseskontor som omhandlet i nævnte forordnings artikel 10 og en valgfri national ekspert, formændene for ADCO'erne og repræsentanter for Kommissionen. Kommissionen bør deltage i møderne hos EU-netværket for produktoverensstemmelse, dets undergrupper og ADCO. Den bør også bistå ADCO med et administrativt sekretariat, der yder teknisk og logistisk støtte. ADCO kan også indbyde uafhængige eksperter til at deltage og samarbejde med andre ADCO'er såsom den, der er oprettet i henhold til direktiv 2014/53/EU.

(109) Markedsovervågningsmyndighederne bør gennem ADCO, der oprettes i henhold til denne forordning, arbejde tæt sammen og bør kunne udarbejde vejledninger for at lette markedsovervågningsaktiviteter på nationalt plan såsom ved at udvikle bedste praksis og indikatorer med henblik på effektivt at kontrollere, at produkter med digitale elementer overholder denne forordning.

(110) For at sikre rettidige, forholdsmæssige og effektive foranstaltninger vedrørende produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, bør der indføres en EU-beskyttelsesprocedure, hvorved berørte parter orienteres om påtænkte foranstaltninger vedrørende sådanne produkter. Herved vil markedsovervågningsmyndighederne i samarbejde med de relevante erhvervsdrivende også få mulighed for at gribe ind i en tidligere fase, hvor det er nødvendigt. Hvor medlemsstaterne og Kommissionen er enige om berettigelsen af en foranstaltning truffet af en medlemsstat, bør Kommissionen ikke inddrages yderligere, medmindre manglende overholdelse af kravene kan tillægges mangler ved en harmoniseret standard.

(111) I visse tilfælde kan et produkt med digitale elementer, der overholder denne forordning, ikke desto mindre udgøre en væsentlig cybersikkerhedsrisiko eller en risiko for menneskers sundhed eller sikkerhed, for misligholdelse af forpligtelser i henhold til den del af EU-retten eller national ret, der har til formål at beskytte de grundlæggende rettigheder, tilgængeligheden, autenticiteten, integriteten eller fortroligheden af tjenester, der leveres ved brug af elektroniske informationssystemer af væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555, eller andre aspekter af beskyttelsen af den offentlige interesse. Det er derfor nødvendigt at fastsætte regler, der sikrer, at disse risici afbødes. Som følge heraf bør markedsovervågningsmyndighederne træffe foranstaltninger til at kræve, at den erhvervsdrivende sikrer, at produktet ikke længere udgør den risiko, eller at det tilbagekaldes eller trækkes tilbage, afhængigt af risikoen. Så snart en markedsovervågningsmyndighed begrænser eller forbyder den frie bevægelighed for et produkt med digitale elementer på en sådan måde, bør medlemsstaten straks underrette Kommissionen og de øvrige medlemsstater om de foreløbige foranstaltninger og angive begrundelserne for afgørelsen. Hvor en markedsovervågningsmyndighed vedtager sådanne foranstaltninger over for produkter med digitale elementer, der udgør en risiko, bør Kommissionen straks rådføre sig med medlemsstaterne og den eller de relevante erhvervsdrivende og evaluere den nationale foranstaltning. På grundlag af resultaterne af denne evaluering bør Kommissionen træffe afgørelse om, hvorvidt den nationale foranstaltning er berettiget eller ej. Kommissionen bør rette sin afgørelse til alle medlemsstaterne og omgående meddele den til disse og til den eller de relevante erhvervsdrivende. Hvis foranstaltningen anses for at være berettiget, bør Kommissionen også overveje, om der skal vedtages forslag til revision af den relevante EU-ret.

(112) For produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, og hvor der er grund til at tro, at de ikke er i overensstemmelse med denne forordning, eller for produkter, som er i overensstemmelse med denne forordning, men indebærer andre betydelige risici såsom risici for menneskers sundhed eller sikkerhed, for overholdelse af forpligtelser i henhold til EU-retten eller national ret, der har til formål at beskytte de grundlæggende rettigheder, eller for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af tjenester, der leveres ved brug af elektroniske informationssystemer af væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555, bør Kommissionen bør kunne anmode ENISA om at foretage en evaluering. På grundlag af denne evaluering bør Kommissionen ved hjælp af gennemførelsesretsakter kunne vedtage korrigerende eller restriktive foranstaltninger på EU-plan, herunder påbud om at trække de pågældende produkter med digitale elementer tilbage fra markedet eller tilbagekalde dem inden for en rimelig tidsfrist, som den fastsætter i forhold til risikoens art. Kommissionen bør kun kunne foretage et sådant indgreb under ekstraordinære omstændigheder, der berettiger et hurtigt indgreb for at bevare et velfungerende indre marked, og kun hvis markedsovervågningsmyndighederne ikke har truffet effektive foranstaltninger til at rette op på situationen. Sådanne ekstraordinære omstændigheder kan være nødsituationer, f.eks. hvor et produkt med digitale elementer, der ikke opfylder kravene, gøres bredt tilgængeligt af fabrikanten i flere medlemsstater og også anvendes af enheder i nøglesektorer, der er omfattet af anvendelsesområdet for direktiv (EU) 2022/2555, selv om det indeholder kendte sårbarheder, der udnyttes af ondsindede aktører, og som fabrikanten ikke udsender rettelser til. Kommissionen bør kun kunne gribe ind i sådanne nødsituationer, så længe de ekstraordinære omstændigheder er til stede, og hvis manglende overholdelse af denne forordning eller de betydelige risici forbundet hermed fortsat er til stede.

(113) Hvor der er tegn på manglende overholdelse af denne forordning i flere medlemsstater, bør markedsovervågningsmyndighederne kunne gennemføre fælles aktiviteter med andre myndigheder med henblik på at verificere overholdelsen og identificere cybersikkerhedsrisici forbundet med produkter med digitale elementer.

(114) Samtidige koordinerede kontrolaktioner er specifikke håndhævelsesforanstaltninger truffet af markedsovervågningsmyndighederne, som kan forbedre produktsikkerheden. Kontrolaktioner bør navnlig foretages, hvor markedstendenser, forbrugerklager eller andre forhold tyder på, at visse kategorier af produkter med digitale elementer ofte viser sig at udgøre en cybersikkerhedsrisiko. Ved fastlæggelsen af, hvilke produktkategorier der skal underkastes kontrolaktioner, bør markedsovervågningsmyndighederne desuden også tage hensyn til omstændigheder vedrørende ikketekniske risikofaktorer. Med henblik herpå bør markedsovervågningsmyndighederne kunne tage hensyn til resultaterne af koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan, der foretages i overensstemmelse med artikel 22 i direktiv (EU) 2022/2555, herunder omstændigheder vedrørende ikketekniske risikofaktorer. ENISA bør indsende forslag til kategorier af produkter med digitale elementer, for hvilke der kan tilrettelægges kontrolaktioner, til markedsovervågningsmyndighederne, bl.a. på grundlag af de underretninger om produktsårbarheder og hændelser, som det modtager.

(115) I betragtning af ENISA's ekspertise og mandat bør det være i stand til at støtte processen for gennemførelse af denne forordning. ENISA bør navnlig kunne foreslå fælles aktiviteter, der skal gennemføres af markedsovervågningsmyndighederne, på grundlag af tegn på eller oplysninger om, at kravene i denne forordning til produkter med digitale elementer muligvis ikke overholdes i flere medlemsstater, eller identificere produktkategorier, for hvilke der bør tilrettelægges kontrolaktioner. Under ekstraordinære omstændigheder bør ENISA efter anmodning fra Kommissionen kunne foretage evalueringer af specifikke produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, hvor der er behov for et hurtigt indgreb for at bevare et velfungerende indre marked.

(116) Denne forordning overdrager visse opgaver til ENISA, som kræver passende ressourcer med hensyn til både ekspertise og menneskelige ressourcer for at sætte ENISA i stand til at udføre disse opgaver effektivt. Kommissionen vil ved udarbejdelsen af forslaget til Unionens almindelige budget foreslå de nødvendige budgetmidler til ENISA's stillingsfortegnelse i overensstemmelse med proceduren i artikel 29 i forordning (EU) 2019/881. Under denne proces vil Kommissionen tage hensyn til ENISA's samlede ressourcer for at sætte det i stand til at udføre sine opgaver, herunder dem, der pålægges ENISA i henhold til nærværende forordning.

(117) For at sikre, at den lovgivningsmæssige ramme kan tilpasses, hvor det er nødvendigt, bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), for så vidt angår opdateringer af et bilag til denne forordning med listen over vigtige produkter med digitale elementer. Beføjelsen til at vedtage retsakter bør delegeres til Kommissionen i overensstemmelse med nævnte artikel for at identificere produkter med digitale elementer, der er omfattet af andre EU-regler og opnår samme beskyttelsesniveau som i denne forordning, og for at præcisere, om en begrænsning eller udelukkelse fra denne forordnings anvendelsesområde er nødvendig, samt omfanget af denne begrænsning, hvis det er relevant. Beføjelsen til at vedtage retsakter bør også delegeres til Kommissionen i overensstemmelse med nævnte artikel for så vidt angår potentiel tildeling af mandat til certificering i henhold til en europæisk cybersikkerhedscertificeringsordning for kritiske produkter med digitale elementer fastsat i et bilag til denne forordning, og til at opdatere listen over kritiske produkter med digitale elementer baseret på kritikalitetskriterier fastsat i denne forordning, samt til at præcisere den europæiske cybersikkerhedscertificeringsordning, der er vedtaget i henhold til forordning (EU) 2019/881, som kan anvendes til at påvise overensstemmelse med de væsentlige cybersikkerhedskrav eller dele heraf som fastsat i et bilag til nærværende forordning. Beføjelsen til at vedtage retsakter bør også delegeres til Kommissionen med henblik på at præcisere minimumssupportperioden for visse produktkategorier, hvis markedsovervågningsdataene tyder på utilstrækkelige supportperioder, samt til at præcisere vilkårene og betingelserne for anvendelse af de cybersikkerhedsrelaterede grunde i forbindelse med udsættelse af formidlingen af underretninger om aktivt udnyttede sårbarheder. Desuden bør beføjelsen til at vedtage retsakter delegeres til Kommissionen med henblik på at fastlægge frivillige sikkerhedscertificeringsprogrammer for at vurdere overensstemmelsen af produkter med digitale elementer, der kan betegnes som gratis open source-software, med alle eller visse væsentlige cybersikkerhedskrav eller andre forpligtelser, der er fastsat i nærværende forordning, samt for at præcisere minimumsindholdet af EU-overensstemmelseserklæringen og supplere de elementer, der skal indgå i den tekniske dokumentation. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning ([31]). For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter. Beføjelsen til at vedtage delegerede retsakter i henhold til nærværende forordning bør tillægges Kommissionen for en periode på fem år fra den 10. december 2024. Kommissionen bør udarbejde en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. Delegationen af beføjelser bør stiltiende forlænges for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.

(118) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser til at præcisere den tekniske beskrivelse af kategorierne af vigtige produkter med digitale elementer, der er fastsat i et bilag til denne forordning, præcisere formatet og elementerne i softwarekomponentlisten, yderligere præcisere formatet og proceduren for underretninger om aktivt udnyttede sårbarheder og alvorlige hændelser, der har indvirkning på sikkerheden af produkter med digitale elementer, der indgives af fabrikanter, fastsætte fælles specifikationer, der dækker tekniske krav, der giver mulighed for at opfylde de væsentlige cybersikkerhedskrav, der er fastsat i et bilag til denne forordning, fastsætte tekniske specifikationer for etiketter, piktogrammer eller andre mærker vedrørende sikkerheden af produkter med digitale elementer, deres supportperiode og mekanismer til at fremme deres anvendelse og øge offentlighedens bevidsthed om sikkerheden ved produkter med digitale elementer, præcisere den forenklede dokumentationsformular, der er rettet mod mikrovirksomheders og små virksomheders behov, og træffe afgørelse om korrigerende eller restriktive

([31]) EUT L 123 af 12.5.2016, s. 1.

foranstaltninger på EU-plan under ekstraordinære omstændigheder, der berettiger et hurtigt indgreb for at bevare et velfungerende indre marked. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 ([32]).

(119) For at sikre et tillidsfuldt og konstruktivt samarbejde mellem markedsovervågningsmyndigheder på EU-plan og nationalt plan bør alle de parter, der er involveret i anvendelsen af denne forordning, respektere fortroligheden af de oplysninger og data, der er indhentet under udførelsen af deres opgaver.

(120) For at sikre en effektiv håndhævelse af de forpligtelser, der er fastsat i denne forordning, bør hver markedsovervågningsmyndighed have beføjelse til at pålægge eller anmode om pålæggelse af administrative bøder. Der bør derfor fastsættes maksimumsniveauer for administrative bøder i national ret for manglende overholdelse af forpligtelserne i denne forordning. Ved fastsættelsen af den administrative bødes størrelse bør der i hvert enkelt tilfælde tages hensyn til alle relevante omstændigheder i den specifikke situation og som minimum dem, der udtrykkeligt er fastsat i denne forordning, herunder hvorvidt fabrikanten er en mikrovirksomhed eller en lille eller mellemstor virksomhed, herunder en nyetableret virksomhed, og hvorvidt andre markedsovervågningsmyndigheder allerede har pålagt den samme erhvervsdrivende administrative bøder for lignende overtrædelser. Sådanne omstændigheder kan enten være skærpende i situationer, hvor den samme erhvervsdrivendes overtrædelse varer ved på en anden medlemsstats område end den, hvor der allerede er pålagt en administrativ bøde, eller formildende ved at sikre, at der i forbindelse med enhver anden administrativ bøde, som en anden markedsovervågningsmyndighed overvejer at pålægge den samme erhvervsdrivende eller for den samme type overtrædelse, tages hensyn til en bøde og størrelsen heraf pålagt i andre medlemsstater og til andre relevante særlige omstændigheder. I alle sådanne tilfælde bør den kumulative administrative bøde, som markedsovervågningsmyndighederne i flere medlemsstater kan pålægge den samme erhvervsdrivende for den samme type overtrædelse, sikre, at proportionalitetsprincippet overholdes. Eftersom administrative bøder ikke finder anvendelse på mikrovirksomheder eller små virksomheder for manglende overholdelse af fristen på 24 timer for tidlig varsling om aktivt udnyttede sårbarheder eller alvorlige hændelser, der har indvirkning på sikkerheden af produktet med digitale elementer, eller på open source software-forvaltere for overtrædelse af denne forordning, og uden at det berører princippet om, at sanktionerne bør være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning, bør medlemsstaterne ikke pålægge disse enheder andre former for bøder.

(121) Hvor en person, der ikke er en virksomhed, pålægges administrative bøder, bør den kompetente myndighed i forbindelse med fastsættelsen af bødestørrelsen tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske situation. Det bør være op til medlemsstaterne at bestemme, om og i hvilket omfang de offentlige myndigheder bør kunne pålægges administrative bøder.

(122) Medlemsstaterne bør under hensyntagen til nationale forhold undersøge muligheden for at anvende indtægterne fra sanktionerne som fastsat i denne forordning eller deres finansielle ækvivalent til at støtte cybersikkerhedspolitikker og øge cybersikkerhedsniveauet i Unionen ved bl.a. at øge antallet af kvalificerede fagfolk inden for cybersikkerhed, styrke kapacitetsopbygningen for mikrovirksomheder og små og mellemstore virksomheder og forbedre offentlighedens bevidsthed om cybertrusler.

(123) I sine relationer med tredjelande tilstræber Unionen at fremme international handel med regulerede produkter. Der kan anvendes en lang række foranstaltninger til at fremme handel, herunder en række retlige instrumenter såsom bilaterale (mellemstatslige) aftaler om gensidig anerkendelse af overensstemmelsesvurdering og mærkning af regulerede produkter. Aftaler om gensidig anerkendelse indgås mellem Unionen og tredjelande, der er på samme tekniske udviklingsniveau og har en tilsvarende tilgang til overensstemmelsesvurdering. Disse aftaler er baseret på gensidig accept af certifikater, overensstemmelsesmærkninger og afprøvningsrapporter udstedt af parternes overensstemmelsesvurderingsorganer i overensstemmelse med den anden parts lovgivning. I øjeblikket er der indgået aftaler om gensidig anerkendelse med flere tredjelande. Disse aftaler er indgået i en række specifikke sektorer, der kan variere fra tredjeland til tredjeland. For yderligere at lette handelen og i erkendelse af, at forsyningskæderne for produkter med digitale elementer er globale, kan aftaler om gensidig anerkendelse vedrørende overensstemmelsesvurdering for produkter, der reguleres i henhold til denne forordning, indgås af Unionen i overensstemmelse med artikel 218 i TEUF. Samarbejde med partnertredjelande er også vigtigt for at styrke cyberrobustheden på globalt plan, da dette på lang sigt vil bidrage til en styrket ramme for cybersikkerhed både i og uden for Unionen.

([32]) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) Forbrugere bør have ret til at håndhæve deres rettigheder i relation til de forpligtelser, som erhvervsdrivende pålægges i henhold til denne forordning, gennem anlæggelse af gruppesøgsmål i overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2020/1828 ([33]). Det bør med henblik herpå fastsættes i denne forordning, at direktiv (EU) 2020/1828 finder anvendelse på gruppesøgsmål vedrørende overtrædelser af denne forordning, som skader eller kan skade forbrugernes kollektive interesser. Bilag I til nævnte direktiv bør derfor ændres i overensstemmelse hermed. Det er op til medlemsstaterne at sikre, at disse ændringer afspejles i gennemførelsesforanstaltningerne, der er vedtaget i henhold til nævnte direktiv, selv om vedtagelsen af nationale gennemførelsesforanstaltninger i denne henseende ikke er en betingelse for, at nævnte direktiv kan finde anvendelse på disse gruppesøgsmål. Anvendeligheden af nævnte direktiv på gruppesøgsmål, der anlægges til prøvelse af erhvervsdrivendes overtrædelser af bestemmelserne i denne forordning, og som skader eller kan skade forbrugernes kollektive interesser, bør begynde fra den 11. december 2027.

(125) Kommissionen bør regelmæssigt evaluere og revidere denne forordning efter høring af relevante interessenter, navnlig med henblik på at afgøre, om der er behov for ændringer i lyset af skiftende samfundsmæssige, politiske eller teknologiske vilkår eller markedsvilkår. Denne forordning vil lette overholdelsen af forpligtelserne vedrørende forsyningskædesikkerhed for enheder, der er omfattet af anvendelsesområdet for forordning (EU) 2022/2554 og direktiv (EU) 2022/2555, og som anvender produkter med digitale elementer. Kommissionen bør som led i denne periodiske revision evaluere de kombinerede virkninger af Unionens ramme for cybersikkerhed.

(126) Erhvervsdrivende bør have tilstrækkelig tid til at tilpasse sig kravene i denne forordning. Denne forordning bør anvendes fra 11. december 2027 med undtagelse af indberetningsforpligtelserne vedrørende aktivt udnyttede sårbarheder og alvorlige hændelser, der har indvirkning på sikkerheden af produkter med digitale elementer, som bør finde anvendelse fra den 11. september 2026, og bestemmelserne om bemyndigelse af overensstemmelsesvurderingsorganer, som bør finde anvendelse fra den 11. juni 2026.

(127) Det er vigtigt at yde støtte til mikrovirksomheder og små og mellemstore virksomheder, herunder nyetablerede virksomheder, i forbindelse med gennemførelsen af denne forordning og minimere risiciene for gennemførelsen som følge af manglende viden og ekspertise på markedet samt for at lette fabrikanternes overholdelse af deres forpligtelser i henhold til denne forordning. Programmet for et digitalt Europa og andre relevante EU-programmer yder finansiel og teknisk støtte, der sætter disse virksomheder i stand til at bidrage til væksten i Unionens økonomi og til styrkelsen af det fælles cybersikkerhedsniveau i Unionen. Det Europæiske Kompetencecenter for Cybersikkerhed og nationale koordinationscentre samt europæiske digitale innovationsknudepunkter, der er oprettet af Kommissionen og medlemsstaterne på EU-plan eller nationalt plan, kan også støtte virksomheder og organisationer i den offentlige sektor og kan bidrage til gennemførelsen af denne forordning. Inden for rammerne af deres respektive ydelser og kompetenceområder kan de yde teknisk og videnskabelig støtte til mikrovirksomheder og små og mellemstore virksomheder såsom til afprøvningsaktiviteter og tredjepartsoverensstemmelsesvurderinger. De kan også fremme anvendelsen af værktøjer til at lette gennemførelsen af denne forordning.

(128) Desuden bør medlemsstaterne overveje at træffe supplerende foranstaltninger, der har til formål at yde vejledning og støtte til mikrovirksomheder og små og mellemstore virksomheder, såsom oprettelse af reguleringsmæssige sandkasser og dedikerede kanaler for kommunikation. For at styrke cybersikkerhedsniveauet i Unionen kan medlemsstaterne også overveje at yde støtte til udvikling af kapacitet og færdigheder inden for cybersikkerhed for produkter med digitale elementer, forbedre erhvervsdrivendes cyberrobusthed, navnlig i mikrovirksomheder og små og mellemstore virksomheder, og fremme offentlighedens bevidsthed om cybersikkerheden for produkter med digitale elementer.

(129) Målet for denne forordning kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke ud over, hvad der er nødvendigt for at nå dette mål.

(130) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([34]) og afgav en udtalelse den 9. november 2022 ([35]) —

([33]) Europa-Parlamentets og Rådets direktiv (EU) 2020/1828 af 25. november 2020 om adgang til anlæggelse af gruppesøgsmål til beskyttelse af forbrugernes kollektive interesser og om ophævelse af direktiv 2009/22/EF (EUT L 409 af 4.12.2020, s. 1).

([34]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

([35]) EUT C 452 af 29.11.2022, s. 23.

VEDTAGET DENNE FORORDNING:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand

Ved denne forordning fastsættes:

a) regler for tilgængeliggørelse på markedet af produkter med digitale elementer for at sikre cybersikkerheden for sådanne produkter

b) væsentlige cybersikkerhedskrav til design, udvikling og produktion af produkter med digitale elementer og forpligtelser for erhvervsdrivende i forbindelse med disse produkter med hensyn til cybersikkerhed

c) væsentlige cybersikkerhedskrav til sårbarhedshåndteringsprocesser, som fabrikanterne skal indføre for at sikre cybersikkerheden for produkter med digitale elementer i den periode, hvor produkterne forventes at være i brug, og forpligtelser for erhvervsdrivende i forbindelse med disse processer

d) regler om markedsovervågning, herunder tilsyn, og håndhævelse af de regler og krav, der er omhandlet i denne artikel.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på produkter med digitale elementer, der gøres tilgængelige på markedet, hvis tilsigtede formål eller rimeligt forudsigelige anvendelse omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk.

2. Denne forordning finder ikke anvendelse på produkter med digitale elementer, som følgende EU-retsakter finder anvendelse på:

a) forordning (EU) 2017/745

b) forordning (EU) 2017/746

c) forordning (EU) 2019/2144.

3. Denne forordning finder ikke anvendelse på produkter med digitale elementer, der er certificeret i overensstemmelse med forordning (EU) 2018/1139.

4. Denne forordning finder ikke anvendelse på udstyr, der er omfattet af Europa-Parlamentets og Rådets direktiv 2014/90/EU ([36]).

5. Anvendelsen af denne forordning på produkter med digitale elementer, som er omfattet af andre EU-forskrifter, der fastlægger krav vedrørende alle eller nogle af de risici, som er omfattet af de væsentlige cybersikkerhedskrav i bilag I, kan begrænses eller udelukkes, hvis:

a) en sådan begrænsning eller udelukkelse er i overensstemmelse med den overordnede lovgivningsmæssige ramme, der gælder for disse produkter, og

b) de sektorspecifikke regler sikrer samme eller højere beskyttelsesniveau som det, der er fastsat i denne forordning.

Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 61 til at supplere denne forordning ved at præcisere, hvorvidt en sådan begrænsning eller udelukkelse er nødvendig, de pågældende produkter og regler samt begrænsningens anvendelsesområde, hvis det er relevant.

([36]) Europa-Parlamentets og Rådets direktiv 2014/90/EU af 23. juli 2014 om skibsudstyr og om ophævelse af Rådets direktiv 96/98/EF (EUT L 257 af 28.8.2014, s. 146).

6. Denne forordning finder ikke anvendelse på reservedele, der gøres tilgængelige på markedet for at udskifte identiske komponenter i produkter med digitale elementer, og som er fremstillet efter de samme specifikationer som de komponenter, de skal udskifte.

7. Denne forordning finder ikke anvendelse på produkter med digitale elementer, der udelukkende udvikles eller ændres til nationale sikkerheds- eller forsvarsformål, eller på produkter, der er specifikt designet til at behandle klassificerede oplysninger.

8. De forpligtelser, der er fastsat i denne forordning, omfatter ikke meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser med hensyn til medlemsstaternes nationale sikkerhed, offentlige sikkerhed eller forsvar.

Artikel 3

Definitioner

I denne forordning forstås ved:

1) »produkt med digitale elementer«: et software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der bringes i omsætning separat

2) »fjerndatabehandling«: databehandling på afstand, til hvilken softwaren er designet og udviklet af fabrikanten eller under fabrikantens ansvar, og hvis fravær ville forhindre produktet med digitale elementer i at udføre en af sine funktioner

3) »cybersikkerhed«: cybersikkerhed som defineret i artikel 2, nr. 1), i forordning (EU) 2019/881

4) »software«: den del af et elektronisk informationssystem, der består af maskinkode

5) »hardware«: et fysisk elektronisk informationssystem eller dele heraf, der kan behandle, lagre eller overføre digitale data

6) »komponent«: software eller hardware, der er beregnet til integration i et elektronisk informationssystem

7) »elektronisk informationssystem«: et system, herunder elektrisk eller elektronisk udstyr, der kan behandle, lagre eller overføre digitale data

8) »logisk forbindelse«: virtuel gengivelse af en dataforbindelse, der implementeres via en softwaregrænseflade

9) »fysisk forbindelse«: en forbindelse mellem elektroniske informationssystemer eller komponenter, der implementeres ved hjælp af fysiske midler, herunder via elektriske, optiske eller mekaniske grænseflader, kabler eller radiobølger

10) »indirekte forbindelse«: en forbindelse til udstyr eller netværk, som ikke sker direkte, men snarere som en del af et større system, der kan tilsluttes direkte til en sådan enhed eller et sådant netværk

11) »adgangspunkt«: enhver enhed, der er tilsluttet et netværk og fungerer som indgangspunkt til dette netværk

12) »erhvervsdrivende«: fabrikanten, den bemyndigede repræsentant, importøren, distributøren eller anden fysisk eller juridisk person, der har forpligtelser i forbindelse med fremstillingen af produkter med digitale elementer eller tilgængeliggørelsen af produkter med digitale elementer på markedet i overensstemmelse med denne forordning

13) »fabrikant«: en fysisk eller juridisk person, som udvikler eller fremstiller produkter med digitale elementer eller får produkter med digitale elementer designet, udviklet eller fremstillet, og som markedsfører dem under sit navn eller varemærke mod vederlag, ved kommerciel udnyttelse eller uden vederlag

14) »open source software-forvalter«: en juridisk person, som ikke er en fabrikant, og som har til formål eller mål systematisk at yde vedvarende støtte til udvikling af specifikke produkter med digitale elementer, der kan betegnes som gratis open source-software, og som er beregnet til kommercielle aktiviteter, og som sikrer disse produkters levedygtighed

15) »bemyndiget repræsentant«: en i Unionen etableret fysisk eller juridisk person, som har modtaget en skriftlig fuldmagt fra en fabrikant til at handle på dennes vegne i forbindelse med varetagelsen af specifikke opgaver

16) »importør«: en i Unionen etableret fysisk eller juridisk person, og som bringer et produkt med digitale elementer, som bærer en uden for Unionen etableret fysisk eller juridisk persons navn eller varemærke, i omsætning

17) »distributør«: en fysisk eller juridisk person i forsyningskæden, bortset fra fabrikanten eller importøren, som gør et produkt med digitale elementer tilgængeligt på EU-markedet uden at have indflydelse på dets egenskaber

18) »forbruger«: en fysisk person, der ikke handler som led i en pågældende persons erhverv, forretning, håndværk eller profession

19) »mikrovirksomheder«, »små virksomheder« og »mellemstore virksomheder«: henholdsvis mikrovirksomheder, små virksomheder og mellemstore virksomheder som defineret i bilaget til henstilling 2003/361/EF

20) »supportperiode«: den periode, hvor det kræves, at en fabrikant sikrer, at sårbarheder i et produkt med digitale elementer håndteres effektivt og i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, del II

21) »bringe i omsætning«: første tilgængeliggørelse af et produkt med digitale elementer på EU-markedet

22) »gøre tilgængelig på markedet«: levering af et produkt med digitale elementer med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed mod eller uden vederlag

23) »tilsigtet formål«: den anvendelse, som et produkt med digitale elementer er bestemt til ifølge fabrikanten, herunder den specifikke sammenhæng og de specifikke betingelser for anvendelse som angivet i de oplysninger, fabrikanten har givet i brugsanvisningerne, i reklame- eller salgsmaterialet og -erklæringerne samt i den tekniske dokumentation

24) »anvendelse, der med rimelighed kan forudses«: anvendelse, som ikke nødvendigvis er det tilsigtede formål, som fabrikanten har angivet i brugsanvisningerne, i reklame- eller salgsmaterialet og -erklæringerne samt i den tekniske dokumentation, men som kan forventes som følge af menneskelig adfærd eller tekniske operationer eller interaktioner, der med rimelighed kan forudses

25) »fejlanvendelse, der med rimelighed kan forudses«: anvendelse af et produkt med digitale elementer på en måde, der ikke er i overensstemmelse med systemets tilsigtede formål, men som kan skyldes menneskelig adfærd eller interaktion med andre systemer, der med rimelighed kan forudses

26) »bemyndigende myndighed«: den nationale myndighed, der er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering, udpegelse og bemyndigelse af overensstemmelsesvurderingsorganer og for overvågning heraf

27) »overensstemmelsesvurdering«: en proces til verificering af, hvorvidt de væsentlige cybersikkerhedskrav i bilag I er opfyldt

28) »overensstemmelsesvurderingsorgan«: et overensstemmelsesvurderingsorgan som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008

29) »bemyndiget organ«: et overensstemmelsesvurderingsorgan, der er udpeget i overensstemmelse med artikel 43 og anden relevant EU-harmoniseringslovgivning

30) »væsentlig ændring«: en ændring af produktet med digitale elementer, efter at det er bragt i omsætning, som har indvirkning på overensstemmelsen af produktet med digitale elementer med de væsentlige cybersikkerhedskrav i bilag I, del I, eller som medfører en ændring af det tilsigtede formål, for hvilket produktet med digitale elementer er blevet vurderet

31) »CE-mærkning«: mærkning, hvormed en fabrikant angiver, at et produkt med digitale elementer og de processer, som fabrikanten har indført, er i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I og anden gældende EU-harmoniseringslovgivning om anbringelse af denne mærkning

32) »EU-harmoniseringslovgivning«: EU-lovgivningen i bilag I til forordning (EU) 2019/1020 og enhver anden EU-lovgivning, der harmoniserer betingelserne for markedsføring af produkter, på hvilke nævnte forordning finder anvendelse

33) »markedsovervågningsmyndighed«: en markedsovervågningsmyndighed som defineret i artikel 3, nr. 4), i forordning (EU) 2019/1020

34) »international standard«: en international standard som defineret i artikel 2, nr. 1), litra a), i forordning (EU) nr. 1025/2012

35) »europæisk standard«: en europæisk standard som defineret i artikel 2, nr. 1), litra b), i forordning (EU) nr. 1025/2012

36) »harmoniseret standard«: en harmoniseret standard som defineret i artikel 2, nr. 1), litra c), i forordning (EU) nr. 1025/2012

37) »cybersikkerhedsrisiko«: potentialet for tab eller forstyrrelse som følge af en hændelse, der skal udtrykkes som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer

38) »væsentlig cybersikkerhedsrisiko«: en cybersikkerhedsrisiko, hvor der som følge af dens tekniske karakteristika kan antages at være en stor sandsynlighed for en hændelse, som kan have en alvorlig negativ indvirkning, herunder ved at forårsage betydelige materielle eller immaterielle tab eller forstyrrelser

39) »softwarekomponentliste«: en formel fortegnelse med nærmere oplysninger om og forsyningskæderelationer for komponenter, der indgår i softwareelementerne i et produkt med digitale elementer

40) »sårbarhed«: en svaghed, modtagelighed eller fejl ved et produkt med digitale elementer, som kan udnyttes af en cybertrussel

41) »sårbarhed, der kan udnyttes«: en sårbarhed, der potentielt kan udnyttes effektivt af en modstander under praktiske operationelle forhold

42) »aktivt udnyttet sårbarhed«: en sårbarhed, hvor der er pålidelig dokumentation for, at en ondsindet aktør har udnyttet sårbarheden i et system uden tilladelse fra systemejeren

43) »hændelse«: en hændelse som defineret i artikel 6, nr. 6), i direktiv (EU) 2022/2555

44) »hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer«: en hændelse, der har en negativ indvirkning på eller negativt kan påvirke evnen for et produkt med digitale elementer til at beskytte tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data eller funktioner

45) »nærvedhændelse«: en nærvedhændelse som defineret i artikel 6, nr. 5), i direktiv (EU) 2022/2555

46) »cybertrussel«: en cybertrussel som defineret i artikel 2, nr. 8), i forordning (EU) 2019/881

47) »personoplysninger«: personoplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679

48) »gratis open source-software«: software, hvis kildekode deles åbent, og som stilles til rådighed under en gratis open source-licens, der giver alle rettigheder til, at den kan deles åbent og er frit tilgængelig, anvendelig, redigerbar og redistribuerbar

49) »tilbagekaldelse«: tilbagekaldelse som defineret i artikel 3, stk. 22, i forordning (EU) 2019/1020

50) »tilbagetrækning«: tilbagetrækning som defineret i artikel 3, nr. 23), i forordning (EU) 2019/1020

51) »CSIRT, der er udpeget som koordinator«: en CSIRT, der er udpeget som koordinator i henhold til artikel 12, stk. 1, i direktiv (EU) 2022/2555.

Artikel 4

Fri bevægelighed

1. Medlemsstaterne må ikke hindre tilgængeliggørelse på markedet af produkter med digitale elementer, der opfylder kravene i denne forordning, for så vidt angår spørgsmål, der er omfattet af denne forordning.

2. Medlemsstaterne må ikke modsætte sig, at der på messer, udstillinger, demonstrationer eller lignende begivenheder præsenteres eller anvendes et produkt med digitale elementer, der ikke overholder denne forordning, herunder dets prototyper, forudsat at produktet præsenteres med et synligt skilt, hvoraf det tydeligt fremgår, at det ikke overholder denne forordning og ikke må gøres tilgængeligt på markedet, før det overholder denne forordning.

3. Medlemsstaterne må ikke forhindre tilgængeliggørelse på markedet af ufærdig software, der ikke overholder denne forordning, såfremt softwaren kun gøres tilgængelig i et begrænset tidsrum, der er nødvendigt til afprøvningsformål, og med et synligt skilt, hvoraf det tydeligt fremgår, at den ikke overholder denne forordning og ikke vil være tilgængelig på markedet til andre formål end afprøvning.

4. Stk. 3 finder ikke anvendelse på sikkerhedskomponenter som omhandlet i anden EU-harmoniseringslovgivning end denne forordning.

Artikel 5

Offentlige indkøb af produkter med digitale elementer

1. Denne forordning er ikke til hinder for, at medlemsstaterne underlægger produkter med digitale elementer yderligere cybersikkerhedskrav med henblik på offentlige indkøb eller anvendelse af disse produkter til specifikke formål, herunder når disse produkter indkøbes eller anvendes til nationale sikkerheds- eller forsvarsformål, forudsat at sådanne krav er i overensstemmelse med medlemsstaternes forpligtelser i henhold til EU-retten, og at de er nødvendige og forholdsmæssige for at opfylde disse formål.

2. Uden at det berører direktiv 2014/24/EU og 2014/25/EU, sikrer medlemsstaterne i forbindelse med indkøb af produkter med digitale elementer, der er omfattet af denne forordnings anvendelsesområde, at der i udbudsprocessen tages hensyn til overholdelsen af de væsentlige cybersikkerhedskrav i bilag I til denne forordning, herunder fabrikanternes evne til at håndtere sårbarheder effektivt.

Artikel 6

Krav til produkter med digitale elementer

Produkter med digitale elementer må kun gøres tilgængelige på markedet, hvis:

a) de opfylder de væsentlige cybersikkerhedskrav i bilag I, del I, forudsat at de er korrekt installeret og vedligeholdt og anvendes til det tilsigtede formål eller på betingelser, der med rimelighed kan forudses, og, i givet fald, at de nødvendige sikkerhedsmæssige opdateringer er blevet installeret, og

b) de processer, som fabrikanten har indført, opfylder de væsentlige cybersikkerhedskrav i bilag I, del II.

Artikel 7

Vigtige produkter med digitale elementer

1. Produkter med digitale elementer, hvis væsentligste funktionalitet henhører under en produktkategori, der er fastsat i bilag III, anses som vigtige produkter med digitale elementer og er omfattet af de overensstemmelsesvurderingsprocedurer, der er omhandlet i artikel 32, stk. 2 og 3. Integrationen af et produkt med digitale elementer, hvis væsentligste funktionalitet henhører under en produktkategori, der er fastsat i bilag III, gør ikke i sig selv det produkt, som det er integreret i, omfattet af de overensstemmelsesvurderingsprocedurer, der er omhandlet i artikel 32, stk. 2 og 3.

2. De kategorier af produkter med digitale elementer, der er omhandlet i denne artikels stk. 1, opdelt i klasse I og II, som fastsat i bilag III, opfylder mindst ét af følgende kriterier:

a) produktet med digitale elementer udfører primært funktioner, der er afgørende for andre produkters, netværks eller tjenesters cybersikkerhed, herunder sikring af autentifikation og adgang, forebyggelse og opdagelse af indtrængen, adgangspunktssikkerhed eller netværksbeskyttelse

b) produktet med digitale elementer udfører en funktion, der indebærer en betydelig risiko for negative virkninger med hensyn til intensitet og evne til at afbryde, kontrollere eller forvolde skade på et stort antal andre produkter eller på brugernes sundhed eller sikkerhed gennem direkte manipulation såsom en central systemfunktion, herunder netværksstyring, konfigurationskontrol, virtualisering eller behandling af personoplysninger.

3. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 61 med henblik på at ændre bilag III ved at føje til listen en ny kategori inden for hver klasse af kategorierne af produkter med digitale elementer og præcisere dens definition, flytte en kategori af produkter fra en klasse til den anden eller fjerne en eksisterende kategori fra denne liste. Ved vurderingen af behovet for at ændre listen fastsat i bilag III tager Kommissionen hensyn til de cybersikkerhedsrelaterede funktioner eller den funktion og det niveau af cybersikkerhedsrisiko, som produkter med digitale elementer udgør som fastsat ved de kriterier, der er omhandlet i nærværende artikels stk. 2.

De delegerede retsakter, der er omhandlet i nærværende stykkes første afsnit, fastsætter, hvor det er relevant, en mindste overgangsperiode på 12 måneder, navnlig hvis en ny kategori af vigtige produkter med digitale elementer føjes til klasse I eller II eller flyttes fra klasse I til II som fastsat i bilag III, inden de relevante overensstemmelsesvurderingsprocedurer som omhandlet i artikel 32, stk. 2, og 3, begynder at finde anvendelse, medmindre en kortere overgangsperiode er berettiget i særligt hastende tilfælde.

4. Senest den 11. december 2025 vedtager Kommissionen en gennemførelsesretsakt, der præciserer den tekniske beskrivelse af kategorier af produkter med digitale elementer i klasse I og II som fastsat i bilag III og den tekniske beskrivelse af de kategorier af produkter med digitale elementer som fastsat i bilag IV. Denne gennemførelsesretsakt vedtages efter undersøgelsesproceduren, jf. artikel 62, stk. 2.

Artikel 8

Kritiske produkter med digitale elementer

1. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 61 med henblik på at supplere denne forordning for at fastlægge, hvilke produkter med digitale elementer, hvis væsentligste funktionalitet henhører under en produktkategori fastsat i bilag IV til denne forordning, skal indhente en europæisk cybersikkerhedsattest på et tillidsniveau, der som minimum er »betydeligt« i henhold til en europæisk cybersikkerhedscertificeringsordning vedtaget i henhold til forordning (EU) 2019/881, for at påvise overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I til nærværende forordning eller dele heraf, forudsat at der er vedtaget en europæisk cybersikkerhedscertificeringsordning i henhold til forordning (EU) 2019/881, der dækker disse kategorier af produkter med digitale elementer, og at den er tilgængelig for fabrikanterne. Disse delegerede retsakter præciserer det krævede tillidsniveau, der skal stå i et rimeligt forhold til det cybersikkerhedsrisikoniveau, der er forbundet med produkter med digitale elementer, og skal tage hensyn til deres tilsigtede formål, herunder den kritiske afhængighed af dem hos væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555.

Inden vedtagelsen af sådanne delegerede retsakter foretager Kommissionen en vurdering af de potentielle markedsvirkninger af de påtænkte foranstaltninger og gennemfører høringer af relevante interessenter, herunder den europæiske cybersikkerhedscertificeringsgruppe, der er oprettet i henhold til forordning (EU) 2019/881. Vurderingen skal tage hensyn til medlemsstaternes parathed og kapacitetsniveau med hensyn til gennemførelsen af den relevante europæiske cybersikkerhedscertificeringsordning. Hvis der ikke er vedtaget delegerede retsakter som omhandlet i nærværende stykkes første afsnit, er produkter med digitale elementer, hvis væsentligste funktionalitet henhører under en produktkategori som fastsat i bilag IV, omfattet af de overensstemmelsesvurderingsprocedurer, der er omhandlet i artikel 32, stk. 3.

De delegerede retsakter, der er omhandlet i første afsnit, fastsætter en mindste overgangsperiode på seks måneder, medmindre en kortere overgangsperiode er berettiget i særligt hastende tilfælde.

2. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 61 med henblik på at ændre bilag IV ved at tilføje eller fjerne kategorier af kritiske produkter med digitale elementer. Ved fastlæggelsen af sådanne kategorier af kritiske produkter med digitale elementer og det krævede tillidsniveau i overensstemmelse med nærværende artikels stk. 1 tager Kommissionen hensyn til de kriterier, der er omhandlet i artikel 7, stk. 2, og sikrer, at kategorierne af produkter med digitale elementer opfylder mindst ét af følgende kriterier:

a) der er en kritisk afhængighed hos væsentlige enheder som omhandlet i artikel 3 i direktiv (EU) 2022/2555 af kategorien af produkter med digitale elementer

b) hændelser og udnyttede sårbarheder vedrørende kategorien af produkter med digitale elementer vil kunne føre til alvorlige forstyrrelser af kritiske forsyningskæder i hele det indre marked.

Inden vedtagelsen af sådanne delegerede retsakter foretager Kommissionen en vurdering af den type, der er omhandlet i stk. 1.

De delegerede retsakter, der er omhandlet i første afsnit, fastsætter en mindste overgangsperiode på seks måneder, medmindre en kortere overgangsperiode er berettiget i særligt hastende tilfælde.

Artikel 9

Høringer af interesserede parter

1. Ved udarbejdelsen af foranstaltninger til gennemførelse af denne forordning hører og tager Kommissionen hensyn til synspunkter fra relevante interessenter såsom relevante myndigheder i medlemsstaterne, virksomheder i den private sektor, herunder mikrovirksomheder og små og mellemstore virksomheder, open source software-samfundet, forbruger-organisationer, den akademiske verden og relevante EU-agenturer og -organer samt ekspertgrupper, der er nedsat på EU-plan. Kommissionen skal navnlig, hvor det er relevant, høre og indhente synspunkter fra disse interessenter på en struktureret måde i forbindelse med:

a) udarbejdelse af den vejledning, der er omhandlet i artikel 26

b) udarbejdelse af de tekniske beskrivelser af produktkategorier fastsat i bilag III i overensstemmelse med artikel 7, stk. 4, vurdering af behovet for potentielle ajourføringer af listen af produktkategorier i overensstemmelse med artikel 7, stk. 3, og artikel 8, stk. 2, eller gennemførelse af vurderingen af den potentielle indvirkning på markedet, der er omhandlet i artikel 8, stk. 1, uden at det berører artikel 61

c) foretagelse af forberedende arbejde med henblik på evaluering og revision af denne forordning.

2. Kommissionen afholder regelmæssige hørings- og informationsmøder, mindst én gang om året, for at indhente synspunkter fra de i stk. 1 omhandlede interessenter om gennemførelsen af denne forordning.

Artikel 10

Forbedring af færdigheder i et cybermodstandsdygtigt digitalt miljø

Med henblik på denne forordning og for at imødekomme fagfolks behov for støtte til gennemførelsen af denne forordning fremmer medlemsstaterne, hvor det er relevant, med støtte fra Kommissionen, Det Europæiske Kompetencecenter for Cybersikkerhed og ENISA, idet de fuldt ud respekterer medlemsstaternes ansvar på uddannelsesområdet, foranstaltninger og strategier, der har til formål at:

a) udvikle færdigheder inden for cybersikkerhed og skabe organisatoriske og teknologiske værktøjer for at sikre tilstrækkelig tilgængelighed af kvalificerede fagfolk med henblik på at støtte markedsovervågningsmyndighedernes og overensstemmelsesvurderingsorganernes aktiviteter

b) øge samarbejdet mellem den private sektor, erhvervsdrivende, herunder gennem omskoling eller opkvalificering af fabrikanternes ansatte, forbrugere, udbydere af uddannelse samt offentlige forvaltninger, hvorved unges muligheder for at få adgang til job i cybersikkerhedssektoren udvides.

Artikel 11

Produktsikkerhed i almindelighed

Uanset artikel 2, stk. 1, tredje afsnit, litra b), i forordning (EU) 2023/988, finder kapitel III, afdeling 1, kapitel V og VII og kapitel IX-XI i nævnte forordning anvendelse på produkter med digitale elementer for så vidt angår aspekter og risici eller kategorier af risici, der ikke er omfattet af nærværende forordning, såfremt disse produkter ikke er omfattet af specifikke sikkerhedskrav i anden »EU-harmoniseringslovgivning« som defineret i artikel 3, nr. 27), i forordning (EU) 2023/988.

Artikel 12

Højrisiko-AI-systemer

1. Uden at dette berører de krav til nøjagtighed og robusthed, der er fastsat i artikel 15 i forordning (EU) 2024/1689, anses produkter med digitale elementer, som er omfattet af nærværende forordnings anvendelsesområde, og som er klassificeret som højrisiko-AI-systemer i henhold til nævnte forordnings artikel 6, for at overholde cybersikkerhedskravene i nævnte forordnings artikel 15, når:

a) disse produkter opfylder de væsentlige cybersikkerhedskrav i bilag I, del I

b) de processer, som fabrikanten har indført, opfylder de væsentlige cybersikkerhedskrav i bilag I, del II, og

c) opnåelsen af det påkrævede niveau af cybersikkerhedsbeskyttelse i henhold til artikel 15 i forordning (EU) 2024/1689 dokumenteres ved en EU-overensstemmelseserklæring udstedt i henhold til nærværende forordning.

2. For de produkter med digitale elementer og cybersikkerhedskrav, der er omhandlet i denne artikels stk. 1, finder den relevante overensstemmelsesvurderingsprocedure i henhold til artikel 43 i forordning (EU) 2024/1689 anvendelse. Med henblik på denne vurdering har bemyndigede organer, der har beføjelse til at kontrollere højrisiko-AI-systemernes overensstemmelse i henhold til forordning (EU) 2024/1689, også beføjelse til at kontrollere, at højrisiko-AI-systemerne, der er omfattet af nærværende forordnings anvendelsesområde, opfylder kravene i bilag I til nærværende forordning, forudsat at disse bemyndigede organers overholdelse af kravene i nærværende forordnings artikel 39 er blevet vurderet i forbindelse med bemyndigelsesproceduren i henhold til forordning (EU) 2024/1689.

3. Uanset denne artikels stk. 2 er vigtige produkter med digitale elementer som opført i bilag III til denne forordning, der er omfattet af overensstemmelsesvurderingsprocedurerne i denne forordnings artikel 32, stk. 2, litra a) og b), og artikel 32, stk. 3, samt kritiske produkter med digitale elementer som opført i bilag IV til denne forordning, som er pålagt at opnå et europæisk cybersikkerhedsattest i henhold til denne forordnings artikel 8, stk. 1, eller, hvis dette ikke er tilfældet, som er genstand for overensstemmelsesvurderingsprocedurerne omhandlet i denne forordnings artikel 32, stk. 3, og som er klassificeret som højrisiko-AI-systemer i henhold til artikel 6 i forordning (EU) 2024/1689, og på hvilke overensstemmelsesvurderingsproceduren baseret på intern kontrol som omhandlet i bilag VI til forordning (EU) 2024/1689 finder anvendelse, omfattet af overensstemmelsesvurderingsprocedurerne fastsat i nærværende forordning for så vidt angår de væsentlige cybersikkerhedskrav i nærværende forordning.

4. Fabrikanter af produkter med digitale elementer som omhandlet i denne artikels stk. 1 kan deltage i de reguleringsmæssige AI-sandkasser, der er omhandlet i artikel 57 i forordning (EU) 2024/1689.

KAPITEL II

ERHVERVSDRIVENDES FORPLIGTELSER OG BESTEMMELSER VEDRØRENDE GRATIS OPEN SOURCE-SOFTware

Artikel 13

Fabrikantens forpligtelser

1. Når et produkt med digitale elementer bringes i omsætning, sikrer fabrikanten, at det er designet, udviklet og produceret i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, del I.

2. Med henblik på at opfylde stk. 1 foretager fabrikanten en vurdering af de cybersikkerhedsrisici, der er forbundet med et produkt med digitale elementer, og tager resultatet af denne vurdering i betragtning i forbindelse med planlægning, design, udvikling, produktion, levering og vedligeholdelse af produktet med digitale elementer for at minimere cybersikkerhedsrisici, forebygge hændelser og minimere deres virkninger, herunder vedrørende brugernes sundhed og sikkerhed.

3. Cybersikkerhedsrisikovurderingen dokumenteres og ajourføres i relevant omfang i løbet af en supportperiode, der skal fastsættes i overensstemmelse med denne artikels stk. 8. Denne cybersikkerhedsrisikovurdering skal som minimum omfatte en analyse af cybersikkerhedsrisici baseret på det tilsigtede formål og den anvendelse, der med rimelighed kan forudses, samt anvendelsesbetingelserne for produktet med digitale elementer såsom driftsmiljøet eller de aktiver, der skal beskyttes, idet der tages højde for, hvor længe produktet forventes at være i brug. Cybersikkerhedsrisikovurderingen skal angive, om og i givet fald på hvilken måde sikkerhedskravene i bilag I, del I, nr. 2, finder anvendelse på det relevante produkt med digitale elementer, og hvordan disse krav gennemføres i overensstemmelse med cybersikkerhedsrisikovurderingen. Det skal også angives, hvordan fabrikanten skal anvende bilag I, del I, nr. 1, og de krav til håndtering af sårbarheder, der er fastsat i bilag I, del II.

4. Når et produkt med digitale elementer bringes i omsætning, medtager fabrikanten den cybersikkerhedsrisikovurdering, der er omhandlet i denne artikels stk. 3, i den tekniske dokumentation, der kræves i henhold til artikel 31 og bilag VII. For produkter med digitale elementer som omhandlet i artikel 12, der også er omfattet af andre EU-retsakter, kan cybersikkerhedsrisikovurderingen indgå i den risikovurdering, der kræves i henhold til disse EU-retsakter. Hvis visse væsentlige cybersikkerhedskrav ikke er relevante for produktet med digitale elementer, medtager fabrikanten en klar begrundelse herfor i den tekniske dokumentation.

5. Med henblik på at opfylde stk. 1 skal fabrikanter foretage due diligence ved integreringen af komponenter fra tredjeparter, således at disse komponenter ikke bringer cybersikkerheden af produktet med digitale elementer i fare, herunder når der integreres komponenter fra gratis open source-software, der ikke er gjort tilgængelige på markedet som led i en kommerciel aktivitet.

6. Ved identifikation af en sårbarhed i en komponent, herunder i en open source-komponent, som er integreret i produktet med digitale elementer, indberetter fabrikanten sårbarheden til den person eller enhed, der fremstiller eller vedligeholder komponenten, og håndterer og afhjælper sårbarheden i overensstemmelse med de krav til håndtering af sårbarheder, der er fastsat i bilag I, del II. Hvis fabrikanten har udviklet en software- eller hardwareændring for at afhjælpe sårbarheden i den pågældende komponent, skal fabrikanten dele den relevante kode eller dokumentation med den person eller enhed, der fremstiller eller vedligeholder komponenten, hvor det er relevant i et maskinlæsbart format.

7. Fabrikanten dokumenterer på en systematisk måde, der står i et rimeligt forhold til cybersikkerhedsrisicienes karakter, relevante cybersikkerhedsaspekter vedrørende produkterne med digitale elementer, herunder sårbarheder, som fabrikanten bliver bekendt med, og alle relevante oplysninger fra tredjeparter, og ajourfører i påkommende tilfælde cybersikkerheds-risikovurderingen af produkterne.

8. Fabrikanten sikrer, når et produkt med digitale elementer bringes i omsætning, og i supportperioden, at det pågældende produkts sårbarheder, herunder dets komponenter, håndteres effektivt og i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, del II.

Fabrikanten fastsætter supportperioden således, at denne afspejler det tidsrum, hvori produktet forventes at være i brug, navnlig under hensyntagen til rimelige brugerforventninger, produktets art, herunder dets tilsigtede formål, samt relevant EU-ret, der fastsætter levetiden for produkter med digitale elementer. Ved fastsættelsen af supportperioden kan fabrikanten også tage hensyn til supportperioderne for produkter med digitale elementer, der tilbyder en lignende funktionalitet, og som er bragt i omsætning af andre fabrikanter, og til tilgængeligheden af driftsmiljøet, supportperioderne for integrerede komponenter, der leverer centrale funktioner og stammer fra tredjeparter, samt relevant vejledning fra den særlige administrative samarbejdsgruppe (ADCO), der er oprettet i henhold til artikel 52, stk. 15, og fra Kommissionen. De forhold, der skal tages hensyn til med henblik på at bestemme f supportperioden, skal overvejes på en måde, der sikrer proportionalitet.

Uden at det berører andet afsnit, skal supportperioden være på mindst fem år. Hvis produktet med digitale elementer forventes at være i brug i mindre end fem år, skal supportperioden svare til den forventede anvendelsestid.

Under hensyntagen til ADCO's henstillinger som omhandlet i artikel 52, stk. 16, kan Kommissionen vedtage delegerede retsakter i overensstemmelse med artikel 61 med henblik på at supplere denne forordning ved at præcisere minimumssupportperioden for specifikke produktkategorier, såfremt markedsovervågningsdataene tyder på utilstrækkelige supportperioder.

Fabrikanten medtager i den tekniske dokumentation de oplysninger, der blev taget i betragtning ved fastlæggelsen af supportperioden for et produkt med digitale elementer, jf. bilag VII.

Fabrikanten indfører passende politikker og procedurer, herunder politikker for koordineret offentliggørelse af sårbarheder, jf. bilag I, del II, nr. 5, til håndtering og afhjælpning af potentielle sårbarheder i produktet med digitale elementer indberettet fra interne eller eksterne kilder.

9. Fabrikanten sikrer, at hver sikkerhedsopdatering, jf. bilag I, del II, nr. 8, som er gjort tilgængelig for brugerne i supportperioden, forbliver tilgængelig efter udstedelsen i mindst ti år eller i resten af supportperioden, alt efter hvilket tidsrum der er længst.

10. Hvis en fabrikant har bragt efterfølgende væsentligt ændrede versioner af et softwareprodukt i omsætning, kan denne fabrikant vælge kun at sikre overholdelse af det væsentlige cybersikkerhedskrav i bilag I, del II, nr. 2, for den version, som fabrikanten senest har bragt i omsætning, forudsat at brugerne af de versioner, der tidligere er bragt i omsætning, har gratis adgang til den version, der senest er bragt i omsætning, og ikke pådrager sig yderligere omkostninger ved tilpasningen af det hardware- og softwaremiljø, hvori de anvender den oprindelige version af det pågældende produkt.

11. Fabrikanten kan opretholde offentlige softwarearkiver, der forbedrer brugernes adgang til historiske versioner. I disse tilfælde skal brugerne på en lettilgængelig måde informeres klart om de risici, der er forbundet med brug af ikkeunderstøttet software.

12. Inden et produkt med digitale elementer bringes i omsætning, udarbejder fabrikanten den tekniske dokumentation, der er omhandlet i artikel 31.

Fabrikanten gennemfører eller får gennemført de valgte overensstemmelsesvurderingsprocedurer som omhandlet i artikel 32.

Hvor det ved en af disse overensstemmelsesvurderingsprocedurer er blevet dokumenteret, at produktet med digitale elementer overholder de væsentlige cybersikkerhedskrav i bilag I, del I, og at de processer, som fabrikanten har indført, overholder de væsentlige cybersikkerhedskrav i bilag I, del II, udarbejder fabrikanten EU-overensstemmelseserklæringen i overensstemmelse med artikel 28 og anbringer CE-mærkningen i overensstemmelse med artikel 30.

13. Fabrikanten opbevarer den tekniske dokumentation og EU-overensstemmelseserklæringen, så de i mindst ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst, står til rådighed for markedsovervågningsmyndighederne.

14. Fabrikanten sikrer, at der findes procedurer til sikring af, at produkter med digitale elementer, der er del af en produktionsserie, fortsat er i overensstemmelse med denne forordning. Fabrikanten tager behørigt hensyn til ændringer i udviklings- og produktionsprocessen eller i designet eller egenskaberne af produktet med digitale elementer og til ændringer i de harmoniserede standarder, europæiske cybersikkerhedscertificeringsordninger eller fælles specifikationer som omhandlet i artikel 27, som der henvises til for at dokumentere overensstemmelsen af produktet med digitale elementer med de gældende krav, eller som anvendes til at kontrollere produktets overensstemmelse.

15. Fabrikanten sikrer, at dennes produkter med digitale elementer er forsynet med et type-, parti- eller serienummer eller en anden form for angivelse, ved hjælp af hvilken de kan identificeres, eller, hvis dette ikke er muligt, at disse oplysninger fremgår af emballagen eller af et dokument, der ledsager produktet med digitale elementer.

16. Fabrikantens navn, registrerede firmanavn eller registrerede varemærke og postadresse, e-mailadresse eller andre digitale kontaktoplysninger samt, i givet fald, webstedet, hvorpå fabrikanten kan kontaktes, skal fremgå af produktet med digitale elementer, af emballagen eller af et dokument, der ledsager produktet med digitale elementer. Disse oplysninger skal også indgå i de oplysninger og anvisninger til brugeren, der er anført i bilag II. Kontaktoplysningerne gives på et sprog, der er letforståeligt for brugere og markedsovervågningsmyndigheder.

17. Med henblik på denne forordning udpeger fabrikanten et centralt kontaktpunkt, der gør det muligt for brugerne at kommunikere direkte og hurtigt med denne, herunder for at lette indberetningen af sårbarheder i produktet med digitale elementer.

Fabrikanten sikrer, at det centrale kontaktpunkt er let at identificere for brugerne. Oplysninger om det centrale kontaktpunkt skal også indgå i de oplysninger og anvisninger til brugeren, der er anført i bilag II.

Det centrale kontaktpunkt skal give brugerne mulighed for at vælge deres foretrukne kommunikationsmiddel og må ikke begrænse sådanne midler til automatiserede værktøjer.

18. Fabrikanten sikrer, at produkter med digitale elementer ledsages af de oplysninger og anvisninger til brugeren, der er anført i bilag II, i papirform eller i elektronisk form. Sådanne oplysninger og anvisninger skal gives på et sprog, der let kan forstås af brugerne og markedsovervågningsmyndighederne. De skal være klare, forståelige og læselige. De skal muliggøre sikker installation, drift og anvendelse af produkter med digitale elementer. Fabrikanten opbevarer de oplysninger og anvisninger til brugeren, der er anført i bilag II, så de i mindst ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst, står til rådighed for de nationale markedsovervågningsmyndigheder. Hvis sådanne oplysninger og anvisninger gives online, sikrer fabrikanten, at de er tilgængelige, brugervenlige og til rådighed online i mindst ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst.

19. Fabrikanten sikrer, at slutdatoen for den supportperiode, der er omhandlet i stk. 8, herunder som minimum måneden og året, er klart og forståeligt angivet på købstidspunktet på en lettilgængelig måde og, i givet fald, på produktet med digitale elementer eller dets emballage eller ved hjælp af digitale midler.

Hvis det er teknisk muligt i lyset af arten af produktet med digitale elementer, skal fabrikanten vise en meddelelse til brugerne om, at deres produkt med digitale elementer har nået slutningen af sin supportperiode.

20. Fabrikanten udleverer enten en kopi af EU-overensstemmelseserklæringen eller en forenklet EU-overensstemmelseserklæring sammen med produktet med digitale elementer. Såfremt en forenklet EU-overensstemmelseserklæring udleveres, skal denne indeholde den nøjagtige internetadresse, hvor den fuldstændige EU-overensstemmelseserklæring kan tilgås.

21. Fra tidspunktet hvor et produkt med digitale elementer er bragt i omsætning og i supportperioden, træffer fabrikanten, hvis vedkommende ved eller har grund til at tro, at produktet med digitale elementer eller de processer, som fabrikanten har indført, ikke er i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, omgående de nødvendige korrigerende foranstaltninger til at bringe produktet med digitale elementer eller fabrikantens processer i overensstemmelse eller til at tilbagetrække eller tilbagekalde produktet, c.

22. Efter en markedsovervågningsmyndigheds begrundede anmodning giver fabrikanten denne myndighed alle de oplysninger og al den dokumentation på papir eller elektronisk, som er nødvendig for at dokumentere, at produkterne med digitale elementer og de processer, der er indført af fabrikanten, er i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, på et for denne myndighed letforståeligt sprog. Hvis denne myndighed anmoder herom, samarbejder fabrikanten med myndigheden om foranstaltninger, der træffes for at eliminere de cybersikkerhedsrisici, som det produkt med digitale elementer, fabrikanten har bragt i omsætning, indebærer.

23. En fabrikant, der indstiller driften og derfor ikke er i stand til at opfylde denne forordning, underretter, inden indstillingen af driften får virkning, de relevante markedsovervågningsmyndigheder om denne situation samt på enhver tilgængelig måde og i videst muligt omfang brugerne af de relevante produkter med digitale elementer, der er bragt i omsætning, om den forestående indstilling af driften.

24. Kommissionen kan ved hjælp af gennemførelsesretsakter, der tager hensyn til europæiske eller internationale standarder og bedste praksis, præcisere formatet for og elementerne i den softwarekomponentliste, der er omhandlet i bilag I, del II, nr. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 62, stk. 2.

25. For at vurdere medlemsstaternes og hele Unionens afhængighed af softwarekomponenter og navnlig af komponenter, der kan betegnes som gratis open source-software, kan ADCO beslutte at foretage en EU-dækkende afhængighedsvurdering for specifikke kategorier af produkter med digitale elementer. Med henblik herpå kan markedsovervågningsmyndighederne anmode fabrikanter af sådanne kategorier af produkter med digitale elementer om at udlevere den relevante softwarekomponentliste som omhandlet i bilag I, del II, nr. 1. På grundlag af sådanne oplysninger kan markedsovervågningsmyndighederne give ADCO anonymiserede og aggregerede oplysninger om softwareafhængighed. ADCO forelægger en rapport om resultaterne af afhængighedsvurderingen for den samarbejdsgruppe, der er oprettet i henhold til artikel 14 i direktiv (EU) 2022/2555.

Artikel 14

Fabrikantens rapporteringsforpligtelser

1. En fabrikant underretter samtidig den CSIRT, der er udpeget som koordinator i overensstemmelse med denne artikels stk. 7, og ENISA om enhver aktivt udnyttet sårbarhed i produktet med digitale elementer, som fabrikanten får kendskab til. Fabrikanten underretter om den aktivt udnyttede sårbarhed via den fælles indberetningsplatform, der er oprettet i henhold til artikel 16.

2. Med henblik på den underretning, der er omhandlet i stk. 1, indgiver fabrikanten:

a) en tidlig varsling om en aktivt udnyttet sårbarhed uden unødigt ophold og under alle omstændigheder senest 24 timer efter, at fabrikanten har fået kendskab hertil, i givet fald med angivelse af de medlemsstater, på hvis område fabrikanten er bekendt med, at dennes produkt med digitale elementer er gjort tilgængeligt

b) medmindre de relevante oplysninger allerede er afgivet, en meddelelse om sårbarhed uden unødigt ophold og under alle omstændigheder senest 72 timer efter, at fabrikanten har fået kendskab til den aktivt udnyttede sårbarhed, hvilken meddelelse skal indeholde generelle oplysninger, i det omfang sådanne foreligger, om det pågældende produkt med digitale elementer, den generelle karakter af udnyttelsen og den pågældende sårbarhed samt eventuelle korrigerende eller afbødende foranstaltninger, der er truffet, og korrigerende eller afbødende foranstaltninger, som brugerne kan træffe, og som i givet fald også angiver, hvor følsomme fabrikanten vurderer de meddelte oplysninger at være

c) medmindre de relevante oplysninger allerede er afgivet, en endelig rapport senest 14 dage efter, at en korrigerende eller afbødende foranstaltning bliver tilgængelig, der som minimum indeholder følgende:

   i) en beskrivelse af sårbarheden, herunder dens alvor og indvirkning

   ii) oplysninger om eventuelle ondsindede aktører, der har udnyttet eller udnytter sårbarheden, hvis sådanne oplysninger foreligger

   iii) oplysninger om sikkerhedsopdateringen eller andre korrigerende foranstaltninger, der er gjort tilgængelige for at afhjælpe sårbarheden.

3. En fabrikant underretter samtidig den CSIRT, der er udpeget som koordinator i overensstemmelse med denne artikels stk. 7, og ENISA, om enhver alvorlig hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer, som fabrikanten får kendskab til. Fabrikanten underretter om hændelsen via den fælles indberetningsplatform, der er oprettet i henhold til artikel 16.

4. Med henblik på den underretning, der er omhandlet i stk. 3, indgiver fabrikanten:

a) en tidlig varsling om en alvorlig hændelse, der indvirker på sikkerheden af produktet med digitale elementer, uden unødigt ophold og under alle omstændigheder senest 24 timer efter, at fabrikanten har fået kendskab hertil, herunder som minimum om, hvorvidt fabrikanten har mistanke om at hændelsen skyldes ulovlige eller ondsindede handlinger, og i givet fald med angivelse af de medlemsstater, på hvis område fabrikanten er bekendt med, at dennes produkt med digitale elementer er blevet gjort tilgængeligt

b) medmindre de relevante oplysninger allerede er afgivet, en underretning om en hændelse uden unødigt ophold og under alle omstændigheder senest 72 timer efter, at fabrikanten har fået kendskab til hændelsen, med generelle oplysninger, hvis sådanne foreligger, om arten af hændelsen, en indledende vurdering af hændelsen samt eventuelle korrigerende eller afbødende foranstaltninger, der er truffet, og korrigerende eller afbødende foranstaltninger, som brugerne kan træffe, og som også, i givet fald, angiver, hvor følsomme fabrikanten vurderer de meddelte oplysninger at være

c) medmindre de relevante oplysninger allerede er afgivet, en endelig rapport senest en måned efter indgivelsen af den i litra b) omhandlede underretning om en hændelse, der som minimum omfatter følgende:

   i) en detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning

   ii) den type trussel eller grundlæggende årsag, der sandsynligvis udløste hændelsen

   iii) anvendte og igangværende afbødende foranstaltninger.

5. Med henblik på stk. 3 anses en hændelse, der indvirker på sikkerheden af produktet med digitale elementer, for at være alvorlig, hvis:

a) den indvirker eller kan indvirke negativt på evnen til at beskytte tilgængeligheden, autenticiteten, integriteten eller fortroligheden af følsomme eller vigtige data eller funktioner, eller

b) den har ført til eller er i stand til at føre til indførelse eller udførelse af ondsindet kode i et produkt med digitale elementer eller i net- og informationssystemer hos en bruger af produktet med digitale elementer.

6. Hvis det er nødvendigt, kan den CSIRT, der er udpeget som koordinator, og som indledningsvist modtager underretningen, anmode fabrikanten om at forelægge en foreløbig rapport om relevante statusopdateringer om den aktivt udnyttede sårbarhed eller alvorlige hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer.

7. De underretninger, der er omhandlet i denne artikels stk. 1 og 3, indgives via den fælles indberetningsplatform, der er omhandlet i artikel 16, ved hjælp af et af de adgangspunkter for elektronisk underretning, der er omhandlet i artikel 16, stk. 1. Underretningen indgives ved hjælp af adgangspunktet for elektronisk underretning i den CSIRT, der er udpeget som koordinator i den medlemsstat, hvor fabrikanten har sit hovedforretningssted i Unionen, og skal samtidig være tilgængelig for ENISA.

Med henblik på denne forordning anses en fabrikant for at have sit hovedforretningssted i Unionen i den medlemsstat, hvor beslutningerne vedrørende cybersikkerheden af fabrikantens produkter med digitale elementer overvejende træffes. Hvis en sådan medlemsstat ikke kan fastslås, anses hovedforretningsstedet for at være i den medlemsstat, hvor den pågældende fabrikant forretningssted med det største antal ansatte i Unionen er beliggende.

Hvis en fabrikant ikke har noget hovedforretningssted i Unionen, indgiver denne de underretninger, der er omhandlet i stk. 1 og 3, ved hjælp af adgangspunktet for elektronisk underretning i den CSIRT, der er udpeget som koordinator i den medlemsstat, der er fastsat i henhold til følgende rækkefølge og på grundlag af de oplysninger, som fabrikanten har til rådighed:

a) den medlemsstat, hvor den bemyndigede repræsentant, som handler på fabrikantens vegne for det største antal produkter med digitale elementer fra den pågældende fabrikant, er etableret

b) den medlemsstat, hvor den importør, som bringer det største antal produkter med digitale elementer fra den pågældende fabrikant i omsætning, er etableret

c) den medlemsstat, hvor den distributør, som bringer det største antal produkter med digitale elementer fra den pågældende fabrikant i omsætning, er etableret

d) den medlemsstat, hvor det største antal brugere af produkter med digitale elementer fra den pågældende fabrikant befinder sig.

For så vidt angår tredje afsnit, litra d), kan en fabrikant indgive underretninger vedrørende enhver efterfølgende aktivt udnyttet sårbarhed eller alvorlig hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer, til den samme CSIRT, der er udpeget som koordinator, og til hvem fabrikanten indberettede i første omgang.

8. Efter at have fået kendskab til en aktivt udnyttet sårbarhed eller en alvorlig hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer, underretter fabrikanten de berørte brugere af produktet med digitale elementer og, hvor det er relevant, alle brugere om denne sårbarhed eller hændelse, og om nødvendigt om eventuel risikobegrænsning og eventuelle korrigerende foranstaltninger, som brugerne kan træffe for at afbøde virkningen af den pågældende sårbarhed eller hændelse, hvor det er relevant i et struktureret maskinlæsbart format, der er let automatisk bearbejdeligt. Hvis fabrikanten ikke rettidigt oplyser brugerne af produktet med digitale elementer, kan de underrettede CSIRT'er, der er udpeget som koordinatorer, give brugerne sådanne oplysninger, når dette anses for at være forholdsmæssigt og nødvendigt for at forebygge eller afbøde virkningen af den pågældende sårbarhed eller hændelse.

9. Senest den 11. december 2025 vedtager Kommissionen delegerede retsakter i overensstemmelse med denne forordnings artikel 61 med henblik på at supplere denne forordning ved at præcisere vilkårene og betingelserne for anvendelse af de cybersikkerhedsrelaterede grunde i forbindelse med udsættelse af formidlingen af underretninger som omhandlet i denne forordnings artikel 16, stk. 2. Kommissionen samarbejder med CSIRT-netværket oprettet i henhold til artikel 15 i direktiv (EU) 2022/2555 og ENISA om udarbejdelsen af udkastene til delegerede retsakter.

10. Kommissionen kan ved hjælp af gennemførelsesretsakter yderligere præcisere formatet og procedurerne for de underretninger, der er omhandlet i denne artikel samt i artikel 15 og 16. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 62, stk. 2. Kommissionen samarbejder med CSIRT-netværket og ENISA om udarbejdelsen af disse udkast til gennemførelsesretsakter.

Artikel 15

Frivillig indberetning

1. Fabrikanter såvel som andre fysiske eller juridiske personer kan på frivillig basis underrette en CSIRT, der er udpeget som koordinator, eller ENISA, om enhver sårbarhed i et produkt med digitale elementer samt om cybertrusler, der kan påvirke risikoprofilen for et produkt med digitale elementer.

2. Fabrikanter såvel som andre fysiske eller juridiske personer kan på frivillig basis underrette en CSIRT, der er udpeget som koordinator, eller ENISA, om enhver hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer, samt nærvedhændelser, som kunne have resulteret i en sådan hændelse.

3. Den CSIRT, der er udpeget som koordinator, eller ENISA behandler de underretninger, der er omhandlet i denne artikels stk. 1 og 2, i overensstemmelse med proceduren i artikel 16.

Den CSIRT, der er udpeget som koordinator, kan prioritere behandlingen af obligatoriske underretninger frem for frivillige underretninger.

4. Hvis en anden fysisk eller juridisk person end fabrikanten indberetter en aktivt udnyttet sårbarhed eller en alvorlig hændelse, der har indvirkning på sikkerheden af et produkt med digitale elementer, i overensstemmelse med stk. 1 eller 2, skal den CSIRT, der er udpeget som koordinator, uden unødigt ophold underrette fabrikanten.

5. De CSIRT'er, der er udpeget som koordinatorer, såvel som ENISA sikrer fortroligheden og den passende beskyttelse af de oplysninger, der afgives af en fysisk eller juridisk person. Uden at det berører forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, må frivillig indberetning ikke medføre, at en underrettende fysisk eller juridisk person pålægges nogen yderligere forpligtelser, som vedkommende ikke ville være underlagt, hvis den ikke havde foretaget underretningen.

Artikel 16

Oprettelse af en fælles indberetningsplatform

1. Med henblik på de underretninger, der er omhandlet i artikel 14, stk. 1 og 3, og artikel 15, stk. 1 og 2, og for at forenkle fabrikanters indberetningsforpligtelser, opretter ENISA en fælles indberetningsplatform. Den daglige drift af denne fælles indberetningsplatform forvaltes og vedligeholdes af ENISA. Arkitekturen for den fælles indberetningsplatform skal gøre det muligt for medlemsstaterne og ENISA at indføre deres egne adgangspunkter for elektronisk underretning.

2. Efter at have modtaget en underretning formidler den CSIRT, der er udpeget som koordinator, og som indledningsvist modtager underretningen, straks meddelelsen via den fælles indberetningsplatform til de CSIRT'er, der er udpeget som koordinatorer på det område, hvor fabrikanten har angivet, at produktet med digitale elementer er blevet gjort tilgængeligt.

Under ekstraordinære omstændigheder og navnlig efter anmodning fra fabrikanten og i lyset af følsomhedsgraden af de indberettede oplysninger som angivet af fabrikanten i henhold til denne forordnings artikel 14, stk. 2, litra a), kan formidlingen af underretningen udsættes på grundlag af begrundede cybersikkerhedsrelaterede grunde i en periode, der er strengt nødvendig, herunder hvis en sårbarhed er omfattet af en koordineret procedure for offentliggørelse af sårbarheder som omhandlet i artikel 12, stk. 1, i direktiv (EU) 2022/2555. Hvis en CSIRT beslutter at tilbageholde en underretning, underretter den omgående ENISA om denne beslutning og giver en begrundelse for tilbageholdelsen af underretningen såvel som en angivelse af, hvornår den vil formidle underretningen i overensstemmelse med den formidlingsprocedure, der er fastsat i nærværende stykke. ENISA kan støtte CSIRT'en for så vidt angår anvendelsen af cybersikkerhedsrelaterede grunde i forbindelse med udsættelse af underretningens formidling.

Under særlige ekstraordinære omstændigheder, hvor fabrikanten i den underretning, der er omhandlet i artikel 14, stk. 2, litra b), anfører:

a) at den anmeldte sårbarhed er blevet aktivt udnyttet af en ondsindet aktør, og at den ifølge de foreliggende oplysninger ikke er blevet udnyttet i nogen anden medlemsstat end den, hvor den CSIRT, der er udpeget som koordinator, befinder sig, og til hvem fabrikanten har anmeldt sårbarheden

b) at enhver øjeblikkelig yderligere formidling af den anmeldte sårbarhed sandsynligvis vil føre til afgivelse af oplysninger, hvis offentliggørelse vil stride mod den pågældende medlemsstats væsentlige interesser, eller

c) at den anmeldte sårbarhed udgør en overhængende høj cybersikkerhedsrisiko som følge af den videre formidling

er det kun oplysningerne om, at fabrikanten har foretaget en underretning, de generelle oplysninger om produktet, oplysningerne om den generelle karakter af den udnyttede sårbarhed og oplysninger om, at der blev gjort opmærksom på sikkerhedsrelaterede grunde, som skal stilles til rådighed samtidig for ENISA, indtil den fuldstændige underretning formidles til de pågældende CSIRT'er og til ENISA. Hvis ENISA på grundlag af disse oplysninger finder, at der er tale om en systemisk risiko, der indvirker på sikkerheden i det indre marked, anbefaler ENISA den modtagende CSIRT at formidle den fuldstændige underretning til de andre CSIRT'er, der er udpeget som koordinatorer, og til ENISA selv.

3. Efter at have modtaget en underretning om en aktivt udnyttet sårbarhed i et produkt med digitale elementer eller om en alvorlig hændelse, der har indvirkning på sikkerheden af et produkt med digitale elementer, giver de CSIRT'er, der er udpeget som koordinatorer, markedsovervågningsmyndighederne i deres respektive medlemsstater de indberettede oplysninger, der er nødvendige for, at markedsovervågningsmyndighederne kan opfylde deres forpligtelser i henhold til denne forordning.

4. ENISA træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at håndtere sikkerhedsrisiciene for den fælles indberetningsplatform og de oplysninger, der indgives eller formidles via den fælles indberetningsplatform. Det underretter uden unødigt ophold CSIRT-netværket og Kommissionen om enhver sikkerhedshændelse, der har indvirkning på den fælles indberetningsplatform.

5. ENISA udarbejder og gennemfører i samarbejde med CSIRT-netværket specifikationer for de tekniske, operationelle og organisatoriske foranstaltninger vedrørende oprettelse, vedligeholdelse og sikker drift af den fælles indberetningsplatform, der er omhandlet i stk. 1, herunder som minimum sikkerhedsordningerne vedrørende oprettelse, drift og vedligeholdelse af den fælles indberetningsplatform samt de adgangspunkter for elektronisk underretning, som er oprettet af de CSIRT'er, der er udpeget som koordinatorer på nationalt plan, og ENISA på EU-plan, herunder proceduremæssige aspekter, så det i tilfælde, hvor der for en anmeldt sårbarhed ikke er nogen korrigerende eller afbødende foranstaltninger, sikres, at oplysninger om denne sårbarhed deles i overensstemmelse med strenge sikkerhedsprotokoller og på need-to-know-basis.

6. Hvis en CSIRT, der er udpeget som koordinator, er blevet gjort opmærksom på en aktivt udnyttet sårbarhed som led i en koordineret procedure for offentliggørelse af sårbarheder som omhandlet i artikel 12, stk. 1, i direktiv (EU) 2022/2555, kan den CSIRT, der er udpeget som koordinator, og som indledningsvist modtager underretningen, på grundlag af begrundede cybersikkerhedsrelaterede grunde udsætte formidlingen af den relevante underretning via den fælles indberetningsplatform i en periode, der ikke er længere, end hvad der er strengt nødvendigt, og indtil de involverede parter, der foretager koordineret offentliggørelse af sårbarheder, har givet deres samtykke til offentliggørelse. Dette krav forhindrer ikke fabrikanten i at anmelde en sådan sårbarhed på frivillig basis i overensstemmelse med proceduren i nærværende artikel.

Artikel 17

Andre bestemmelser vedrørende indberetning

1. ENISA kan forelægge det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe), der er oprettet ved artikel 16 i direktiv (EU) 2022/2555, oplysninger, der er meddelt i henhold til denne forordnings artikel 14, stk. 1 og 3, og artikel 15, stk. 1 og 2, hvis sådanne oplysninger er relevante for den koordinerede forvaltning af omfattende cybersikkerhedshændelser og -kriser på operationelt plan. Med henblik på at fastslå en sådan relevans kan ENISA overveje tekniske analyser udført af CSIRT-netværket, hvis sådanne foreligger.

2. Hvor offentlighedens kendskab er nødvendig for at forebygge eller afbøde en alvorlig hændelse, der har indvirkning på sikkerheden af produktet med digitale elementer, eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af hændelsen på anden vis er i den offentlige interesse, kan den CSIRT, der er udpeget som koordinator i den relevante medlemsstat, efter høring af den pågældende fabrikant og, hvor det er relevant, i samarbejde med ENISA, informere offentligheden om hændelsen eller kræve, at fabrikanten gør det.

3. ENISA udarbejder på grundlag af de underretninger, der er modtaget i henhold til denne forordnings artikel 14, stk. 1 og 3, og artikel 15, stk. 1 og 2, hver 24. måned en teknisk rapport om nye tendenser med hensyn til cybersikkerhedsrisici forbundet med produkter med digitale elementer og forelægger den for den samarbejdsgruppe, der er nedsat i henhold til artikel 14 i direktiv (EU) 2022/2555. Den første rapport forelægges senest 24 måneder efter datoen for anvendelsen af forpligtelserne i denne forordnings artikel 14, stk. 1 og 3. ENISA medtager relevante oplysninger fra sine tekniske rapporter i sin rapport om cybersikkerhedssituationen i Unionen i henhold til artikel 18 i direktiv (EU) 2022/2555.

4. Underretningen i sig selv i henhold til artikel 14, stk. 1 og 3, eller artikel 15, stk. 1 og 2, medfører ikke et øget ansvar for den underrettende fysiske eller juridiske person.

5. Når en sikkerhedsopdatering eller en anden form for korrigerende eller afbødende foranstaltning er tilgængelig, tilføjer ENISA efter aftale med fabrikanten af det pågældende produkt med digitale elementer den offentligt kendte sårbarhed, der er meddelt i henhold til denne forordnings artikel 14, stk. 1, eller artikel 15, stk. 1, til den europæiske sårbarhedsdatabase, der er oprettet i henhold til artikel 12, stk. 2, i direktiv (EU) 2022/2555.

6. De CSIRT'er, der er udpeget som koordinatorer, yder i forbindelse med rapporteringsforpligtelserne i henhold til artikel 14 helpdesk-støtte til fabrikanter, og navnlig til fabrikanter, der er mikrovirksomheder eller små eller mellemstore virksomheder.

Artikel 18

Bemyndigede repræsentanter

1. En fabrikant kan via en skriftlig fuldmagt udpege en bemyndiget repræsentant.

2. Forpligtelserne i artikel 13, stk. 1-11, stk. 12, første afsnit, og stk. 14, er ikke en del af den bemyndigede repræsentants fuldmagt.

3. En bemyndiget repræsentant udfører de opgaver, der er angivet i den fuldmagt, denne har modtaget fra fabrikanten. Den bemyndigede repræsentant forelægger på anmodning den kompetente myndighed en kopi af fuldmagten. Fuldmagten skal som minimum sætte den bemyndigede repræsentant i stand til:

a) at opbevare den i artikel 28 omhandlede EU-overensstemmelseserklæring og den i artikel 31 omhandlede tekniske dokumentation, så den i mindst ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst, står til rådighed for de nationale markedsovervågningsmyndigheder

b) på grundlag af en markedsovervågningsmyndigheds begrundede anmodning at give den al den information og dokumentation, der er nødvendig for at dokumentere, at produktet med digitale elementer er i overensstemmelse med kravene

c) at samarbejde med markedsovervågningsmyndighederne, hvis disse anmoder herom, om tiltag, der træffes for at undgå risici, som et produkt med digitale elementer, der er omfattet af den bemyndigede repræsentants fuldmagt, udgør.

Artikel 19

Importørens forpligtelser

1. Importøren må kun bringe produkter med digitale elementer, der opfylder de væsentlige cybersikkerhedskrav i bilag I, del I„ og hvor de processer, der er indført af fabrikanten, overholder de væsentlige cybersikkerhedskrav i bilag I, del II, i omsætning.

2. Importøren sikrer, før denne bringer et produkt med digitale elementer i omsætning, at:

a) fabrikanten har gennemført de relevante overensstemmelsesvurderingsprocedurer som omhandlet i artikel 32

b) fabrikanten har udarbejdet den tekniske dokumentation

c) produktet med digitale elementer er forsynet med den i artikel 30 omhandlede CE-mærkning og er ledsaget af EU-overensstemmelseserklæringen som omhandlet i artikel 13, stk. 20, og oplysningerne og anvisningerne til brugerne anført i bilag II på et for brugerne og markedsovervågningsmyndighederne letforståeligt sprog

d) fabrikanten har opfyldt kravene i artikel 13, stk. 15, 16 og 19.

Med henblik på dette stykke skal importører kunne fremlægge de nødvendige dokumenter som bevis for, at kravene i denne artikel er opfyldt.

3. Hvis en importør finder eller har grund til at tro, at et produkt med digitale elementer eller de processer, som fabrikanten har indført, ikke er i overensstemmelse med denne forordning, må importøren ikke bringe produktet i omsætning, før produktet eller de processer, som fabrikanten har indført, er blevet bragt i overensstemmelse med denne forordning. Hvis produktet med digitale elementer udgør en væsentlig cybersikkerhedsrisiko, underretter importøren endvidere fabrikanten og markedsovervågningsmyndighederne herom.

Hvis en importør har grund til at tro, at et produkt med digitale elementer kan udgøre en betydelig cybersikkerhedsrisiko i lyset af ikketekniske risikofaktorer, underretter importøren markedsovervågningsmyndighederne herom. Efter modtagelse af sådanne oplysninger følger markedsovervågningsmyndighederne de procedurer, der er omhandlet i artikel 54, stk. 2.

4. Importørens navn, registrerede firmanavn eller registrerede varemærke, postadresse, e-mailadresse eller anden digital kontakt samt, hvor det er relevant, det websted, hvor vedkommende kan kontaktes, skal fremgå af produktet med digitale elementer eller af emballagen eller af et dokument, der ledsager produktet med digitale elementer. Kontaktoplysningerne angives på et for brugere og markedsovervågningsmyndigheder letforståeligt sprog.

5. Hvis importøren ved eller har grund til at tro, at et produkt med digitale elementer, som importøren har bragt i omsætning, ikke er i overensstemmelse med denne forordning, træffer importøren omgående de nødvendige korrigerende foranstaltninger til at sikre, at produktet med digitale elementer bringes i overensstemmelse med denne forordning, eller til at tilbagetrække eller tilbagekalde produktet, hvis det er relevant.

Når importøren bliver bekendt med en sårbarhed i produktet med digitale elementer, underretter importøren uden unødigt ophold fabrikanten om denne sårbarhed. Hvis produktet med digitale elementer udgør en væsentlig cybersikkerhedsrisiko, underretter importøren endvidere omgående markedsovervågningsmyndighederne i de medlemsstater, hvor importøren har gjort produktet med digitale elementer tilgængeligt på markedet, herom og giver nærmere oplysninger, navnlig om den manglende overholdelse og om de trufne afhjælpende foranstaltninger.

6. Importøren opbevarer i mindst ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst, en kopi af EU-overensstemmelseserklæringen, så den står til rådighed for markedsovervågningsmyndighederne, og sikrer, at den tekniske dokumentation kan stilles til rådighed for disse myndigheder, hvis de anmoder herom.

7. Efter en markedsovervågningsmyndigheds begrundede anmodning giver importøren denne myndighed alle de oplysninger og al den dokumentation på papir eller elektronisk, som er nødvendig for at dokumentere, at produkterne med digitale elementer er i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, del I, og at de processer, der er indført af fabrikanten, er i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, del II, på et for denne

myndighed letforståeligt sprog. Hvis denne myndighed anmoder herom, samarbejder importøren med myndigheden om foranstaltninger, der træffes for at eliminere de cybersikkerhedsrisici, som et produkt med digitale elementer, importøren har bragt i omsætning, indebærer.

8. Hvor importøren af et produkt med digitale elementer bliver bekendt med, at fabrikanten af det pågældende produkt har indstillet driften og derfor ikke er i stand til at opfylde de forpligtelser, der er fastsat i denne forordning, underretter importøren de relevante markedsovervågningsmyndigheder om denne situation samt, på enhver tilgængelig måde og i videst muligt omfang, brugerne af produkterne med digitale elementer, der er bragt i omsætning.

Artikel 20

Distributørens forpligtelser

1. Distributøren skal, når denne gør et produkt med digitale elementer tilgængeligt på markedet, handle med fornøden omhu for så vidt angår kravene i denne forordning.

2. Inden et produkt med digitale elementer gøres tilgængeligt på markedet, kontrollerer distributøren, at:

a) produktet med digitale elementer er forsynet med CE-mærkning

b) fabrikanten og importøren har opfyldt forpligtelserne i artikel 13, stk. 15, 16, 18, 19 og 20, og artikel 19, stk. 4, og har afgivet alle nødvendige dokumenter til distributøren.

3. Hvis en distributør på baggrund af oplysninger i vedkommendes besiddelse finder eller har grund til at tro, at et produkt med digitale elementer eller de processer, der er indført af fabrikanten, ikke er i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, må distributøren ikke gøre produktet med digitale elementer tilgængeligt på markedet, før det pågældende produkt eller de processer, som fabrikanten har indført, er blevet bragt i overensstemmelse med denne forordning. Hvis produktet med digitale elementer udgør en væsentlig cybersikkerhedsrisiko, underretter distributøren endvidere uden unødigt ophold markedsovervågningsmyndighederne herom.

4. Hvis distributøren på baggrund af oplysninger i vedkommendes besiddelse ved eller har grund til at tro, at et produkt med digitale elementer, som distributøren har gjort tilgængeligt på markedet, eller de processer, der er indført af fabrikanten, ikke er i overensstemmelse med denne forordning, træffer distributøren de nødvendige korrigerende foranstaltninger til at bringe produktet med digitale elementer eller de processer, som fabrikanten har indført, i overensstemmelse eller til at tilbagetrække eller tilbagekalde produktet, hvis det er relevant.

Når distributøren bliver bekendt med en sårbarhed i produktet med digitale elementer, underretter distributøren uden unødigt opholde fabrikanten om denne sårbarhed. Hvis produktet med digitale elementer udgør en væsentlig cybersikkerhedsrisiko, underretter distributøren endvidere omgående markedsovervågningsmyndighederne i de medlemsstater, hvor distributøren har gjort produktet med digitale elementer tilgængeligt på markedet, herom og giver nærmere oplysninger, navnlig om den manglende overholdelse og de trufne afhjælpende foranstaltninger.

5. Efter en markedsovervågningsmyndigheds begrundede anmodning giver distributøren denne myndighed alle de oplysninger og al den dokumentation på papir eller elektronisk, som er nødvendig for at dokumentere, at produkterne med digitale elementer og de processer, der er indført af fabrikanten, er i overensstemmelse med denne forordning, på et for denne myndighed letforståeligt sprog. Hvis denne myndighed anmoder herom, samarbejder distributøren med myndigheden om foranstaltninger, der træffes for at eliminere de cybersikkerhedsrisici, som et produkt med digitale elementer, distributøren har gjort tilgængeligt på markedet, indebærer.

6. Når distributøren af et produkt med digitale elementer på baggrund af oplysninger i vedkommendes besiddelse bliver bekendt med, at fabrikanten af det pågældende produkt har indstillet driften og derfor ikke er i stand til at opfylde de forpligtelser, der er fastsat i denne forordning, underretter distributøren uden unødigt ophold de relevante markedsovervågningsmyndigheder om denne situation samt, på enhver tilgængelig måde og i videst muligt omfang, brugerne af produkterne med digitale elementer, der er bragt i omsætning.

Artikel 21

Tilfælde, hvor fabrikantens forpligtelser finder anvendelse på importører og distributører

En importør eller distributør anses for at være fabrikant i denne forordnings forstand og er omfattet af artikel 13 og 14, hvor denne importør eller distributør bringer et produkt med digitale elementer i omsætning under sit navn eller varemærke eller foretager en væsentlig ændring af et produkt med digitale elementer, der allerede er bragt i omsætning.

Artikel 22

Andre tilfælde, hvor fabrikantens forpligtelser finder anvendelse

1. En fysisk eller juridisk person, bortset fra fabrikanten, importøren eller distributøren, som foretager en væsentlig ændring af et produkt med digitale elementer og bringer dette produkt i omsætning, anses for at være fabrikant i denne forordnings forstand.

2. Den person, der er omhandlet i denne artikels stk. 1, er underlagt forpligtelserne i artikel 13 og 14 for den del af produktet med digitale elementer, der berøres af den væsentlige ændring, eller, hvis den væsentlige ændring har indvirkning på cybersikkerheden af produktet med digitale elementer som helhed, for hele produktet.

Artikel 23

Identifikation af erhvervsdrivende

1. Erhvervsdrivende giver efter anmodning markedsovervågningsmyndighederne følgende oplysninger:

a) navn og adresse på enhver erhvervsdrivende, som har leveret et produkt med digitale elementer til dem

b) hvis de foreligger, navn og adresse på enhver erhvervsdrivende, som de har leveret et produkt med digitale elementer til

2. Erhvervsdrivende skal i ti år efter, at de har fået leveret eller har leveret produktet med digitale elementer, kunne forelægge de i stk. 1 nævnte oplysninger.

Artikel 24

Forpligtelser for open source software-forvaltere

1. Open source software-forvaltere indfører og dokumenterer på en verificerbar måde en cybersikkerhedspolitik med henblik på at fremme udviklingen af et sikkert produkt med digitale elementer samt en effektiv håndtering af sårbarheder hos udviklerne af det pågældende produkt. Denne politik skal også fremme frivillig indberetning af sårbarheder fra udviklerne af det pågældende produkt som fastsat i artikel 15 og tage højde for open source software-forvalterens specifikke karakter og de juridiske og organisatoriske ordninger, som vedkommende er underlagt. Denne politik skal navnlig omfatte aspekter vedrørende dokumentation, håndtering og afhjælpning af sårbarheder og i open source-samfundet fremme udvekslingen af oplysninger om opdagede sårbarheder.

2. Open source software-forvaltere samarbejder på anmodning fra markedsovervågningsmyndighederne med disse med henblik på at afbøde de cybersikkerhedsrisici, der er forbundet med et produkt med digitale elementer, som kan betegnes som gratis open source-software.

På grundlag af en begrundet anmodning fra en markedsovervågningsmyndighed giver open source software-forvaltere denne myndighed den i stk. 1 omhandlede dokumentation på et for denne myndighed letforståeligt sprog, i papirform eller i elektronisk form.

3. Forpligtelserne i artikel 14, stk. 1, finder anvendelse på open source software-forvaltere, i det omfang de er involveret i udviklingen af produkter med digitale elementer. Forpligtelserne i artikel 14, stk. 3 og 8, finder anvendelse på open source software-forvaltere, i det omfang alvorlige hændelser, der har indvirkning på sikkerheden af produkter med digitale elementer, påvirker net- og informationssystemer, der leveres af open source software-forvalterne til udvikling af sådanne produkter.

Artikel 25

Sikkerhedscertificering af gratis open source-software

For at lette den due diligence-forpligtelse, der er fastsat i artikel 13, stk. 5, navnlig for så vidt angår fabrikanter, der integrerer gratis open source software-komponenter i deres produkter med digitale elementer, tillægges Kommissionen beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 61 med henblik på at supplere denne forordning ved at indføre frivillige sikkerhedscertificeringsprogrammer, der gør det muligt for udviklere eller brugere af produkter med digitale elementer, der kan betegnes som gratis open source-software, samt andre tredjeparter at vurdere sådanne produkters overensstemmelse med alle eller visse væsentlige cybersikkerhedskrav eller andre forpligtelser, der er fastsat i denne forordning.

Artikel 26

Vejledning

1. For at lette gennemførelsen og sikre sammenhæng i en sådan gennemførelse offentliggør Kommissionen vejledning, der skal bistå de økonomiske aktører ved anvendelsen af denne forordning, med særligt fokus på at lette mikrovirksomheders og små og mellemstore virksomheders overholdelse af reglerne.

2. Hvor Kommissionen har til hensigt at yde vejledning som omhandlet i stk. 1, behandler den mindst følgende aspekter:

a) denne forordnings anvendelsesområde, med særligt fokus på fjerndatabehandlingsløsninger og gratis open source-software

b) anvendelsen af supportperioder i forbindelse med særlige kategorier af produkter med digitale elementer

c) vejledning rettet mod fabrikanter, der er omfattet af denne forordning, og som også er omfattet af anden EU-harmoniseringslovgivning end denne forordning eller af andre relaterede EU-retsakter

d) begrebet væsentlig ændring.

Kommissionen fører også en lettilgængelig liste over de delegerede retsakter og gennemførelsesretsakter, der vedtages i henhold til denne forordning.

3. Kommissionen hører relevante interessenter, når den udarbejder vejledning i henhold til denne artikel.

KAPITEL III

OVERENSSTEMMELSEN AF PRODUKTER MED DIGITALE ELEMENTER

Artikel 27

Overensstemmelsesformodning

1. Produkter med digitale elementer og processer indført af fabrikanten, som er i overensstemmelse med harmoniserede standarder eller dele deraf, hvis referencer er offentliggjort i *Den Europæiske Unions Tidende*, formodes at være i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, der er omfattet af disse standarder eller dele deraf.

Kommissionen anmoder i overensstemmelse med artikel 10, stk. 1, i forordning (EU) nr. 1025/2012 en eller flere europæiske standardiseringsorganisationer om at udarbejde harmoniserede standarder for de væsentlige cybersikkerhedskrav i bilag I til nærværende forordning. Ved udarbejdelsen af anmodninger om standardisering for nærværende forordning bestræber Kommissionen sig på at tage højde for eksisterende europæiske og internationale standarder for cybersikkerhed, som er gældende eller under udvikling, med henblik på at forenkle udviklingen af harmoniserede standarder i overensstemmelse med forordning (EU) nr. 1025/2012.

2. Kommissionen kan vedtage gennemførelsesretsakter, der fastlægger fælles specifikationer vedrørende tekniske krav, der giver mulighed for at opfylde de væsentlige cybersikkerhedskrav i bilag I for produkter med digitale elementer, som er omfattet af denne forordnings anvendelsesområde.

Disse gennemførelsesretsakter vedtages kun, når følgende betingelser er opfyldt:

a) Kommissionen har i henhold til artikel 10, stk. 1, i forordning (EU) nr. 1025/2012 anmodet en eller flere europæiske standardiseringsorganisationer om at udarbejde en harmoniseret standard for de væsentlige cybersikkerhedskrav i bilag I og:

   i) anmodningen er ikke blevet accepteret

   ii) de harmoniserede standarder, der forholder sig til denne anmodning, er ikke færdiggjort inden for den tidsfrist, der er fastsat i artikel 10, stk. 1, i forordning (EU) nr. 1025/2012, eller

   iii) de harmoniserede standarder er ikke i overensstemmelse med anmodningen, og

b) der offentliggøres ingen henvisning til harmoniserede standarder, som omfatter de relevante væsentlige cybersikkerhedskrav i denne forordnings bilag I, i *Den Europæiske Unions Tidende* i overensstemmelse med forordning (EU) nr. 1025/2012, og der forventes ingen offentliggørelse af en sådan henvisning inden for et rimeligt tidsrum.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 62, stk. 2.

3. Inden Kommissionen udarbejder det i denne artikels stk. 2 omhandlede udkast til gennemførelsesretsakt, underretter den det udvalg, der er omhandlet i artikel 22 i forordning (EU) nr. 1025/2012, om, at den anser betingelserne i nærværende artikels stk. 2 for at være opfyldt.

4. Når Kommissionen udarbejder det i stk. 2 omhandlede udkast til gennemførelsesretsakt, tager den synspunkter fra relevante organer i betragtning og hører alle relevante interessenter behørigt.

5. Produkter med digitale elementer og processer indført af fabrikanten, som er i overensstemmelse med de fælles specifikationer, der er fastsat ved gennemførelsesretsakter omhandlet i denne artikels stk. 2, eller dele heraf, formodes at være i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, der er omfattet af disse fælles specifikationer eller dele heraf.

6. Når en europæisk standardiseringsorganisation vedtager en harmoniseret standard og fremlægger denne for Kommissionen med henblik på offentliggørelse af henvisningen hertil i *Den Europæiske Unions Tidende*, foretager Kommissionen en vurdering af den harmoniserede standard i overensstemmelse med forordning (EU) nr. 1025/2012. Når en henvisning vedrørende en harmoniseret standard offentliggøres i *Den Europæiske Unions Tidende*, ophæver Kommissionen de i denne forordnings stk. 2 omhandlede gennemførelsesretsakter, eller dele deraf, som omfatter de samme væsentlige cybersikkerhedskrav, der er omfattet af denne harmoniserede standard.

7. Hvor en medlemsstat mener, at en fælles specifikation ikke lever helt op til de væsentlige cybersikkerhedskrav i bilag I, underretter medlemsstaten Kommissionen herom ved at give en udførlig forklaring. Kommissionen vurderer den udførlige forklaring og kan, hvis det er hensigtsmæssigt, ændre den gennemførelsesretsakt, som den pågældende fælles specifikation er oprettet ved.

8. Produkter med digitale elementer og processer indført af fabrikanten, for hvilke der er udstedt en EU-overensstemmelseserklæring eller attest i henhold til en europæisk cybersikkerhedscertificeringsordning vedtaget i medfør af forordning (EU) 2019/881, formodes at være i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, i det omfang EU-overensstemmelseserklæringen eller den europæiske cybersikkerhedsattest eller dele heraf dækker disse krav.

9. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med denne forordnings artikel 61 med henblik på at supplere denne forordning ved at præcisere de europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til forordning (EU) 2019/881, og som kan anvendes til at påvise overensstemmelsen af produkter med digitale elementer med de væsentlige cybersikkerhedskrav eller dele heraf i bilag I til nærværende forordning. Udstedelsen af en europæisk cybersikkerhedsattest i henhold til sådanne ordninger på et tillidsniveau, der som minimum er »betydeligt«, fritager derudover fabrikanten fra forpligtelsen til at lade foretage en tredjepartsoverensstemmelsesvurdering vedrørende de tilsvarende krav, jf. nærværende forordnings artikel 32, stk. 2, litra a) og b) og artikel 32, stk. 3, litra a) og b).

Artikel 28

EU-overensstemmelseserklæring

1. EU-overensstemmelseserklæringen skal udfærdiges af fabrikanten i overensstemmelse med artikel 13, stk. 12, og det skal af EU-overensstemmelseserklæringen fremgå, at det er blevet dokumenteret, at de gældende væsentlige cybersikkerhedskrav i bilag I er opfyldt.

2. EU-overensstemmelseserklæringen skal følge den model, der er fastsat i bilag V, og indeholde de elementer, der er angivet i de relevante overensstemmelsesvurderingsprocedurer i bilag VIII. En sådan erklæring skal ajourføres, i det omfang det er relevant. Den stilles til rådighed på de sprog, der kræves af den medlemsstat, hvor produktet med digitale elementer bringes i omsætning eller gøres tilgængeligt på markedet.

Den forenklede EU-overensstemmelseserklæring, der er omhandlet i artikel 13, stk. 20, skal følge den model, der er fastsat i bilag VI. Den stilles til rådighed på de sprog, der kræves af den medlemsstat, hvor produktet med digitale elementer bringes i omsætning eller gøres tilgængeligt på markedet.

3. Hvis et produkt med digitale elementer er omfattet af mere end én EU-retsakt, der kræver en EU-overensstemmelseserklæring, udfærdiges der en enkelt EU-overensstemmelseserklæring for alle sådanne EU-retsakter. Det skal af erklæringen fremgå, hvilke EU-retsakter den vedrører, herunder hvor disse er offentliggjort.

4. Ved at udarbejde EU-overensstemmelseserklæringen påtager fabrikanten sig ansvaret for, at produktet med digitale elementer opfylder de gældende krav.

5. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 61 med henblik på at supplere denne forordning ved at tilføje elementer til minimumsindholdet af EU-overensstemmelseserklæringen i bilag V for at tage hensyn til den teknologiske udvikling.

Artikel 29

Generelle principper for CE-mærkningen

CE-mærkningen er underkastet de generelle principper i artikel 30 i forordning (EF) nr. 765/2008.

Artikel 30

Regler og betingelser for anbringelse af CE-mærkning

1. CE-mærkningen anbringes synligt, let læseligt og uudsletteligt på produktet med digitale elementer. Hvis produktet med digitale elementer er af en sådan art, at dette ikke er muligt eller berettiget, anbringes CE-mærkningen på emballagen og på den i artikel 28 omhandlede EU-overensstemmelseserklæring, der ledsager produktet med digitale elementer. For produkter med digitale elementer i form af software anbringes CE-mærkningen enten på den i artikel 28 omhandlede EU-overensstemmelseserklæring eller på webstedet for softwareproduktet. I sidstnævnte tilfælde skal der være nem og direkte adgang for forbrugere til den relevante sektion på webstedet.

2. CE-mærkning på produktet med digitale elementer kan, såfremt arten af produktet med digitale elementer nødvendiggør det, være lavere end 5 mm, forudsat at den fortsat er synlig og læselig.

3. CE-mærkningen anbringes, før produktet med digitale elementer bringes i omsætning. Den kan følges af et piktogram eller en anden form for angivelse vedrørende cybersikkerhedsrisiko- eller brugskategori, der er fastsat i de i stk. 6 omhandlede gennemførelsesretsakter.

4. Efter CE-mærkningen anføres identifikationsnummeret på det bemyndigede organ, hvis dette organ deltager i den i stk. 6 omhandlede overensstemmelsesvurderingsprocedure på grundlag af fuld kvalitetssikring (baseret på modul H).

Det bemyndigede organs identifikationsnummer anbringes af organet selv eller efter dettes anvisninger af fabrikanten eller dennes bemyndigede repræsentant.

5. Medlemsstaterne benytter eksisterende mekanismer til at sikre, at CE-mærkningsordningen anvendes korrekt, og tager passende skridt i tilfælde af uretmæssig anvendelse af mærkningen. Hvis produktet med digitale elementer er omfattet af anden EU-harmoniseringslovgivning end denne forordning, som også indeholder bestemmelser om anbringelse af CE-mærkning, skal CE-mærkningen angive, at produktet ligeledes opfylder kravene i en anden sådan EU-harmoniseringslovgivning.

6. Kommissionen kan ved hjælp af gennemførelsesretsakter fastsætte tekniske specifikationer for etiketter, piktogrammer eller andre mærker vedrørende sikkerheden af produkter med digitale elementer, deres supportperioder og mekanismer til at fremme deres anvendelse og til at øge offentlighedens bevidsthed om sikkerheden ved produkter med digitale elementer. Når Kommissionen udarbejder udkastene til gennemførelsesretsakter, hører den relevante interessenter og, hvis denne allerede er blevet nedsat i henhold til artikel 52, stk. 15, ADCO. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 62, stk. 2.

Artikel 31

Teknisk dokumentation

1. Den tekniske dokumentation skal indeholde alle relevante data eller oplysninger om de midler, som fabrikanten anvender for at sikre, at produktet med digitale elementer og de processer, som fabrikanten har indført, opfylder de væsentlige cybersikkerhedskrav i bilag I. Den skal som minimum indeholde de i bilag VII fastsatte elementer.

2. Den tekniske dokumentation udarbejdes, inden produktet med digitale elementer bringes i omsætning, og ajourføres løbende, hvor det er relevant, i det mindste i supportperioden.

3. For produkter med digitale elementer som omhandlet i artikel 12, der også er omfattet af andre EU-retsakter, som indeholder bestemmelser om teknisk dokumentation, udarbejdes der en samlet teknisk dokumentation, som indeholder de oplysninger, der er omhandlet i bilag VII, og de oplysninger, der kræves i henhold til disse EU-retsakter.

4. Den tekniske dokumentation og korrespondance vedrørende overensstemmelsesvurderingsprocedurer udfærdiges på et officielt sprog i den medlemsstat, hvor det bemyndigede organ er etableret, eller på et for dette organ acceptabelt sprog.

5. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 61 med henblik på at supplere denne forordning ved at tilføje de elementer, der skal indgå i den tekniske dokumentation fastsat jf. bilag VII, for at tage hensyn til den teknologiske udvikling samt udviklingen i forbindelse med gennemførelsen af denne forordning. Med henblik herpå sikrer Kommissionen, at den administrative byrde for mikrovirksomheder og små og mellemstore virksomheder er forholdsmæssig.

Artikel 32

Overensstemmelsesvurderingsprocedurer for produkter med digitale elementer

1. Fabrikanten foretager en overensstemmelsesvurdering af produktet med digitale elementer og de processer, som fabrikanten har indført, med henblik på at fastslå, om de væsentlige cybersikkerhedskrav i bilag I er opfyldt. Fabrikanten påviser overensstemmelse med de væsentlige cybersikkerhedskrav ved brug af en af følgende procedurer:

a) proceduren for intern kontrol (baseret på modul A) fastsat i bilag VIII

b) EU-typeafprøvning (baseret på modul B) fastsat i bilag VIII efterfulgt af typeoverensstemmelse på grundlag af intern produktionskontrol (baseret på modul C) fastsat i bilag VIII

c) en overensstemmelsesvurdering på grundlag af fuld kvalitetssikring (baseret på modul H) fastsat i bilag VIII, eller

d) hvor en sådan foreligger og er relevant, en europæisk cybersikkerhedscertificeringsordning i medfør af artikel 27, stk. 9.

2. Hvis fabrikanten ved vurderingen af, hvorvidt et vigtigt produkt med digitale elementer, der henhører under klasse I som fastsat i bilag III, og de processer, der er indført af fabrikanten, overholder de væsentlige cybersikkerhedskrav i bilag I, ikke har anvendt eller kun delvist har anvendt harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger på et tillidsniveau, der som minimum er »betydeligt«, som omhandlet i artikel 27, eller hvis sådanne harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger ikke findes, underkastes det pågældende produkt med digitale elementer og de processer, som fabrikanten har indført, for så vidt angår disse væsentlige cybersikkerhedskrav en af følgende procedurer:

a) EU-typeafprøvningen (baseret på modul B) fastsat i bilag VIII efterfulgt af typeoverensstemmelse på grundlag af intern produktionskontrol (baseret på modul C) fastsat i bilag VIII, eller

b) en overensstemmelsesvurdering på grundlag af fuld kvalitetssikring (baseret på modul H) fastsat i bilag VIII,

3. Hvis produktet er et vigtigt produkt med digitale elementer, der henhører under klasse II som fastsat i bilag III, påviser fabrikanten overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I ved brug af en af følgende procedurer:

a) EU-typeafprøvning (baseret på modul B) som fastsat i bilag VIII efterfulgt af typeoverensstemmelse på grundlag af intern produktionskontrol (baseret på modul C) som fastsat i bilag VIII

b) en overensstemmelsesvurdering på grundlag af fuld kvalitetssikring (baseret på modul H) som fastsat i bilag VIII, eller

c) hvor en sådan foreligger og er relevant, en europæisk cybersikkerhedscertificeringsordning i henhold til denne forordnings artikel 27, stk. 9, på et tillidsniveau, der som minimum er »betydeligt« i henhold til forordning (EU) 2019/881.

4. Kritiske produkter med digitale elementer, der er opført i bilag IV, skal påvise overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I ved hjælp af en af følgende procedurer:

a) en europæisk cybersikkerhedscertificeringsordning i overensstemmelse med artikel 8, stk. 1, eller

b) hvis betingelserne i artikel 8, stk. 1, ikke er opfyldt, en af de procedurer, der er omhandlet i nærværende artikels stk. 3.

5. Fabrikanter af produkter med digitale elementer, der kan betegnes som gratis open source-software, og som er omfattet af kategorierne i bilag III, skal kunne påvise overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I ved hjælp af en af de procedurer, der er omhandlet i denne artikels stk. 1, forudsat at den tekniske dokumentation, der er omhandlet i artikel 31, gøres tilgængelig for offentligheden på det tidspunkt, hvor de pågældende produkter bringes i omsætning.

6. Der skal tages hensyn til mikrovirksomheders og små og mellemstore virksomheders, herunder nyetablerede virksomheders, særlige interesser og behov ved fastsættelsen af gebyrerne for overensstemmelsesvurderingsprocedurer, og disse gebyrer skal reduceres i forhold til deres særlige interesser og behov.

Artikel 33

Støtteforanstaltninger for mikrovirksomheder og små og mellemstore virksomheder, herunder nyetablerede virksomheder

1. Medlemsstaterne iværksætter, hvor det er relevant, følgende tiltag skræddersyet til mikrovirksomheders og små virksomheders behov:

a) tilrettelæggelse af specifikke oplysnings- og uddannelsesaktiviteter om anvendelsen af denne forordning

b) oprettelse af en særlig kommunikationskanal for mikrovirksomheder og små virksomheder og, i det omfang det er relevant, lokale offentlige myndigheder med henblik på at yde rådgivning og besvare spørgsmål om gennemførelsen af denne forordning

c) støtte af afprøvnings- og overensstemmelsesvurderingsaktiviteter, herunder, hvor det er relevant, med støtte fra Det Europæiske Kompetencecenter for Cybersikkerhed.

2. Medlemsstaterne kan, hvor det er relevant, oprette reguleringsmæssige sandkasser for cyberrobusthed. Sådanne reguleringsmæssige sandkasser skal sikre kontrollerede afprøvningsmiljøer for innovative produkter med digitale elementer for at lette deres udvikling, design, validering og afprøvning med henblik på at overholde denne forordning i en begrænset periode, inden de bringes i omsætning. Kommissionen og, hvor det er relevant, ENISA kan yde teknisk støtte og rådgivning samt tilvejebringe værktøjer til oprettelse og drift af reguleringsmæssige sandkasser. De reguleringsmæssige sandkasser oprettes under direkte tilsyn, vejledning og støtte fra markedsovervågningsmyndighederne. Medlemsstaterne underretter Kommissionen og de øvrige markedsovervågningsmyndigheder om oprettelsen af en reguleringsmæssig sandkasse gennem ADCO. De reguleringsmæssige sandkasser berører ikke de kompetente myndigheders tilsynsbeføjelser eller korrigerende beføjelser. Medlemsstaterne sikrer åben, retfærdig og gennemsigtig adgang til reguleringsmæssige sandkasser og letter navnlig adgangen for mikrovirksomheder og små virksomheder, herunder nyetablerede virksomheder.

3. I overensstemmelse med artikel 26 yder Kommissionen vejledning til mikrovirksomheder og små og mellemstore virksomheder i forbindelse med gennemførelsen af denne forordning.

4. Kommissionen bekendtgør den finansielle støtte, der er tilgængelig inden for de lovgivningsmæssige rammer for eksisterende EU-programmer, navnlig for at lette den finansielle byrde for mikrovirksomheder og små virksomheder.

5. Mikrovirksomheder og små virksomheder kan tilvejebringe alle elementer af den tekniske dokumentation, der er angivet i bilag VII, ved hjælp af et forenklet format. Med henblik herpå præciserer Kommissionen ved hjælp af gennemførelsesretsakter den forenklede tekniske dokumentationsformular, der er rettet mod mikrovirksomheders og små virksomheders behov, herunder hvordan elementerne i bilag VII skal tilvejebringes. Hvis en mikrovirksomhed eller en lille virksomhed vælger at tilvejebringe de oplysninger, der er fastlagt i bilag VII, på en forenklet måde, skal den anvende den formular, der er omhandlet i dette stykke. Bemyndigede organer accepterer denne formular med henblik på en overensstemmelsesvurdering.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 62, stk. 2.

Artikel 34

Aftaler om gensidig anerkendelse

Unionen kan under hensyntagen til niveauet for teknisk udvikling og tilgangen til overensstemmelsesvurdering i et tredjeland indgå aftaler om gensidig anerkendelse med tredjelande i overensstemmelse med artikel 218 i TEUF med det formål at fremme og lette international handel.

KAPITEL IV

BEMYNDIGELSE AF OVERENSSTEMMELSESVURDERINGSORGANER

Artikel 35

Bemyndigelse og underretning

1. Medlemsstaterne underretter Kommissionen og de øvrige medlemsstater om, hvilke organer der er bemyndiget til at udføre overensstemmelsesvurderingsopgaver i overensstemmelse med denne forordning.

2. Medlemsstaterne bestræber sig på senest den 11. december 2026 at sikre, at der er et tilstrækkeligt antal bemyndigede organer i Unionen til at foretage overensstemmelsesvurderinger, så der undgås flaskehalse og forhindringer for markedsadgang.

Artikel 36

Bemyndigende myndigheder

1. Hver medlemsstat udpeger en bemyndigende myndighed, som er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering, udpegning og bemyndigelse af overensstemmelsesvurderingsorganer og for overvågning heraf, herunder overholdelsen af artikel 41.

2. Medlemsstater kan bestemme, at den stk. 1 omhandlede vurdering og overvågning foretages af et nationalt akkrediteringsorgan i den i forordning (EF) nr. 765/2008 anvendte betydning og i overensstemmelse med nævnte forordning.

3. Hvis den bemyndigende myndighed uddelegerer eller på anden måde betror den vurdering, bemyndigelse eller overvågning, der er omhandlet i denne artikels stk. 1, til et organ, der ikke er en statslig enhed, skal dette organ være en juridisk enhed og på tilsvarende vis overholde artikel 37. Derudover skal det have truffet foranstaltninger til dækning af erstatningsansvar i forbindelse med sine aktiviteter.

4. Den bemyndigende myndighed påtager sig det fulde ansvar for de opgaver, der udføres af det i stk. 3 omhandlede organ.

Artikel 37

Krav til bemyndigende myndigheder

1. En bemyndigende myndighed skal oprettes på en sådan måde, at der ikke opstår interessekonflikter med overensstemmelsesvurderingsorganer.

2. En bemyndigende myndighed skal være organiseret og arbejde på en sådan måde, at det sikres, at dens aktiviteter udøves objektivt og uvildigt.

3. En bemyndigende myndighed skal være organiseret på en sådan måde, at alle beslutninger om bemyndigelse af overensstemmelsesvurderingsorganet træffes af kompetente personer, der ikke er identiske med dem, der foretog vurderingen.

4. En bemyndigende myndighed må ikke udføre aktiviteter, som udføres af overensstemmelsesvurderingsorganer, eller yde rådgivningsservice på kommercielt eller konkurrencemæssigt grundlag.

5. En bemyndigende myndighed skal sikre, at de oplysninger, som den indhenter, behandles fortroligt.

6. En bemyndigende myndighed skal have et tilstrækkeligt antal kompetente medarbejdere til, at den kan udføre sine opgaver behørigt.

Artikel 38

Oplysningskrav for bemyndigende myndigheder

1. Medlemsstaterne underretter Kommissionen om deres procedurer for vurdering og bemyndigelse af overensstemmelsesvurderingsorganer og overvågning af bemyndigede organer og om eventuelle ændringer heraf.

2. Kommissionen gør de i stk. 1 omhandlede oplysninger offentligt tilgængelige.

Artikel 39

Krav til bemyndigede organer

1. Med henblik på bemyndigelse skal et overensstemmelsesvurderingsorgan opfylde kravene i stk. 2-12.

2. Et overensstemmelsesvurderingsorgan skal oprettes i henhold til national ret og skal være en juridisk person.

3. Et overensstemmelsesvurderingsorgan skal være et tredjepartsorgan, der er uafhængigt af den organisation eller det produkt med digitale elementer, som det vurderer.

Et organ, der tilhører en erhvervsorganisation eller brancheforening, som repræsenterer virksomheder, der er involveret i design, udvikling, produktion, tilvejebringelse, sammensætning, brug eller vedligeholdelse af produkter med digitale elementer, som det vurderer, kan, forudsat at det er påvist, at det er uafhængigt, og at der ikke foreligger interessekonflikter, anses for at være et sådant tredjepartsorgan.

4. Overensstemmelsesvurderingsorganet, dets øverste ledelse og det personale, der er ansvarligt for at foretage overensstemmelsesvurdering, må ikke være designeren, udvikleren, fabrikanten, leverandøren, importøren, distributøren, montøren, køberen, ejeren, brugeren eller reparatøren af de produkter med digitale elementer, som de vurderer, eller den bemyndigede repræsentant for nogen af disse parter. Dette forhindrer ikke anvendelse af vurderede produkter, der er nødvendige for overensstemmelsesvurderingsorganets aktiviteter, eller anvendelse af sådanne produkter til personlige formål.

Overensstemmelsesvurderingsorganet, dets øverste ledelse og det personale, der er ansvarligt for at foretage overensstemmelsesvurdering, må ikke være direkte involveret i design, udvikling, produktion, import, distribution, markedsføring, montering, anvendelse eller vedligeholdelse af de produkter med digitale elementer, som de vurderer, eller repræsentere parter, der er involveret i disse aktiviteter. De må ikke deltage i aktiviteter, som kan være i strid med deres objektivitet og integritet i forbindelse med de overensstemmelsesvurderingsaktiviteter, de er bemyndiget til. Dette gælder navnlig rådgivningstjenester.

Overensstemmelsesvurderingsorganer skal sikre, at deres dattervirksomheders eller underleverandørers aktiviteter ikke påvirker fortroligheden, objektiviteten eller uvildigheden af deres overensstemmelsesvurderingsaktiviteter.

5. Overensstemmelsesvurderingsorganerne og deres personale skal udføre overensstemmelsesvurderingsaktiviteterne med den størst mulige faglige integritet og den nødvendige tekniske kompetence på det specifikke område og må ikke påvirkes af nogen form for pression eller incitament, navnlig af økonomisk art, som kan have indflydelse på deres afgørelser eller resultaterne af deres overensstemmelsesvurderingsaktiviteter, særlig fra personer eller grupper af personer, som har en interesse i resultaterne af disse aktiviteter.

6. Et overensstemmelsesvurderingsorgan skal være i stand til at gennemføre alle de i bilag VIII omhandlede overensstemmelsesvurderingsopgaver, for hvilke det er blevet notificeret, uanset om disse opgaver udføres af overensstemmelsesvurderingsorganet selv eller på dets vegne og under dets ansvar.

Til enhver tid og for hver overensstemmelsesvurderingsprocedure og type eller kategori af produkter med digitale elementer, for hvilket det er blevet notificeret, skal et overensstemmelsesvurderingsorgan have følgende til rådighed:

a) personale med teknisk viden og med tilstrækkelig og relevant erfaring til at udføre overensstemmelsesvurderingsopgaverne

b) beskrivelser af de procedurer, i henhold til hvilke overensstemmelsesvurderingen skal foretages, således at gennemsigtigheden og muligheden for at reproducere disse procedurer sikres. Det skal have indført hensigtsmæssige politikker og procedurer, som skelner mellem de opgaver, det udfører som bemyndiget organ, og andre aktiviteter

c) procedurer, der sætter det i stand til at udføre sine aktiviteter under behørig hensyntagen til en virksomheds størrelse, den sektor, som virksomheden opererer i, virksomhedens struktur, den pågældende produktteknologis kompleksitet og produktionsprocessens karakter af masse- eller serieproduktion.

Et overensstemmelsesvurderingsorgan skal råde over de fornødne midler til på en passende måde at udføre de tekniske og administrative opgaver, der er forbundet med overensstemmelsesvurderingsarbejdet, og det skal have adgang til alt nødvendigt udstyr og alle nødvendige faciliteter.

7. Det personale, som skal udføre overensstemmelsesvurderingsopgaverne, skal have:

a) en solid teknisk og faglig uddannelse inden for alle de overensstemmelsesvurderingsaktiviteter, som organets bemyndigelse dækker

b) tilfredsstillende kendskab til kravene vedrørende de vurderinger, de foretager, og tilstrækkelig bemyndigelse til at udføre sådanne vurderinger

c) tilstrækkeligt kendskab til og tilstrækkelig forståelse af de væsentlige cybersikkerhedskrav i bilag I, de gældende harmoniserede standarder og fælles specifikationer samt de relevante bestemmelser i EU-harmoniseringslovgivning og gennemførelsesretsakter

d) færdighed i at udarbejde attester, registreringer og rapporter, der viser, at vurderingerne er udført.

8. Det skal sikres, at overensstemmelsesvurderingsorganerne, den øverste ledelse og det personale, der er ansvarligt for at foretage overensstemmelsesvurdering, arbejder uvildigt.

Aflønningen af den øverste ledelse og vurderingspersonalet må ikke afhænge af, hvor mange vurderinger de udfører eller resultaterne af disse vurderinger.

9. Overensstemmelsesvurderingsorganerne skal tegne en ansvarsforsikring, medmindre deres medlemsstat har overtaget ansvaret efter national ret, eller medmindre medlemsstaten selv er direkte ansvarlig for overensstemmelsesvurderingen.

10. Overensstemmelsesvurderingsorganets personale har tavshedspligt med hensyn til alle oplysninger, det kommer i besiddelse af ved udførelsen af dets opgaver i henhold til bilag VIII eller enhver bestemmelse i national ret til gennemførelse heraf, undtagen over for markedsovervågningsmyndighederne i den medlemsstat, hvor aktiviteterne udføres. Ejendomsrettigheder skal beskyttes. Overensstemmelsesvurderingsorganet skal have dokumenterede procedurer, der sikrer overholdelse af dette stykke.

11. Overensstemmelsesvurderingsorganet skal deltage i, eller sikre at dets vurderingspersonale er orienteret om, de relevante standardiseringsaktiviteter og aktiviteterne i den koordineringsgruppe af bemyndigede organer, der er nedsat i henhold til artikel 51, og skal som generel retningslinje anvende de administrative afgørelser og dokumenter, som arbejdet i denne gruppe udmøntes i.

12. Overensstemmelsesvurderingsorganer skal fungere i henhold til et sæt konsekvente, retfærdige, forholdsmæssige og rimelige vilkår og betingelser, samtidig med at unødvendige byrder undgås for erhvervsdrivende, idet der særlig tages hensyn til mikrovirksomheders og små og mellemstore virksomheders interesser for så vidt angår gebyrer.

Artikel 40

Formodning om bemyndigede organers overensstemmelse

Hvis et overensstemmelsesvurderingsorgan dokumenterer, at det opfylder kriterierne i de relevante harmoniserede standarder eller dele heraf, hvortil der er offentliggjort referencer i *Den Europæiske Unions Tidende*, formodes det at opfylde kravene i artikel 39, for så vidt som de gældende harmoniserede standarder dækker disse krav.

Artikel 41

Dattervirksomheder og underleverandører i tilknytning til bemyndigede organer

1. Hvis et bemyndiget organ giver bestemte opgaver i forbindelse med overensstemmelsesvurdering til underleverandører eller anvender en dattervirksomhed, sikrer det bemyndigede organ, at underleverandøren eller dattervirksomheden opfylder kravene i artikel 39, og underretter den bemyndigende myndighed herom.

2. De bemyndigede organer har det fulde ansvar for de opgaver, der udføres af underleverandører eller dattervirksomheder, uanset hvor de er etableret.

3. Aktiviteter må kun gives til underleverandører eller udføres af en dattervirksomhed, hvis fabrikanten har givet sit samtykke.

4. De bemyndigede organer sikrer, at de relevante dokumenter vedrørende vurderingen af underleverandørens eller dattervirksomhedens kvalifikationer og det arbejde, som de har udført i henhold til denne forordning, er til rådighed for den bemyndigende myndighed.

Artikel 42

Ansøgning om bemyndigelse

1. Et overensstemmelsesvurderingsorgan indgiver en ansøgning om bemyndigelse til den bemyndigende myndighed i den medlemsstat, hvor det er etableret.

2. Ansøgningen ledsages af en beskrivelse af de overensstemmelsesvurderingsaktiviteter, den eller de overensstemmelsesvurderingsprocedurer og det eller de produkter med digitale elementer, som organet hævder at være kompetent til, samt, i givet fald, af et akkrediteringscertifikat udstedt af et nationalt akkrediteringsorgan, hvor det attesteres, at overensstemmelsesvurderingsorganet opfylder kravene i artikel 39.

3. Hvis det pågældende overensstemmelsesvurderingsorgan ikke kan forelægge et akkrediteringscertifikat, forelægger det den bemyndigende myndighed al den dokumentation, der er nødvendig for at kontrollere, anerkende og regelmæssigt overvåge, at det opfylder kravene i artikel 39.

Artikel 43

Bemyndigelsesprocedure

1. De bemyndigende myndigheder må kun bemyndige overensstemmelsesvurderingsorganer, som opfylder kravene i artikel 39.

2. Den bemyndigende myndighed underretter Kommissionen og de øvrige medlemsstater ved hjælp af informationssystemet New Approach Notified and Designated Organisations, der er udviklet og forvaltes af Kommissionen.

3. Underretningen skal indeholde fyldestgørende oplysninger om overensstemmelsesvurderingsaktiviteterne, det pågældende overensstemmelsesvurderingsmodul eller de pågældende overensstemmelsesvurderingsmoduler og det pågældende produkt eller de pågældende produkter med digitale elementer og den relevante dokumentation for kompetencen.

4. Hvis en bemyndigelse ikke er baseret på et akkrediteringscertifikat som anført i artikel 42, stk. 2, forelægger den bemyndigende myndighed Kommissionen og de øvrige medlemsstater dokumentation, der attesterer overensstemmelsesvurderingsorganets kompetence og de ordninger, der er indført til sikring af, at der regelmæssigt føres tilsyn med organet, og at organet også fremover vil opfylde de i artikel 39 fastsatte krav.

5. Det pågældende organ må kun udføre aktiviteter som bemyndiget organ, hvis Kommissionen og de øvrige medlemsstater ikke har gjort indsigelse inden for to uger efter en underretning baseret på et akkrediteringscertifikat eller inden for to måneder efter en underretning, der ikke er baseret på et akkrediteringscertifikat.

Kun et sådant organ anses for at være et bemyndiget organ i denne forordnings forstand.

6. Kommissionen og de øvrige medlemsstater skal underrettes om eventuelle efterfølgende relevante ændringer af bemyndigelsen.

Artikel 44

Identifikationsnumre for og lister over bemyndigede organer

1. Kommissionen tildeler et bemyndiget organ et identifikationsnummer.

Hvert bemyndiget organ tildeles kun ét sådant nummer, også selv om organet er notificeret i henhold til flere EU-retsakter.

2. Kommissionen offentliggør listen over organer, der er notificeret i henhold til denne forordning, herunder de identifikationsnumre, de er blevet tildelt, og de aktiviteter, for hvilke de er notificeret.

Kommissionen sikrer, at denne liste holdes ajour.

Artikel 45

Ændringer af bemyndigelser

1. Hvis en bemyndigende myndighed har konstateret eller er blevet underrettet om, at et bemyndiget organ ikke længere opfylder kravene i artikel 39, eller at det ikke opfylder sine forpligtelser, begrænser, suspenderer eller inddrager den bemyndigende myndighed bemyndigelsen, alt efter hvad der er relevant, og afhængigt af i hvor høj grad disse krav eller forpligtelser ikke er blevet opfyldt. Den underretter omgående Kommissionen og de øvrige medlemsstater herom.

2. Hvis en bemyndigelse begrænses, suspenderes eller inddrages, eller hvis det bemyndigede organ har indstillet sin virksomhed, træffer den bemyndigende medlemsstat de nødvendige foranstaltninger for at sikre, at dette organs sager enten behandles af et andet bemyndiget organ eller gøres tilgængelige for de ansvarlige bemyndigende myndigheder og markedsovervågningsmyndigheder efter disses anmodning.

Artikel 46

Anfægtelse af de bemyndigede organers kompetence

1. Kommissionen undersøger alle tilfælde, hvor den tvivler på et bemyndiget organs kompetence eller på, at et bemyndiget organ fortsat opfylder de krav og forpligtelser, der påhviler det, og tilfælde, hvor den bliver gjort opmærksom på en sådan tvivl.

2. Den bemyndigende medlemsstat forelægger efter anmodning Kommissionen alle oplysninger om grundlaget for bemyndigelsen eller fastholdelsen af det bemyndigede organs kompetence.

3. Kommissionen sikrer, at alle følsomme oplysninger, den indhenter som led i sine undersøgelser, behandles fortroligt.

4. Hvis Kommissionen konstaterer, at et bemyndiget organ ikke eller ikke længere opfylder kravene vedrørende dets bemyndigelse, underretter Kommissionen den bemyndigende medlemsstat herom og anmoder den om at træffe de nødvendige korrigerende foranstaltninger, herunder om nødvendigt inddragelse af bemyndigelsen.

Artikel 47

Bemyndigede organers operationelle forpligtelser

1. Bemyndigede organer foretager overensstemmelsesvurdering i overensstemmelse med de overensstemmelsesvurderingsprocedurer, der er fastsat i artikel 32 og bilag VIII.

2. Overensstemmelsesvurderingerne foretages i overensstemmelse med proportionalitetsprincippet, således at de erhvervsdrivende ikke pålægges unødige byrder. Overensstemmelsesvurderingsorganer udfører deres aktiviteter under behørig hensyntagen til virksomhedernes størrelse, især med hensyn til mikrovirksomheder og små og mellemstore virksomheder, den sektor, som de opererer inden for, deres struktur, deres kompleksitet og cybersikkerhedsrisikoniveauet for de pågældende produkter med digitale elementer og den pågældende teknologi, og om produktionsprocessen har karakter af masse- eller serieproduktion.

3. Bemyndigede organer skal dog respektere den grad af strenghed og det beskyttelsesniveau, der kræves for, at produkterne med digitale elementer opfylder denne forordning.

4. Hvis et bemyndiget organ finder, at fabrikanten ikke har opfyldt kravene i bilag I eller i de dertil svarende harmoniserede standarder eller de fælles specifikationer som omhandlet i artikel 27, kræver det, at det fabrikanten træffer afhjælpende foranstaltninger, og det udsteder ikke en overensstemmelsesattest.

5. Hvis et bemyndiget organ i forbindelse med overensstemmelsesovervågning efter udstedelse af en attest finder, at et produkt med digitale elementer ikke længere opfylder kravene i denne forordning, kræver det, at fabrikanten afhjælper dette og suspenderer eller inddrager attesten om nødvendigt.

6. Hvis der ikke træffes afhjælpende foranstaltninger, eller hvis disse ikke har den ønskede virkning, begrænser, suspenderer eller inddrager det bemyndigede organ eventuelle attester, alt efter hvad der er relevant.

Artikel 48

Klage over afgørelser truffet af bemyndigede organer

Medlemsstaterne sikrer, at der findes en procedure for klager over de bemyndigede organers afgørelser.

Artikel 49

Oplysningspligt for bemyndigede organer

1. De bemyndigede organer oplyser den bemyndigende myndighed om følgende:

a) ethvert afslag på udstedelse, eller enhver begrænsning, suspension eller inddragelse, af en attest

b) alle forhold, der har indflydelse på omfanget af og betingelserne for bemyndigelsen

c) eventuelle anmodninger om oplysninger, de har modtaget fra markedsovervågningsmyndigheder vedrørende overensstemmelsesvurderingsaktiviteter

d) efter anmodning, overensstemmelsesvurderingsaktiviteter, der er udført på det område, som deres bemyndigelse gælder for, og enhver anden udført aktivitet, herunder grænseoverskridende aktiviteter og brug af underleverandører.

2. De bemyndigede organer giver de øvrige organer, der er bemyndiget i henhold til denne forordning, og som udfører lignende overensstemmelsesvurderingsaktiviteter og dækker samme produkter med digitale elementer, relevante oplysninger om spørgsmål vedrørende negative og, efter anmodning, positive overensstemmelsesvurderingsresultater.

Artikel 50

Erfaringsudveksling

Kommissionen sørger for, at der tilrettelægges erfaringsudveksling mellem medlemsstaternes nationale myndigheder med ansvar for bemyndigelsespolitik.

Artikel 51

Koordinering af bemyndigede organer

1. Kommissionen sikrer, at der etableres passende koordinering og samarbejde mellem bemyndigede organer, og at denne koordinering og dette samarbejde fungerer efter hensigten i form af en tværsektoriel gruppe af bemyndigede organer.

2. Medlemsstaterne sørger for, at de organer, de har bemyndiget, deltager i arbejdet i denne gruppe enten direkte eller gennem udpegede repræsentanter.

KAPITEL V

MARKEDSOVERVÅGNING OG HÅNDHÆVELSE

Artikel 52

Markedsovervågning og kontrol af produkter med digitale elementer på EU-markedet

1. Forordning (EU) 2019/1020 finder anvendelse på produkter med digitale elementer, der er omfattet af nærværende forordnings anvendelsesområde.

2. Hver medlemsstat udpeger med henblik på en virkningsfuld gennemførelse af denne forordning en eller flere markedsovervågningsmyndigheder. Medlemsstaterne kan udpege en eksisterende eller ny myndighed til at virke som markedsovervågningsmyndighed med henblik på denne forordning.

3. De markedsovervågningsmyndigheder, der er udpeget i henhold til denne artikels stk. 2, er også ansvarlige for at gennemføre markedsovervågningsaktiviteter i forbindelse med de forpligtelser for open source software-forvaltere, der er fastsat i artikel 24. Hvis en markedsovervågningsmyndighed finder, at en open source software-forvalter ikke opfylder forpligtelserne i nævnte artikel, skal den kræve, at open source software-forvalteren sikrer, at der træffes alle passende korrigerende tiltag. Open source software-forvaltere sikrer, at der træffes alle passende korrigerende tiltag med hensyn til deres forpligtelser i henhold til denne forordning.

4. Markedsovervågningsmyndighederne samarbejder, hvor det er relevant, med de nationale cybersikkerhedscertificeringsmyndigheder, der er udpeget i henhold til artikel 58 i forordning (EU) 2019/881, og udveksler regelmæssigt oplysninger. De udpegede markedsovervågningsmyndigheder samarbejder og udveksler regelmæssigt oplysninger med de CSIRT'er, der er udpeget som koordinatorer, og ENISA for så vidt angår tilsynet med gennemførelsen af rapporteringsforpligtelserne i henhold til nærværende forordnings artikel 14.

5. Markedsovervågningsmyndighederne kan anmode en CSIRT, der er udpeget som koordinator, eller ENISA om at yde teknisk rådgivning om spørgsmål vedrørende gennemførelsen og håndhævelsen af denne forordning. Markedsovervågningsmyndighederne kan, når de foretager en undersøgelse i henhold til artikel 54, anmode den CSIRT, der er udpeget som koordinator, eller ENISA om at fremlægge en analyse for at understøtte overensstemmelsesvurderinger af produkter med digitale elementer.

6. Markedsovervågningsmyndighederne samarbejder, hvor det er relevant, med andre markedsovervågningsmyndigheder, der er udpeget på grundlag af anden EU-harmoniseringslovgivning end denne forordning, og udveksler regelmæssigt oplysninger.

7. Markedsovervågningsmyndighederne samarbejder, alt efter hvad der er relevant, med de myndigheder, der fører tilsyn med EU- databeskyttelsesretten. Et sådant samarbejde omfatter underretning af disse myndigheder om ethvert resultat, der er relevant for udøvelsen af deres beføjelser, herunder ved ydelse af vejledning og rådgivning i henhold til stk. 10, hvis sådan vejledning og rådgivning vedrører behandling af personoplysninger.

De myndigheder, der fører tilsyn med EU-databeskyttelsesretten, har beføjelse til at anmode om og få adgang til al dokumentation, der er udarbejdet eller opbevares i henhold til denne forordning, når adgang til denne dokumentation er nødvendig for udførelsen af deres opgaver. De underretter de udpegede markedsovervågningsmyndigheder i den berørte medlemsstat om enhver sådan anmodning.

8. Medlemsstaterne sikrer, at de udpegede markedsovervågningsmyndigheder modtager tilstrækkelige finansielle og tekniske ressourcer, herunder, hvor det er relevant, behandlingsautomatiseringsværktøjer, samt menneskelige ressourcer med de cybersikkerhedsfærdigheder, der er nødvendige for at kunne udføre deres opgaver i henhold til denne forordning.

9. Kommissionen tilskynder til og letter udvekslingen af erfaringer mellem udpegede markedsovervågningsmyndigheder.

10. Markedsovervågningsmyndighederne kan yde vejledning og rådgivning til erhvervsdrivende om gennemførelsen af denne forordning med støtte fra Kommissionen og, hvor det er relevant, CSIRT'er og ENISA.

11. Markedsovervågningsmyndighederne oplyser forbrugerne om, hvor der kan indgives klager, der kunne tyde på manglende overholdelse af denne forordning, i overensstemmelse med artikel 11 i forordning (EU) 2019/1020, og giver forbrugerne oplysninger om, hvor og hvordan de kan få adgang til mekanismer, som kan lette indberetningen af sårbarheder, hændelser og cybertrusler, der kan påvirke produkter med digitale elementer.

12. Markedsovervågningsmyndighederne letter, hvor det er relevant, samarbejdet med relevante interessenter, herunder videnskabelige organisationer og forsknings- og forbrugerorganisationer.

13. Markedsovervågningsmyndighederne aflægger årligt rapport til Kommissionen om resultaterne af relevante markedsovervågningsaktiviteter. Den udpegede markedsovervågningsmyndighed indberetter straks alle oplysninger, der er fremskaffet i forbindelse med markedsovervågningsaktiviteter, og som kan være af potentiel interesse for anvendelsen af EU-konkurrenceretten, til Kommissionen og de relevante nationale konkurrencemyndigheder.

14. For produkter med digitale elementer, der er omfattet af denne forordnings anvendelsesområde, og som er klassificeret som højrisiko-AI-systemer i henhold til artikel 6 i forordning (EU) 2024/1689, skal de markedsovervågningsmyndigheder, der udpeges med henblik på nævnte forordning, være de myndigheder, der er ansvarlige for de markedsovervågningsaktiviteter, der kræves i henhold til nærværende forordning. De markedsovervågningsmyndigheder, der er udpeget i henhold til forordning (EU) 2024/1689, samarbejder, hvor det er relevant, med de markedsovervågningsmyndigheder, der er udpeget i henhold til nærværende forordning, og med de CSIRT'er, der er udpeget som koordinatorer, og med ENISA om tilsynet med gennemførelsen af rapporteringsforpligtelserne i henhold til nærværendes forordnings artikel 14. Markedsovervågningsmyndigheder udpeget i henhold til forordning (EU) 2024/1689 underretter navnlig markedsovervågningsmyndigheder udpeget i henhold til nærværende forordning om ethvert resultat, der er relevant for udførelsen af deres opgaver i forbindelse med gennemførelsen af nærværende forordning.

15. ADCO oprettes i henhold til artikel 30, stk. 2, i forordning (EU) 2019/1020 med henblik på ensartet gennemførelse af nærværende forordning. ADCO skal bestå af repræsentanter fra de udpegede markedsovervågningsmyndigheder og, hvis det er relevant, repræsentanter fra centrale forbindelseskontorer. ADCO behandler også specifikke spørgsmål vedrørende markedsovervågningsaktiviteterne i forbindelse med de forpligtelser, der pålægges open source software-forvaltere.

16. Markedsovervågningsmyndighederne overvåger, hvordan fabrikanterne har anvendt de kriterier, der er omhandlet i artikel 13, stk. 8, når de fastsætter supportperioden for deres produkter med digitale elementer.

ADCO offentliggør i en offentligt tilgængelig og brugervenlig form relevante statistikker om kategorier af produkter med digitale elementer, herunder gennemsnitlige supportperioder som fastsat af fabrikanten i henhold til artikel 13, stk. 8, og udstikker retningslinjer, der omfatter vejledende supportperioder for kategorier af produkter med digitale elementer.

Hvis dataene tyder på utilstrækkelige supportperioder for specifikke kategorier af produkter med digitale elementer, kan ADCO udstede henstillinger til markedsovervågningsmyndighederne om at fokusere deres aktiviteter på sådanne kategorier af produkter med digitale elementer.

Artikel 53

Adgang til oplysninger og dokumentation

Hvis det er nødvendigt for at vurdere, om produkter med digitale elementer og de processer, som fabrikanten har indført, opfylder de væsentlige cybersikkerhedskrav i bilag I, tildeles markedsovervågningsmyndighederne efter begrundet anmodning adgang til de data på et for dem let forståeligt sprog, som er nødvendige for at vurdere designet, udviklingen, produktionen og sårbarhedshåndteringen af sådanne produkter, herunder den relevante interne dokumentation fra den relevante erhvervsdrivende.

Artikel 54

Procedure på nationalt plan vedrørende produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko

1. Hvis en medlemsstats markedsovervågningsmyndighed har tilstrækkelig grund til at antage, at et produkt med digitale elementer, herunder dets sårbarhedshåndtering, udgør en væsentlig cybersikkerhedsrisiko, foretager den uden unødigt ophold og, hvor det er hensigtsmæssigt, i samarbejde med den relevante CSIRT en evaluering af det pågældende produkt med digitale elementer for så vidt angår dets opfyldelse af alle de krav, der er fastsat i denne forordning. De relevante erhvervsdrivende samarbejder i nødvendigt omfang med markedsovervågningsmyndigheden.

Hvis markedsovervågningsmyndigheden i forbindelse med denne evaluering konstaterer, at produkter med digitale elementer ikke opfylder kravene i denne forordning, pålægger den straks den pågældende erhvervsdrivende at træffe alle fornødne afhjælpende tiltag for at bringe produktet med digitale elementer i overensstemmelse med disse krav, trække produktet med digitale elementer tilbage fra markedet eller tilbagekalde det inden for en rimelig tidsfrist, alt efter hvad markedsovervågningsmyndigheden måtte fastsætte i forhold til cybersikkerhedsrisikoens art.

Markedsovervågningsmyndigheden underretter det relevante bemyndigede organ herom. Artikel 18 i forordning (EU) 2019/1020 finder anvendelse på de afhjælpende tiltag.

2. Ved fastlæggelsen af væsentligheden af en cybersikkerhedsrisiko, der er omhandlet i denne artikels stk. 1, tager markedsovervågningsmyndighederne også hensyn til ikketekniske risikofaktorer, navnlig dem, der er fastsat som følge af koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan, som foretages i overensstemmelse med artikel 22 i direktiv (EU) 2022/2555. Hvor en markedsovervågningsmyndighed har tilstrækkelig grund til at antage, at et produkt med digitale elementer udgør en væsentlig cybersikkerhedsrisiko i lyset af ikketekniske risikofaktorer, underretter den de kompetente myndigheder, der er udpeget eller oprettet i henhold til artikel 8 i direktiv (EU) 2022/2555, og samarbejder i nødvendigt omfang med disse myndigheder.

3. Hvis markedsovervågningsmyndigheden finder, at den manglende overensstemmelse ikke er begrænset til dens nationale område, underretter den Kommissionen og de øvrige medlemsstater om resultaterne af evalueringen og om de tiltag, som den har pålagt den erhvervsdrivende at træffe.

4. Den erhvervsdrivende sikrer, at der træffes alle passende afhjælpende tiltag for så vidt angår alle de produkter med digitale elementer, som den erhvervsdrivende har gjort tilgængelige på EU-markedet.

5. Hvis den erhvervsdrivende ikke træffer tilstrækkelige afhjælpende tiltag inden for den frist, der er omhandlet i stk. 1, andet afsnit, træffer markedsovervågningsmyndigheden de nødvendige foreløbige foranstaltninger for at forbyde eller begrænse tilgængeliggørelsen af produktet med digitale elementer på det nationale marked eller for at trække produktet tilbage fra markedet eller kalde det tilbage.

Myndigheden underretter straks Kommissionen og de øvrige medlemsstater om disse foranstaltninger.

6. De i stk. 5 omhandlede oplysninger skal indeholde alle tilgængelige oplysninger, navnlig de data, der er nødvendige for identifikation af det produkt med digitale elementer, der ikke opfylder kravene, oprindelsesstedet for produktet med digitale elementer, arten af den påståede manglende opfyldelse af kravene og af den pågældende risiko, arten og varigheden af de trufne nationale foranstaltninger samt de synspunkter, som den pågældende erhvervsdrivende har fremsat. Markedsovervågningsmyndighederne oplyser navnlig, om den manglende overensstemmelse med kravene skyldes:

a) at produktet med digitale elementer eller de processer, som fabrikanten har indført, ikke opfylder de væsentlige cybersikkerhedskrav i bilag I

b) at der er mangler ved de harmoniserede standarder, europæiske cybersikkerhedscertificeringsordninger eller fælles specifikationer som omhandlet i artikel 27.

7. De øvrige medlemsstater ud over den medlemsstat, der har indledt proceduren, underretter straks Kommissionen og de øvrige medlemsstater om eventuelt trufne foranstaltninger og om yderligere oplysninger, som de måtte råde over, om, at det pågældende produkt med digitale elementer ikke opfylder kravene, og om deres indsigelser, i fald de ikke er indforstået med den meddelte nationale foranstaltning.

8. Hvis der ikke inden for tre måneder efter modtagelsen af den i stk. 5 i denne artikel omhandlede underretning er blevet gjort indsigelse af en medlemsstat eller Kommissionen mod en foreløbig foranstaltning truffet af en medlemsstat, anses denne foranstaltning for at være berettiget. Dette berører ikke den berørte erhvervsdrivendes procedurerettigheder i henhold til artikel 18 i forordning (EU) 2019/1020.

9. Markedsovervågningsmyndighederne i alle medlemsstaterne sikrer, at der straks træffes de fornødne restriktive foranstaltninger med hensyn til det pågældende produkt med digitale elementer såsom tilbagetrækning af dette produkt fra deres marked.

Artikel 55

EU-beskyttelsesprocedure

1. Hvor en medlemsstat inden for tre måneder efter modtagelsen af den i artikel 54, stk. 5, omhandlede underretning gør indsigelse mod en anden medlemsstats foranstaltning, eller hvor Kommissionen finder, at foranstaltningen er i strid med EU-retten, drøfter Kommissionen straks spørgsmålet med den relevante medlemsstat og den eller de relevante erhvervsdrivende og evaluerer den nationale foranstaltning. På grundlag af resultaterne af denne evaluering træffer Kommissionen senest ni måneder efter den i artikel 54, stk. 5, omhandlede underretning afgørelse om, hvorvidt den nationale foranstaltning er berettiget eller ej, og meddeler den pågældende medlemsstat denne afgørelse.

2. Hvis den nationale foranstaltning anses for at være berettiget, træffer alle medlemsstaterne de nødvendige foranstaltninger for at sikre, at produktet med digitale elementer, der ikke er i overensstemmelse med kravene, trækkes tilbage fra deres marked, og underretter Kommissionen herom. Hvis den nationale foranstaltning ikke anses for at være berettiget, trækker den pågældende medlemsstat foranstaltningen tilbage.

3. Hvor den nationale foranstaltning anses for at være berettiget, og produktet med digitale elementer ikke overholder kravene som følge af mangler ved de harmoniserede standarder, anvender Kommissionen proceduren i artikel 11 i forordning (EU) nr. 1025/2012.

4. Hvor den nationale foranstaltning anses for at være berettiget, og produktet med digitale elementer ikke overholder kravene som følge af mangler ved en europæisk cybersikkerhedscertificeringsordning som omhandlet i artikel 27, tager Kommissionen stilling til, om en eventuel delegeret retsakt, der er vedtaget i henhold til artikel 27, stk. 9, og som fastsætter formodningen om overensstemmelse for den pågældende certificeringsordning, skal ændres eller ophæves.

5. Hvor den nationale foranstaltning anses for at være berettiget, og den manglende overensstemmelse for så vidt angår produktet med digitale elementer tilskrives mangler ved de fælles specifikationer som omhandlet i artikel 27, tager Kommissionen stilling til, om en eventuel gennemførelsesretsakt, der er vedtaget i henhold til artikel 27, stk. 2, og som fastsætter disse fælles specifikationer, skal ændres eller ophæves.

Artikel 56

Procedure på EU-plan vedrørende produkter med digitale elementer, der udgør en væsentlig cybersikkerheds-risiko

1. Hvor Kommissionen har tilstrækkelig grund til at antage, herunder på grundlag af oplysninger fra ENISA, at et produkt med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, ikke opfylder kravene i denne forordning, underretter den de relevante markedsovervågningsmyndigheder. Hvor markedsovervågningsmyndighederne foretager en evaluering af det pågældende produkt med digitale elementer, der kan udgøre en væsentlig cybersikkerhedsrisiko for så vidt angår dets overholdelse af kravene i denne forordning, finder de procedurer, der er omhandlet i artikel 54 og 55, anvendelse.

2. Hvor Kommissionen har tilstrækkelig grund til at antage, at et produkt med digitale elementer udgør en væsentlig cybersikkerhedsrisiko i lyset af ikketekniske risikofaktorer, underretter den de relevante markedsovervågningsmyndigheder og, hvor det er relevant, de kompetente myndigheder, der er udpeget eller oprettet i henhold til artikel 8 i direktiv (EU) 2022/2555, og samarbejder i nødvendigt omfang med disse myndigheder. Kommissionen tager også hensyn til relevansen af de identificerede risici for det pågældende produkt med digitale elementer i lyset af dens opgaver vedrørende de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan, der er foreskrevet i artikel 22 i direktiv (EU) 2022/2555, og hører i nødvendigt omfang den samarbejdsgruppe, der er nedsat i henhold til artikel 14 i direktiv (EU) 2022/2555, og ENISA.

3. Under omstændigheder, der berettiger et hurtigt indgreb for at bevare et velfungerende indre marked, og hvor Kommissionen har tilstrækkelig grund til at antage, at det i stk. 1 omhandlede produkt med digitale elementer fortsat ikke overholder kravene i denne forordning, og de relevante markedsovervågningsmyndigheder ikke har truffet effektive foranstaltninger, foretager Kommissionen en evaluering af overholdelsen og kan anmode ENISA om at fremlægge en analyse for at understøtte denne. Kommissionen underretter de relevante markedsovervågningsmyndigheder herom. De relevante erhvervsdrivende samarbejder i nødvendigt omfang med ENISA.

4. På grundlag af den evaluering, der er omhandlet i stk. 3, kan Kommissionen beslutte, at en korrigerende eller restriktiv foranstaltning er nødvendig på EU-plan. Med henblik herpå hører den straks de berørte medlemsstater og den eller de relevante erhvervsdrivende.

5. På grundlag af den denne artikels stk. 4 omhandlede høring kan Kommissionen vedtage gennemførelsesretsakter med henblik på at træffe korrigerende eller restriktive foranstaltninger på EU-plan, herunder krav om, at de pågældende produkter med digitale elementer skal trækkes tilbage fra markedet eller tilbagekaldes inden for en rimelig tidsfrist, alt efter risikoens art. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, artikel 62, stk. 2.

6. Kommissionen meddeler omgående de i stk. 5 omhandlede gennemførelsesretsakter til den eller de relevante erhvervsdrivende. Medlemsstaterne gennemfører disse gennemførelsesretsakter straks og underretter Kommissionen herom.

7. Stk. 3-6 finder anvendelse, så længe den ekstraordinære situation, der begrundede Kommissionens indgreb, gør sig gældende, forudsat at produktet med digitale elementer ikke er bragt til at overholde denne forordning.

Artikel 57

Produkter med digitale elementer, der overholder kravene og udgør en væsentlig cybersikkerhedsrisiko

1. En medlemsstats markedsovervågningsmyndighed pålægger en erhvervsdrivende at træffe alle passende foranstaltninger, hvor den efter at have foretaget en evaluering i henhold til artikel 54 finder, at et produkt med digitale elementer og de processer, som fabrikanten har indført, overholder denne forordning, men at de udgør en væsentlig cybersikkerhedsrisiko og en risiko for:

a) menneskers sundhed eller sikkerhed

b) overholdelsen af forpligtelser i henhold til EU-ret eller national ret, der har til formål at beskytte de grundlæggende rettigheder

c) tilgængeligheden, autenticiteten, integriteten eller fortroligheden af tjenester, der leveres ved brug af et elektronisk informationssystem af væsentlige enheder som omhandlet i artikel 3, stk. 1, i direktiv (EU) 2022/2555, eller

d) andre aspekter af beskyttelsen af den offentlige interesse.

De foranstaltninger, der er omhandlet i første afsnit, kan omfatte foranstaltninger til at sikre, at det pågældende produkt med digitale elementer og de processer, som fabrikanten har indført, ikke længere udgør de relevante risici, når det gøres tilgængeligt på markedet, tilbagetrækning fra markedet af det pågældende produkt med digitale elementer eller tilbagekaldelse af det, og de skal stå i et rimeligt forhold til arten af disse risici.

2. Fabrikanten eller andre relevante erhvervsdrivende sikrer, at der træffes korrigerende foranstaltninger med hensyn til de produkter med digitale elementer, som de har gjort tilgængelige på markedet i hele Unionen, inden for den tidsfrist, der er fastsat af medlemsstatens i stk. 1 omhandlede markedsovervågningsmyndighed.

3. Medlemsstaten underretter omgående Kommissionen og de øvrige medlemsstater om de foranstaltninger, der er truffet i henhold til stk. 1. Denne underretning skal omfatte alle tilgængelige oplysninger, særlig de data, der er nødvendige til identifikation af de pågældende produkter med digitale elementer, disse produkters oprindelse og forsyningskæde, arten af den pågældende risiko og arten og varigheden af de trufne nationale foranstaltninger.

4. Kommissionen drøfter straks spørgsmålet med medlemsstaterne og den relevante erhvervsdrivende og evaluerer de trufne nationale foranstaltninger. På grundlag af resultaterne af denne evaluering træffer Kommissionen afgørelse om, hvorvidt foranstaltningen er berettiget eller ej, og foreslår om nødvendigt passende foranstaltninger.

5. Kommissionen retter den i stk. 4 omhandlede afgørelse til medlemsstaterne.

6. Hvor Kommissionen har tilstrækkelig grund til at antage, herunder på grundlag af oplysninger fra ENISA, at et produkt med digitale elementer, selv om det overholder denne forordning, udgør de i denne artikels stk. 1 omhandlede risici, skal den informere den relevante markedsovervågningsmyndighed eller de relevante markedsovervågningsmyndigheder og kan anmode den eller dem om at foretage en evaluering og følge de procedurer, der er omhandlet i artikel 54 og i nærværende artikels stk. 1, 2 og 3.

7. Under omstændigheder, der berettiger et hurtigt indgreb for at bevare et velfungerende indre marked, og hvor Kommissionen har tilstrækkelig grund til at antage, at det i stk. 6 omhandlede produkt med digitale elementer fortsat udgør de i stk. 1 omhandlede risici, og de relevante nationale markedsovervågningsmyndigheder ikke har truffet effektive foranstaltninger, foretager Kommissionen en evaluering af risiciene forbundet med det pågældende produkt med digitale elementer og kan anmode ENISA om at fremlægge en analyse for at understøtte denne evaluering, og Kommissionen underretter de relevante markedsovervågningsmyndigheder herom. De relevante erhvervsdrivende samarbejder i nødvendigt omfang med ENISA.

8. På grundlag af den evaluering, der er omhandlet i stk. 7, kan Kommissionen beslutte, at der skal træffes en korrigerende eller restriktiv foranstaltning på EU-plan. Med henblik herpå hører den straks de berørte medlemsstater og den eller de relevante erhvervsdrivende.

9. På grundlag af den i denne artikels stk. 8 omhandlede høring kan Kommissionen vedtage gennemførelsesretsakter med henblik på at træffe afgørelse om korrigerende eller restriktive foranstaltninger på EU-plan, herunder krav om, at de pågældende produkter med digitale elementer skal trækkes tilbage fra markedet eller tilbagekaldes inden for en rimelig tidsfrist, alt efter risikoens art. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 62, stk. 2.

10. Kommissionen meddeler omgående de i stk. 9 omhandlede gennemførelsesretsakter til den eller de relevante erhvervsdrivende. Medlemsstaterne gennemfører disse gennemførelsesretsakter straks og underretter Kommissionen herom.

11. Stk. 6-10 finder anvendelse, indtil den ekstraordinære situation, der begrundede Kommissionens indgreb, ikke længere er til stede, og så længe det pågældende produkt med digitale elementer fortsat udgør de i stk. 1 omhandlede risici.

Artikel 58

Formel manglende overholdelse

1. Hvor en medlemsstats markedsovervågningsmyndighed konstaterer et af følgende forhold, pålægger myndigheden den pågældende fabrikant at bringe den manglende overholdelse til ophør:

a) CE-mærkningen er anbragt i strid med artikel 29 og 30

b) CE-mærkningen er ikke anbragt

c) EU-overensstemmelseserklæringen er ikke udarbejdet

d) EU-overensstemmelseserklæringen er ikke udarbejdet korrekt

e) identifikationsnummeret på det bemyndigede organ, der er involveret i overensstemmelsesvurderingsproceduren, hvor dette er relevant, er ikke anbragt

f) den tekniske dokumentation mangler eller er ufuldstændig.

2. Hvis den i stk. 1 omhandlede manglende overholdelse varer ved, træffer den pågældende medlemsstat alle nødvendige foranstaltninger til at begrænse eller forbyde tilgængeliggørelsen af produktet med digitale elementer på markedet eller sikre, at det tilbagekaldes eller trækkes tilbage fra markedet.

Artikel 59

Markedsovervågningsmyndighedernes fælles aktiviteter

1. Markedsovervågningsmyndighederne kan aftale med andre relevante myndigheder at gennemføre fælles aktiviteter, der har til formål at sikre cybersikkerhed og forbrugerbeskyttelse for så vidt angår specifikke produkter med digitale elementer, der bringes i omsætning eller gøres tilgængelige på markedet, navnlig produkter med digitale elementer, der ofte viser sig at udgøre en cybersikkerhedsrisiko.

2. Kommissionen eller ENISA foreslår fælles aktiviteter til kontrol af overholdelsen af denne forordning, der skal udføres af markedsovervågningsmyndighederne på grundlag af tegn på eller oplysninger om, at kravene i denne forordning til produkter med digitale elementer, der falder inden for denne forordnings anvendelsesområde, muligvis ikke overholdes i flere medlemsstater.

3. Markedsovervågningsmyndighederne og, i givet fald, Kommissionen sikrer, at aftalen om at udføre fælles aktiviteter ikke medfører illoyal konkurrence mellem de erhvervsdrivende og ikke påvirker aftaleparternes objektivitet, uafhængighed og uvildighed negativt.

4. En markedsovervågningsmyndighed kan anvende alle oplysninger, der er opnået som resultat af de fælles aktiviteter, der gennemføres som led i en undersøgelse, som den iværksætter.

5. Den pågældende markedsovervågningsmyndighed og, i givet fald, Kommissionen gør aftalen om fælles aktiviteter, herunder de involverede parters navne, tilgængelig for offentligheden.

Artikel 60

Kontrolaktioner

1. Markedsovervågningsmyndighederne gennemfører samtidige, koordinerede kontrolaktioner af bestemte produkter med digitale elementer eller kategorier heraf for at kontrollere overholdelse eller afsløre overtrædelser af denne forordning. Disse kontrolaktioner kan omfatte inspektioner af produkter med digitale elementer, der er erhvervet under en dækidentitet.

2. Medmindre andet aftales af de involverede markedsovervågningsmyndigheder, koordinerer Kommissionen kontrolaktionerne. Kontrolaktionens koordinator gør, hvor det er hensigtsmæssigt, de samlede resultater offentligt tilgængelige.

3. Hvor ENISA i forbindelse med udførelsen af sine opgaver, herunder på grundlag af underretningerne modtaget i henhold til artikel 14, stk. 1 og 3, identificerer kategorier af produkter med digitale elementer, for hvilke der kan tilrettelægges kontrolaktioner, forelægger ENISA et forslag til kontrolaktion for den koordinator, der er omhandlet i nærværende artikels stk. 2, med henblik på markedsovervågningsmyndighedernes vurdering.

4. Ved gennemførelsen af kontrolaktioner kan de involverede kontrolovervågningsmyndigheder gøre brug af undersøgelsesbeføjelserne i artikel 52-58 og eventuelle andre beføjelser, som de er tillagt i henhold til national ret.

5. Markedsovervågningsmyndighederne kan opfordre tjenestemænd i Kommissionen og andre ledsagende personer, der er bemyndiget af Kommissionen, til at deltage i kontrolaktioner.

KAPITEL VI

DELEGEREDE BEFØJELSER OG UDVALGSPROCEDURE

Artikel 61

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 2, stk. 5, andet afsnit, artikel 7, stk. 3, artikel 8, stk. 1 og 2, artikel 13, stk. 8, fjerde afsnit, artikel 14, stk. 9, artikel 25, artikel 27, stk. 9, artikel 28, stk. 5, og artikel 31, stk. 5, tillægges Kommissionen for en periode på fem år fra den 10. december 2024. Kommissionen udarbejder en rapport vedrørende delegationen af beføjelser senest ni måneder inden udløbet af femårsperioden. Delegationen af beføjelser forlænges stiltiende for perioder af samme varighed, medmindre Europa-Parlamentet eller Rådet modsætter sig en sådan forlængelse senest tre måneder inden udløbet af hver periode.

3. Den i artikel 2, stk. 5, andet afsnit, artikel 7, stk. 3, artikel 8, stk. 1 og 2, artikel 13, stk. 8, fjerde afsnit, artikel 14, stk. 9, artikel 25, artikel 27, stk. 9, artikel 28, stk. 5, og artikel 31, stk. 5, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelse af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 2, stk. 5, andet afsnit, artikel 7, stk. 3, artikel 8, stk. 1 eller 2, artikel 13, stk. 8, fjerde afsnit, artikel 14, stk. 9, artikel 25, artikel 27, stk. 9, artikel 28, stk. 5, eller artikel 31, stk. 5, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 62

Udvalgsprocedure

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

3. Når udvalgets udtalelse indhentes efter en skriftlig procedure, afsluttes proceduren uden noget resultat, hvis formanden for udvalget træffer beslutning herom, eller et udvalgsmedlem anmoder herom inden fristen for afgivelse af udtalelsen.

KAPITEL VII

FORTROLIGHED OG SANKTIONER

Artikel 63

Fortrolighed

1. Alle parter, der involveret i anvendelsen af denne forordning, skal overholde tavshedspligten for oplysninger og data, der indhentes under udførelsen af deres opgaver og arbejde, på en sådan måde, at de navnlig beskytter:

a) intellektuelle ejendomsrettigheder og fysiske eller juridiske personers fortrolige forretningsoplysninger eller forretningshemmeligheder, herunder kildekode, med undtagelse af de tilfælde, der er omhandlet i artikel 5 i Europa-Parlamentets og Rådets direktiv (EU) 2016/943 ([37])

b) den effektive gennemførelse af denne forordning, navnlig for så vidt angår inspektioner, undersøgelser eller kontrolbesøg

c) offentlige og nationale sikkerhedsinteresser

d) strafferetlige eller administrative procedurers integritet.

2. Uden at det berører stk. 1, må oplysninger, der udveksles på fortrolig basis mellem markedsovervågningsmyndighederne og mellem markedsovervågningsmyndighederne og Kommissionen, ikke videregives uden forudgående tilladelse fra den oprindelige markedsmyndighed.

3. Stk. 1 og 2 berører ikke Kommissionens, medlemsstaternes og de bemyndigede organers rettigheder og forpligtelser med hensyn til udveksling af oplysninger og udsendelse af advarsler eller de berørte personers forpligtelse til at afgive oplysninger inden for rammerne af medlemsstaternes strafferet.

4. Kommissionen og medlemsstaterne kan om nødvendigt udveksle følsomme oplysninger med relevante myndigheder i tredjelande, med hvilke de har indgået bilaterale eller multilaterale aftaler om fortrolighed, der garanterer en tilstrækkelig grad af beskyttelse.

Artikel 64

Sanktioner

1. Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af bestemmelserne i denne forordning, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver straks Kommissionen meddelelse om disse regler og foranstaltninger og underretter den straks om senere ændringer, der berører dem.

2. Manglende opfyldelse af de væsentlige cybersikkerhedskrav i bilag I og forpligtelserne i artikel 13 og 14 straffes med administrative bøder på op til 15 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 2,5 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

3. Manglende opfyldelse af forpligtelserne i artikel 18-23, artikel 28, artikel 30, stk. 1-4, artikel 31, stk. 1-4, artikel 32, stk. 1, 2 og 3, artikel 33, stk. 5, og artikel 39, 41, 47, 49 og 53, straffes med administrative bøder på op til 10 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 2 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

4. Afgivelse af ukorrekte, ufuldstændige eller vildledende oplysninger til bemyndigede organer og markedsovervågningsmyndigheder som svar på en anmodning straffes med administrative bøder på op til 5 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 1 % af dens samlede globale årlige omsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

([37]) Europa-Parlamentets og Rådets direktiv (EU) 2016/943 af 8. juni 2016 om beskyttelse af fortrolig knowhow og fortrolige forretningsoplysninger (forretningshemmeligheder) mod ulovlig erhvervelse, brug og videregivelse (EUT L 157 af 15.6.2016, s. 1).

5. Ved fastsættelsen af den administrative bødes størrelse tages der i hvert enkelt tilfælde hensyn til alle relevante omstændigheder i den specifikke situation, og der tages behørigt hensyn til følgende:

a) overtrædelsens art, grovhed og varighed samt dens konsekvenser

b) hvorvidt de samme eller andre markedsovervågningsmyndigheder allerede har pålagt den samme erhvervsdrivende administrative bøder for en lignende overtrædelse

c) størrelsen på, navnlig med hensyn til mikrovirksomheder og små og mellemstore virksomheder, herunder nyetablerede virksomheder, og markedsandelen for den erhvervsdrivende, der har begået overtrædelsen.

6. Markedsovervågningsmyndigheder, der pålægger administrative bøder, underretter markedsovervågningsmyndighederne i andre medlemsstater om denne pålæggelse gennem det informations- og kommunikationssystem, der er omhandlet i artikel 34 i forordning (EU) 2019/1020.

7. Hver medlemsstat fastsætter regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og offentlige organer, der er etableret i den pågældende medlemsstat.

8. Afhængigt af medlemsstaternes retssystem kan reglerne om administrative bøder anvendes på en sådan måde, at bøderne pålægges af kompetente nationale domstole eller andre organer i overensstemmelse med de kompetencer, der er fastlagt på nationalt plan i de pågældende medlemsstater. Anvendelsen af sådanne regler i disse medlemsstater har tilsvarende virkning.

9. Afhængigt af omstændighederne i hver enkelt sag kan der pålægges administrative bøder i tillæg til eventuelle andre korrigerende eller restriktive foranstaltninger, som markedsovervågningsmyndighederne anvender for den samme overtrædelse.

10. Uanset stk. 3-9 finder de administrative bøder, der er omhandlet i disse stykker, ikke anvendelse på følgende:

a) fabrikanter, der betragtes som mikrovirksomheder eller små virksomheder for så vidt angår manglende overholdelse af den frist, som er omhandlet i artikel 14, stk. 2, litra a), eller artikel 14, stk. 4, litra a)

b) enhver overtrædelse af denne forordning begået af open source software-forvaltere.

Artikel 65

Gruppesøgsmål

Direktiv (EU) 2020/1828 finder anvendelse på gruppesøgsmål, som anlægges som følge af erhvervsdrivendes overtrædelser af bestemmelser i denne forordning, som skader eller kan skade forbrugernes kollektive interesser.

KAPITEL VIII

OVERGANGSBESTEMMELSER OG AFSLUTTENDE BESTEMMELSER

Artikel 66

Ændring af forordning (EU) 2019/1020

I bilag I til forordning (EU) 2019/1020 indsættes følgende punkt:

»72. Europa-Parlamentets og Rådets forordning (EU) 2024/2847 (*).

(*) Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).«

Artikel 67

Ændring af direktiv (EU) 2020/1828

I bilag I til direktiv (EU) 2020/1828 tilføjes følgende punkt:

»69. Europa-Parlamentets og Rådets forordning (EU) 2024/2847 (*).

(*) Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).«

Artikel 68

Ændring af forordning (EU) nr. 168/2013

I tabellen i del C i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 168/2013 ([38]) tilføjes følgende punkt:

»

16	18	beskyttelse af køretøjer mod cyberangreb		x	x	x	x	x	x	x	x	x	x	x	x	x	X

«

Artikel 69

Overgangsbestemmelser

1. Udstedte EU-typeafprøvningsattester og afgørelser om godkendelse vedrørende cybersikkerhedskrav til produkter med digitale elementer, der er omfattet af anden EU-harmoniseringslovgivning end denne forordning, forbliver gyldige indtil 11. juni 2028, medmindre de udløber inden denne dato, eller medmindre andet er angivet i sådan anden EU-harmoniseringslovgivning, i hvilket tilfælde de forbliver gyldige som omhandlet i den pågældende lovgivning.

2. Produkter med digitale elementer, der er bragt i omsætning inden den 11. december 2027, er kun omfattet af kravene i denne forordning, hvis disse produkter fra denne dato er genstand for væsentlige ændringer.

3. Uanset denne artikels stk. 2 finder de forpligtelser, der er fastsat i artikel 14, anvendelse på alle produkter med digitale elementer, der er omfattet af denne forordnings anvendelsesområde, og som er bragt i omsætning inden den 11. december 2027.

Artikel 70

Evaluering og revision

1. Senest den 11. december 2030 og hvert fjerde år derefter forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision af denne forordning. Disse rapporter offentliggøres.

2. Senest den 11. september 2028 forelægger Kommissionen efter høring af ENISA og CSIRT-netværket en rapport for Europa-Parlamentet og Rådet med en vurdering af effektiviteten af den fælles indberetningsplatform, der er fastsat i artikel 16, og indvirkningen af anvendelsen af de cybersikkerhedsrelaterede grunde, der er omhandlet i artikel 16, stk. 2, af de CSIRT'er, der er udpeget som koordinatorer, på effektiviteten af den fælles indberetningsplatform for så vidt angår rettidig formidling af modtagne underretninger til andre relevante CSIRT'er.

Artikel 71

Ikrafttræden og anvendelse

1. Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

([38]) Europa-Parlamentets og Rådets forordning (EU) nr. 168/2013 af 15. januar 2013 om godkendelse og markedsovervågning af to- og trehjulede køretøjer samt quadricykler (EUT L 60 af 2.3.2013, s. 52).

2. Denne forordning finder anvendelse fra den 11. december 2027.

Artikel 14 finder dog anvendelse fra den 11. september 2026, og kapitel IV (artikel 35 til 51) finder anvendelse fra den 11. juni 2026.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Strasbourg, den 23. oktober 2024.

På Europa-Parlamentets vegne	*På Rådets vegne*
R. METSOLA	ZSIGMOND B. P.
Formand	*Formand*

BILAG I

VÆSENTLIGE CYBERSIKKERHEDSKRAV

Del I Cybersikkerhedskrav vedrørende egenskaberne ved produkter med digitale elementer

1) Produkter med digitale elementer skal designes, udvikles og produceres på en sådan måde, at de sikrer et passende cybersikkerhedsniveau baseret på risiciene.

2) På grundlag af den cybersikkerhedsrisikovurdering, der er omhandlet i artikel 13, stk. 2, og hvor det er relevant, skal produkter med digitale elementer:

   a) gøres tilgængelige på markedet uden kendte sårbarheder, der kan udnyttes

   b) gøres tilgængelige på markedet med en sikker konfiguration som standard, medmindre andet er aftalt mellem fabrikanten og erhvervsbrugeren i forbindelse med et skræddersyet produkt med digitale elementer, herunder muligheden for at nulstille produktet til dets oprindelige tilstand

   c) sikre, at sårbarheder kan afhjælpes gennem sikkerhedsopdateringer, herunder, hvor det er relevant, ved hjælp af automatiske sikkerhedsopdateringer, der som standardindstilling installeres, inden for en passende tidsramme, med en klar og brugervenlig fravalgsmekanisme og gennem underretning af brugerne om tilgængelige opdateringer og muligheden for midlertidigt at udsætte dem

   d) sikre beskyttelse mod uautoriseret adgang ved hjælp af passende kontrolmekanismer, herunder, men ikke begrænset til, autentificerings-, identitets- eller adgangsstyringssystemer, og give melding om mulig ikkeautoriseret adgang

   e) beskytte fortroligheden af opbevarede, videresendte eller på anden måde behandlede personoplysninger eller andre data, såsom ved at kryptere relevante data i hvile eller i transit ved brug af mekanismer på det aktuelle tekniske niveau og ved brug af andre tekniske midler

   f) beskytte integriteten af opbevarede, videresendte eller på anden måde behandlede personoplysninger eller andre data, kommandoer, programmer og konfigurationer mod enhver manipulation eller ændring, som brugeren ikke har givet tilladelse til, og give melding om korruption

   g) kun behandle personoplysninger eller andre data, der er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til det tilsigtede formål med produktet med digitale elementer (»dataminimering«)

   h) beskytte tilgængeligheden af væsentlige og grundlæggende funktioner, også efter en hændelse, herunder gennem modstandsdygtigheds- og afbødningsforanstaltninger mod denial of service-angreb

   i) minimere den negative indvirkning af selve produkterne eller forbundne enheder på tilgængeligheden af tjenester, der leveres af andre enheder eller netværk

   j) designes, udvikles og produceres med henblik på at begrænse angrebsflader, herunder eksterne grænseflader

   k) designes, udvikles og produceres med henblik på at mindske virkningen af en hændelse ved hjælp af passende mekanismer og teknikker til begrænsning af udnyttelsen

   l) levere sikkerhedsrelaterede oplysninger ved at registrere og overvåge relevante interne aktiviteter, herunder adgang til eller ændring af data, tjenester eller funktioner, med en fravalgsmekanisme for brugeren

   m) give brugerne mulighed for på sikker og nem vis at fjerne alle data og indstillinger på permanent basis og, hvis sådanne data kan overføres til andre produkter eller systemer, sikre, at dette gøres på en sikker måde.

Del II Krav til håndtering af sårbarheder

Fabrikanter af produkter med digitale elementer skal:

1) identificere og dokumentere sårbarheder og komponenter i produkter med digitale elementer, herunder ved at udarbejde en softwarekomponentliste i et almindeligt anvendt og maskinlæsbart format, der som minimum dækker de vigtigste produktafhængigheder

2) i forbindelse med risiciene forbundet med produkter med digitale elementer straks håndtere og afhjælpe sårbarheder, herunder ved at sørge for sikkerhedsopdateringer, og hvor det er teknisk muligt, skal nye sikkerhedsopdateringer leveres adskilt fra funktionalitetsopdateringer

3) anvende effektive og regelmæssige afprøvninger og gennemgange af sikkerheden af produktet med digitale elementer

4) når en sikkerhedsopdatering er gjort tilgængelig, dele og offentliggøre oplysninger om afhjulpne sårbarheder, herunder en beskrivelse af sårbarhederne, oplysninger, der gør det muligt for brugerne at identificere det berørte produkt med digitale elementer, sårbarhedernes indvirkning og alvor, og tydelige og tilgængelige oplysninger, der gør det lettere for brugerne at afhjælpe sårbarhederne; i behørigt begrundede tilfælde, hvor fabrikanterne mener, at sikkerhedsrisiciene ved offentliggørelse opvejer sikkerhedsfordelene, kan de udsætte offentliggørelsen af oplysninger om en afhjulpen sårbarhed, indtil brugerne har fået mulighed for at anvende den relevante rettelse

5) indføre og håndhæve en politik for koordineret offentliggørelse af sårbarheder

6) træffe foranstaltninger til at lette udvekslingen af oplysninger om potentielle sårbarheder i deres produkt med digitale elementer samt i tredjepartskomponenter indeholdt i det pågældende produkt, herunder ved at anføre en kontaktadresse til indberetning af de sårbarheder, der opdages i produktet med digitale elementer

7) sørge for mekanismer til sikker distribution af opdateringer for produkter med digitale elementer for at sikre, at sårbarheder afhjælpes eller afbødes rettidigt og, hvor det er relevant for sikkerhedsopdateringer, automatisk

8) sikre, at tilgængelige sikkerhedsopdateringer til afhjælpning af identificerede sikkerhedsproblemer formidles uden unødigt ophold og, medmindre andet er aftalt mellem en fabrikant og en erhvervsbruger i forhold til et skræddersyet produkt med digitale elementer, gratis sammen med vejledende meddelelser, der giver brugerne de relevante oplysninger, herunder om mulige foranstaltninger, der skal træffes.

BILAG II

OPLYSNINGER OG ANVISNINGER TIL BRUGEREN

Produktet med digitale elementer skal som minimum ledsages af:

1. Fabrikantens navn, registrerede firmanavn eller registrerede varemærke og postadresse, e-mailadresse eller andre digitale kontaktoplysninger samt, hvis et sådant foreligger, det websted, hvor fabrikanten kan kontaktes
2. det centrale kontaktpunkt, hvor oplysninger om sårbarheder i produktet med digitale elementer kan indberettes og modtages, og hvor fabrikantens politik for koordineret offentliggørelse af sårbarheder kan findes
3. navn og type og eventuelle yderligere oplysninger, der gør det muligt entydigt at identificere produktet med digitale elementer
4. det tilsigtede formål med produktet med digitale elementer, herunder det sikkerhedsmiljø, som fabrikanten leverer, samt produktets væsentlige funktioner og oplysninger om sikkerhedsegenskaberne
5. alle kendte eller forudsigelige omstændigheder vedrørende anvendelsen af produktet med digitale elementer i overensstemmelse med dets tilsigtede formål eller ved fejlanvendelse, der med rimelighed kan forudses, der kan medføre betydelige cybersikkerhedsrisici
6. i givet fald den internetadresse, hvor der er adgang til EU-overensstemmelseserklæringen
7. den type tekniske sikkerhedsstøtte, som fabrikanten tilbyder, og slutdatoen for den supportperiode, hvor brugerne kan forvente, at sårbarheder håndteres, og hvor brugerne kan forvente at modtage sikkerhedsopdateringer
8. detaljerede anvisninger eller en internetadresse med henvisning til sådanne detaljerede anvisninger og oplysninger om:
   a) de nødvendige foranstaltninger ved første ibrugtagning og i hele levetiden for produktet med digitale elementer for at sikre en sikker anvendelse heraf
   b) hvordan ændringer af produktet med digitale elementer kan påvirke datasikkerheden
   c) hvordan sikkerhedsrelevante opdateringer kan installeres
   d) sikker nedlukning af produktet med digitale elementer, herunder oplysninger om, hvordan brugerdata kan fjernes sikkert
   e) hvordan den standardindstilling, der muliggør automatisk installation af sikkerhedsopdateringer som krævet af bilag I, del I, nr. 2, litra c), kan slås fra
   f) hvor produktet med digitale elementer er beregnet til at blive integreret i andre produkter med digitale elementer, de oplysninger, der er nødvendige for, at integratoren kan opfylde de væsentlige cybersikkerhedskrav, der er fastlagt i bilag I, og de dokumentationskrav, der er fastlagt i bilag VII
9. hvis fabrikanten beslutter at stille softwarekomponentlisten til rådighed for brugeren, oplysninger om, hvor softwarekomponentlisten kan tilgås.

BILAG III

VIGTIGE PRODUKTER MED DIGITALE ELEMENTER

Klasse I

1. Software og hardware til identitetsstyringssystemer og til styring af privilegeret adgang, herunder autentificerings- og adgangskontrollæsere, herunder biometriske læsere
2. Enkeltstående og indlejrede browsere
3. Adgangskoder
4. Software, der søger efter, fjerner eller sætter ondsindet software i karantæne
5. Produkter med digitale elementer, der fungerer som et virtuelt privat netværk (VPN)
6. Netstyringssystemer
7. Systemer til sikkerhedsinformations- og hændelseshåndtering (SIEM)
8. Boot managers
9. Public key-infrastruktur og software for udstedelse af digitale certifikater
10. Fysiske og virtuelle netværksgrænseflader
11. Operativsystemer
12. Routere, modemmer til internetforbindelse og afbrydere
13. Mikroprocessorer med sikkerhedsrelaterede funktioner
14. Mikrocontrollere med sikkerhedsrelaterede funktioner
15. Applikationsspecifikke integrerede kredsløb (ASIC) og programmerbare porte (FPPT) med sikkerhedsrelaterede funktioner
16. Virtuelle assistenter til generelle formål i intelligente bygninger
17. Produkter til intelligente bygninger med sikkerhedsfunktioner, herunder intelligente dørlåse, sikkerhedskameraer, systemer til overvågning af spædbørn og alarmsystemer
18. Internetforbundet legetøj, der er omfattet af Europa-Parlamentets og Rådets direktiv 2009/48/EF ([1]), og som har sociale interaktive funktioner (f.eks. at det kan tale eller filme), eller som har lokaliseringsfunktioner
19. Personlige wearable-produkter, der skal bæres af eller anbringes på et menneskelegeme, og som har et sundhedsovervågningsformål (såsom sporing), og som forordning (EU) 2017/745 eller (EU) 2017/746 ikke finder anvendelse på, eller personlige wearable-produkter, der skal anvendes af og til børn.

Klasse II

1. Hypervisorer og container runtime-systemer, der understøtter virtuel udførelse af operativsystemer og lignende miljøer
2. Firewalls, systemer til opdagelse og forebyggelse af indtrængen
3. Mikroprocessorer, der er sikret mod manipulation
4. Mikrocontrollere, der er sikret mod manipulation.

([1]) Europa-Parlamentets og Rådets direktiv 2009/48/EF af 18. juni 2009 om sikkerhedskrav til legetøj (EUT L 170 af 30.6.2009, s. 1).

BILAG IV

KRITISKE PRODUKTER MED DIGITALE ELEMENTER

1. Hardwareenheder med sikkerhedsbokse.
2. Gateways til intelligente målere inden for intelligente målersystemer som defineret i artikel 2, nr. 23), i Europa-Parlamentets og Rådets direktiv (EU) 2019/944 ([1]) og andre enheder til avancerede sikkerhedsformål, herunder til sikker krypteringsbehandling.
3. Smartcards eller lignende enheder, herunder sikre elementer.

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2019/944 af 5. juni 2019 om fælles regler for det indre marked for elektricitet og om ændring af direktiv 2012/27/EU (EUT L 158 af 14.6.2019, s. 125).

BILAG V

EU-OVERENSSTEMMELSESERKLÆRING

Den i artikel 28 omhandlede EU-overensstemmelseserklæring skal indeholde følgende oplysninger:

1. Navn og type og eventuelle yderligere oplysninger, der gør det muligt entydigt at identificere produktet med digitale elementer.
2. Navn og adresse på fabrikanten eller dennes bemyndigede repræsentant.
3. En erklæring om, at EU-overensstemmelseserklæringen udstedes på udbyderens eksklusive ansvar.
4. Erklæringens genstand (identifikation af produktet med digitale elementer, så det kan spores, hvilket kan omfatte et foto, hvor det er relevant).
5. En erklæring om, at genstanden for erklæringen beskrevet ovenfor er i overensstemmelse med den relevante EU-harmoniseringslovgivning.
6. Henvisninger til de relevante anvendte harmoniserede standarder eller referencer til anden fælles specifikation eller cybersikkerhedscertificering, som der erklæres overensstemmelse med.
7. Hvis det er relevant, navnet og nummeret på det bemyndigede organ, en beskrivelse af den udførte overensstemmelsesvurderingsprocedure og identifikation af den udstedte attest.
8. Yderligere oplysninger:

   Underskrevet for og på vegne af:

   (udstedelsessted og -dato):

   (navn, stilling) (underskrift):

BILAG VI

FORENKLET EU-OVERENSSTEMMELSESERKLÆRING

Den i artikel 13, stk. 20, omhandlede forenklede EU-overensstemmelseserklæring udformes som følger:

… [fabrikantens navn] erklærer herved, at typen af produktet med digitale elementer … [betegnelse for type af produkt med digitale elementer] er i overensstemmelse med forordning (EU) 2024/2847 ([1]).

EU-overensstemmelseserklæringens fulde tekst kan findes på følgende internetadresse: …

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

BILAG VII

INDHOLD AF DEN TEKNISKE DOKUMENTATION

Den i artikel 31 omhandlede tekniske dokumentation skal som minimum indeholde følgende oplysninger, alt efter hvad der er relevant for det pågældende produkt med digitale elementer:

1. en generel beskrivelse af produktet med digitale elementer, herunder:
   a) dets tilsigtede formål
   b) softwareversioner, der påvirker overholdelsen af de væsentlige cybersikkerhedskrav
   c) hvis produktet med digitale elementer er et hardwareprodukt, fotografier eller illustrationer af dets eksterne elementer, mærkninger og intern indretning
   d) oplysninger og anvisninger til brugeren som anført bilag II
2. en beskrivelse af design, udvikling og produktion af produktet med digitale elementer og af sårbarhedshåndteringsprocesser, herunder:
   a) nødvendige oplysninger om design og udvikling af produktet med digitale elementer, herunder i givet fald tegninger og skemaer og en beskrivelse af systemarkitekturen, der forklarer, hvordan softwarekomponenter bygger på eller indgår i hinanden og integreres i den samlede behandling
   b) nødvendige oplysninger om og specifikationer for de sårbarhedshåndteringsprocesser, som fabrikanten har indført, herunder softwarekomponentlisten, politikken for koordineret offentliggørelse af sårbarheder, dokumentation for angivelse af en kontaktadresse til indberetning af sårbarheder og en beskrivelse af de tekniske løsninger, der er valgt til sikker distribution af opdateringer
   c) nødvendige oplysninger om og specifikationer for produktions- og overvågningsprocesserne for produktet med digitale elementer og validering af disse processer
3. en vurdering af de cybersikkerhedsrisici, som produktet med digitale elementer i henhold til artikel 13 designes, udvikles, produceres, leveres og vedligeholdes til at beskytte imod, herunder hvordan de væsentlige cybersikkerhedskrav i bilag I, del 1, finder anvendelse
4. relevante oplysninger, der blev taget i betragtning ved fastlæggelsen af supportperioden i henhold til artikel 13, stk. 8, for produktet med digitale elementer
5. en liste over de helt eller delvist anvendte harmoniserede standarder, hvis referencer er offentliggjort i *Den Europæiske Unions Tidende*, fælles specifikationer som fastsat i denne forordnings artikel 27 eller europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til forordning (EU) 2019/881 i henhold til nærværende forordnings artikel 27, stk. 8, og, hvor disse harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger ikke er blevet anvendt, beskrivelser af de løsninger, der er anvendt for at opfylde de væsentlige cybersikkerhedskrav i bilag I, del I og II, herunder en liste over andre relevante tekniske specifikationer, som er anvendt. I tilfælde af delvis anvendelse af harmoniserede standarder, fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger skal den tekniske dokumentation angive, hvilke dele der er anvendt
6. rapporter om de afprøvninger, der er foretaget for at kontrollere, at produktet med digitale elementer og sårbarhedshåndteringsprocesserne opfylder de gældende væsentlige cybersikkerhedskrav som fastsat i bilag I, del I og II
7. en kopi af EU-overensstemmelseserklæringen
8. i givet fald softwarekomponentlisten efter en begrundet anmodning fra en markedsovervågningsmyndighed, forudsat at det er nødvendigt for, at denne myndighed kan kontrollere overholdelsen af de væsentlige cybersikkerhedskrav i bilag I.

BILAG VIII

OVERENSSTEMMELSESVURDERINGSPROCEDURER

Del I Overensstemmelsesvurderingsprocedure på grundlag af intern kontrol (baseret på modul A)

1. Intern kontrol er den procedure for overensstemmelsesvurdering, hvorved fabrikanten opfylder forpligtelserne i denne dels punkt 2, 3 og 4 og på eget eksklusive ansvar sikrer og erklærer, at produkterne med digitale elementer opfylder alle de væsentlige cybersikkerhedskrav i bilag I, del I, og at fabrikanten opfylder de væsentlige cybersikkerhedskrav i bilag I, del II.

2. Fabrikanten udarbejder den tekniske dokumentation, der er beskrevet i bilag VII.

3. Design, udvikling, produktion og håndtering af sårbarheder i produkter med digitale elementer

   Fabrikanten træffer alle nødvendige foranstaltninger for, at det i forbindelse med design, udvikling og produktion og sårbarhedshåndteringsprocesserne og overvågningen heraf sikres, at de fremstillede eller udviklede produkter med digitale elementer og de procedurer, som fabrikanten har indført, opfylder de væsentlige cybersikkerhedskrav i bilag I, del I og II.

4. Overensstemmelsesmærkning og overensstemmelseserklæring

   4.1. Fabrikanten anbringer CE-mærkningen på hvert enkelt produkt med digitale elementer, der opfylder kravene i denne forordning.

   4.2. Fabrikanten udarbejder en skriftlig EU-overensstemmelseserklæring for hvert enkelt produkt med digitale elementer i overensstemmelse med artikel 28 og opbevarer den sammen med den tekniske dokumentation, så den står til rådighed for de nationale myndigheder i ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst. Det skal af EU-overensstemmelseserklæringen fremgå, hvilket produkt med digitale elementer den vedrører. Et eksemplar af EU-overensstemmelseserklæringen stilles efter anmodning til rådighed for de relevante myndigheder.

5. Bemyndigede repræsentanter

   Fabrikantens forpligtelser i punkt 4 kan opfyldes af dennes bemyndigede repræsentant på fabrikantens vegne og ansvar, forudsat at de relevante forpligtelser er angivet i fuldmagten.

Del II EU-typeafprøvning (baseret på modul B)

1. EU-typeafprøvning er den del af overensstemmelsesvurderingsproceduren, hvor et bemyndiget organ undersøger det tekniske design og udviklingen af et produkt med digitale elementer og de sårbarhedshåndteringsprocesser, som fabrikanten har indført, og attesterer, at et produkt med digitale elementer opfylder de væsentlige cybersikkerhedskrav i bilag I, del I, og at fabrikanten opfylder de væsentlige cybersikkerhedskrav i bilag I, del II.

2. EU-typeafprøvning udføres som en vurdering af egnetheden af det tekniske design og udviklingen af et produkt med digitale elementer ved undersøgelse af den tekniske dokumentation og den støttedokumentation, der er omhandlet i punkt 3, samt undersøgelse af prøveeksemplarer af en eller flere kritiske dele af produktet (kombination af produktionstype og designtype)

3. Fabrikanten indgiver ansøgning om EU-typeafprøvning til et enkelt bemyndiget organ efter eget valg.

   Ansøgningen skal indeholde:

   3.1. fabrikantens navn og adresse samt, hvis ansøgningen indgives af den bemyndigede repræsentant, denne bemyndigede repræsentants navn og adresse

   3.2. en skriftlig erklæring om, at samme ansøgning ikke er indgivet til et andet bemyndiget organ

   3.3. den tekniske dokumentation, der skal gøre det muligt at vurdere, om produktet med digitale elementer er i overensstemmelse med de gældende væsentlige cybersikkerhedskrav i bilag I, del I, og fabrikantens sårbarhedshåndteringsprocesser i bilag I, del II, og skal indeholde en fyldestgørende analyse og vurdering af risiciene. Den tekniske dokumentation skal angive de gældende krav og skal, i det omfang det er relevant for vurderingen, omfatte designet, fremstillingen og brugen af produktet med digitale elementer. Den tekniske dokumentation skal, hvor det er relevant, mindst indeholde de elementer, der er anført i bilag VII

3.4. støttedokumentationen, der viser egnetheden af de tekniske design- og udviklingsløsninger og sårbarhedshåndteringsprocesserne. I denne støttedokumentation skal nævnes al dokumentation, der er blevet anvendt, særlig hvis de relevante harmoniserede standarder eller tekniske specifikationer ikke er blevet anvendt fuldt ud. I støttedokumentationen skal om nødvendigt indgå resultaterne af afprøvninger, som er blevet foretaget af fabrikantens laboratorium eller af et andet afprøvningslaboratorium på fabrikantens vegne og ansvar.

4. Det bemyndigede organ skal træffe følgende foranstaltninger:

4.1. undersøge den tekniske dokumentation og støttedokumentationen for at vurdere tilstrækkeligheden af det tekniske design og udviklingen af produktet med digitale elementer for så vidt angår de væsentlige cybersikkerhedskrav i bilag I, del I, og af de sårbarhedshåndteringsprocesser, som fabrikanten har indført, for så vidt angår de væsentlige cybersikkerhedskrav i bilag I, del II

4.2. kontrollere, at prøveeksemplarer er udviklet og fremstillet i overensstemmelse med den tekniske dokumentation, og fastslå, hvilke elementer der er designet og udviklet i overensstemmelse med de relevante bestemmelser i de pågældende harmoniserede standarder eller tekniske specifikationer, samt hvilke elementer der er designet og udviklet uden anvendelse af de relevante bestemmelser i disse standarder

4.3. foretage eller lade foretage de nødvendige undersøgelser og afprøvninger til at kontrollere, at de relevante harmoniserede standarder eller tekniske specifikationer for kravene i bilag I er blevet anvendt korrekt, såfremt fabrikanten har valgt at anvende de løsninger, der er nævnt heri

4.4. foretage eller lade foretage de nødvendige undersøgelser og afprøvninger til at kontrollere, at fabrikantens løsninger opfylder de væsentlige cybersikkerhedskrav, såfremt fabrikanten ikke har anvendt de løsninger, der er omhandlet i de relevante harmoniserede standarder eller tekniske specifikationer for kravene i bilag I

4.5. aftale med fabrikanten, hvor undersøgelserne og afprøvningerne skal foretages.

5. Det bemyndigede organ udarbejder en evalueringsrapport om aktiviteterne udført i overensstemmelse med punkt 4 og resultatet af disse. Uden at dette berører det bemyndigede organs ansvar over for de bemyndigende myndigheder, offentliggør det bemyndigede organ ikke indholdet af denne rapport, hverken helt eller delvist, uden fabrikantens samtykke.

6. Hvor typen og sårbarhedshåndteringsprocesserne opfylder de væsentlige cybersikkerhedskrav i bilag I, udsteder det bemyndigede organ en EU-typeafprøvningsattest til fabrikanten. Attesten skal indeholde fabrikantens navn og adresse, undersøgelsens konklusioner, eventuelle betingelser for attestens gyldighed og de oplysninger, der er nødvendige for at identificere den godkendte type og sårbarhedshåndteringsprocesserne. Attesten kan have et eller flere bilag.

Attesten og bilagene dertil skal indeholde alle relevante oplysninger for at gøre det muligt at vurdere, om fremstillede eller udviklede produkter med digitale elementer er i overensstemmelse med den undersøgte type og de undersøgte sårbarhedshåndteringsprocesser, og at foretage kontrol under brug.

Hvor typen og sårbarhedshåndteringsprocesserne ikke opfylder de relevante væsentlige cybersikkerhedskrav i bilag I, afviser det bemyndigede organ at udstede en EU-typeafprøvningsattest og oplyser ansøgeren herom med en detaljeret begrundelse for afslaget.

7. Det bemyndigede organ holder sig ajour med eventuelle ændringer i det generelt anerkendte aktuelle tekniske niveau, som tyder på, at den godkendte type og sårbarhedshåndteringsprocesserne måske ikke længere opfylder de relevante væsentlige cybersikkerhedskrav i bilag I, og beslutter, om sådanne ændringer kræver yderligere undersøgelser. I bekræftende fald underretter det bemyndigede organ fabrikanten herom.

Fabrikanten underretter det bemyndigede organ, som opbevarer den tekniske dokumentation vedrørende EU-typeafprøvningsattesten, om enhver ændring af den godkendte type og sårbarhedshåndteringsprocesserne, som kan påvirke overensstemmelsen med de væsentlige cybersikkerhedskrav i bilag I eller betingelserne for attestens gyldighed. Sådanne ændringer kræver en tillægsgodkendelse i form af en tilføjelse til den oprindelige EU-typeafprøvningsattest.

8. Det bemyndigede organ aflægger regelmæssigt kontrolbesøg for at sikre, at sårbarhedshåndteringsprocesserne som fastsat i bilag I, del II, gennemføres på passende vis.

9. Hvert bemyndiget organ oplyser dets bemyndigende myndigheder om de EU-typeafprøvningsattester og tillæg hertil, som det har udstedt eller trukket tilbage, og stiller med jævne mellemrum eller efter anmodning listen over attester og eventuelle tillæg hertil, der er blevet afvist, suspenderet eller på anden måde begrænset, til rådighed for dets bemyndigende myndigheder

   Hvert bemyndiget organ oplyser de øvrige bemyndigede organer om de EU-typeafprøvningsattester og tillæg hertil, som det har afvist, trukket tilbage, suspenderet eller på anden måde begrænset, og, efter anmodning, om attester og tillæg hertil, som det har udstedt.

   Kommissionen, medlemsstaterne og de øvrige bemyndigede organer kan efter anmodning få en kopi af EU-typeafprøvningsattesterne og eventuelle tillæg hertil. Efter anmodning kan Kommissionen og medlemsstaterne få en kopi af den tekniske dokumentation og resultaterne af de undersøgelser, som det bemyndigede organ har foretaget. Det bemyndigede organ opbevarer en kopi af EU-typeafprøvningsattesten, bilagene og tillæggene hertil samt den tekniske dokumentation, herunder den dokumentation, som fabrikanten har indgivet, indtil udløbet af attestens gyldighedsperiode.

10. Fabrikanten opbevarer en kopi af EU-typeafprøvningsattesten, bilagene og tillæggene hertil samt den tekniske dokumentation, så disse dokumenter står til rådighed for de nationale myndigheder i ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst.

11. Fabrikantens bemyndigede repræsentant kan indgive den i punkt 3 omhandlede ansøgning og opfylde de i punkt 7 og 10 omhandlede forpligtelser, forudsat at de relevante forpligtelser er angivet i fuldmagten.

Del III Typeoverensstemmelse på grundlag af intern produktionskontrol (baseret på modul C)

1. Typeoverensstemmelse på grundlag af intern produktionskontrol er den del af overensstemmelsesvurderingsproceduren, hvorved fabrikanten opfylder forpligtelser i denne dels punkt 2 og 3 og sikrer og erklærer, at produkterne med digitale elementer er i overensstemmelse med den type, der er beskrevet i EU-typeafprøvningsattesten, og opfylder de væsentlige cybersikkerhedskrav i bilag I, del I, og at fabrikanten opfylder de væsentlige cybersikkerhedskrav i bilag I, del II.

2. Produktion

   Fabrikanten træffer alle nødvendige foranstaltninger for, at det ved produktionen og overvågningen heraf sikres, at de fremstillede produkter med digitale elementer er i overensstemmelse med den godkendte type beskrevet i EU-typeafprøvningsattesten og opfylder de væsentlige cybersikkerhedskrav i bilag I, del I, og sikrer, at fabrikanten opfylder de væsentlige cybersikkerhedskrav i bilag I, del II.

3. Overensstemmelsesmærkning og overensstemmelseserklæring

   3.1. Fabrikanten anbringer CE-mærkningen på hvert enkelt produkt med digitale elementer, som er i overensstemmelse med typen beskrevet i EU-typeafprøvningsattesten, og som opfylder de relevante krav i denne forordning.

   3.2. Fabrikanten udarbejder en skriftlig overensstemmelseserklæring for hver produktmodel og opbevarer den, så den står til rådighed for de nationale myndigheder i ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst. Det skal af overensstemmelseserklæringen fremgå, hvilken produktmodel den vedrører. Et eksemplar af overensstemmelseserklæringen stilles efter anmodning til rådighed for de relevante myndigheder.

4. Bemyndiget repræsentant

   Fabrikantens forpligtelser i henhold til punkt 3 kan opfyldes af dennes bemyndigede repræsentant på fabrikantens vegne og ansvar, forudsat at de relevante forpligtelser er angivet i fuldmagten.

Del IV Overensstemmelse på grundlag af fuld kvalitetssikring (baseret på modul H)

1. Overensstemmelse på grundlag af fuld kvalitetssikring er den procedure for overensstemmelsesvurdering, hvorved fabrikanten opfylder forpligtelserne i denne dels punkt 2 og 5 og på eget eksklusive ansvar sikrer og erklærer, at de pågældende produkter med digitale elementer eller produktkategorier opfylder de væsentlige cybersikkerhedskrav i bilag I, del I, og at de sårbarhedshåndteringsprocesser, som fabrikanten har indført, opfylder kravene i bilag I, del II.

2. Design, udvikling, produktion og håndtering af sårbarheder i produkter med digitale elementer

Fabrikanten skal ved design, udvikling og endelig produktinspektion og -afprøvning af de pågældende produkter med digitale elementer og ved håndtering af sårbarheder anvende et godkendt kvalitetsstyringssystem som angivet i punkt 3, sikre dets effektivitet i hele supportperioden og være underlagt overvågning som angivet i punkt 4.

3. Kvalitetsstyringssystem

3.1. Fabrikanten indgiver en ansøgning om vurdering af kvalitetsstyringssystemet for de pågældende produkter med digitale elementer til et bemyndiget organ efter eget valg.

Ansøgningen skal indeholde:

a) fabrikantens navn og adresse samt, hvis ansøgningen indgives af den bemyndigede repræsentant, denne bemyndigede repræsentants navn og adresse

b) den tekniske dokumentation for en model af hver kategori af produkter med digitale elementer, der påtænkes fremstillet eller udviklet. Den tekniske dokumentation skal, hvor det er relevant, mindst indeholde de elementer, der er anført i bilag VII

c) dokumentation vedrørende kvalitetsstyringssystemet, og

d) en skriftlig erklæring om, at samme ansøgning ikke er blevet indgivet til et andet bemyndiget organ.

3.2. Kvalitetsstyringssystemet skal sikre, at produkterne med digitale elementer opfylder de væsentlige cybersikkerhedskrav i bilag I, del I, og at de sårbarhedshåndteringsprocesser, som fabrikanten har indført, opfylder kravene i bilag I, del II.

Alle de forhold, krav og bestemmelser, som fabrikanten har taget hensyn til, skal dokumenteres på en systematisk og overskuelig måde i form af skriftlige politikker, procedurer og anvisninger. Dokumentationen vedrørende kvalitetsstyringssystemet skal sikre, at kvalitetsprogrammer, -planer, -manualer og -registreringer fortolkes ens.

Den skal navnlig indeholde en fyldestgørende beskrivelse af:

a) kvalitetsmålsætningerne og organisationsstrukturerne samt ledelsens ansvar og beføjelser med hensyn til design, udvikling, fremstilling, produktkvalitet og håndtering af sårbarheder

b) de tekniske design- og udviklingsspecifikationer, herunder standarder, som vil blive anvendt, og, hvor de relevante harmoniserede standarder eller tekniske specifikationer ikke vil blive anvendt fuldt ud, de metoder, der vil blive anvendt til at sikre, at de væsentlige cybersikkerhedskrav i bilag I, del I, der gælder for produkterne med digitale elementer, vil blive opfyldt

c) de proceduremæssige specifikationer, herunder standarder, som vil blive anvendt, og, hvor de relevante harmoniserede standarder eller tekniske specifikationer ikke vil blive anvendt fuldt ud, de metoder, der vil blive anvendt til at sikre, at de væsentlige cybersikkerhedskrav i bilag I, del II, der gælder for fabrikanten, vil blive opfyldt

d) de teknikker og processer og systematiske foranstaltninger til design- og udviklingskontrol og -verifikation, der vil blive anvendt ved design og udvikling af produkter med digitale elementer, der henhører under den pågældende produktkategori

e) de teknikker, fremgangsmåder og systematiske foranstaltninger, der vil blive anvendt ved produktion, kvalitetskontrol og kvalitetssikring

f) de undersøgelser og afprøvninger, der skal udføres før, under og efter produktionen, og den hyppighed, hvormed dette sker

g) kvalitetsregistreringerne såsom inspektionsrapporter og afprøvningsdata, kalibreringsdata og rapporter vedrørende det berørte personales kvalifikationer

h) metoderne til kontrol af, at den krævede design- og produktkvalitet er opnået, og at kvalitetsstyringssystemet fungerer effektivt.

3.3. Det bemyndigede organ vurderer kvalitetsstyringssystemet for at fastslå, om det opfylder de i punkt 3.2 omhandlede krav.

De elementer i kvalitetsstyringssystemet, som overholder de relevante specifikationer i den nationale standard, der gennemfører den relevante harmoniserede standard eller tekniske specifikation, skal af det bemyndigede organ anses for at opfylde kravene.

Ud over erfaring med kvalitetsstyringssystemer skal kontrolholdet have mindst ét medlem med erfaring i vurdering på det relevante produktområde og inden for den pågældende produktteknologi og have viden om de gældende krav i denne forordning. Kontrollen skal indbefatte et besøg på fabrikantens eventuelle anlæg. Kontrolholdet skal gennemgå den tekniske dokumentation, der er omhandlet i punkt 3.1, litra b), med henblik på at kontrollere fabrikantens evne til at fastslå de relevante krav i denne forordning og foretage de nødvendige undersøgelser for at sikre, at produktet med digitale elementer overholder disse krav.

Afgørelsen meddeles fabrikanten eller dennes bemyndigede repræsentant.

Meddelelsen skal indeholde resultaterne af kontrollen og begrundelsen for afgørelsen.

3.4. Fabrikanten forpligter sig til at opfylde de forpligtelser, der stammer fra kvalitetsstyringssystemet, således som det er godkendt, og til at vedligeholde det, således at det forbliver hensigtsmæssigt og effektivt.

3.5. Fabrikanten underretter det bemyndigede organ, som har godkendt kvalitetsstyringssystemet, om enhver påtænkt ændring af systemet.

Det bemyndigede organ evaluerer de foreslåede ændringer og afgør, om det ændrede kvalitetsstyringssystem stadig opfylder de i punkt 3.2 omhandlede krav, eller om en fornyet vurdering er nødvendig.

Det bemyndigede organ meddeler fabrikanten sin afgørelse. Meddelelsen skal indeholde resultaterne af undersøgelsen og en begrundelse for afgørelsen.

4. Overvågning under det bemyndigede organs ansvar

4.1. Formålet med overvågningen er at sikre, at fabrikanten behørigt opfylder de forpligtelser der stammer fra det godkendte kvalitetssystem.

4.2. Fabrikanten skal med henblik på kontrol give det bemyndigede organ adgang til design-, udviklings-, produktions-, inspektions-, afprøvnings- og lagerfaciliteterne og give det alle nødvendige oplysninger, navnlig:

a) dokumentation om kvalitetsstyringssystemet

b) kvalitetsregistreringer som fastsat i konstruktionsdelen af kvalitetsstyringssystemet, herunder resultater af analyser, beregninger og afprøvninger

c) kvalitetsregistreringer som fastsat i produktionsdelen af kvalitetsstyringssystemet såsom inspektionsrapporter og afprøvningsdata, kalibreringsdata og rapporter om personalets kvalifikationer.

4.3. Det bemyndigede organ aflægger jævnligt kontrolbesøg for at sikre, at fabrikanten opretholder og anvender kvalitetsstyringssystemet, og det udsteder en kontrolrapport til fabrikanten.

5. Overensstemmelsesmærkning og overensstemmelseserklæring

5.1. Fabrikanten anbringer CE-mærkningen, og på det i punkt 3.1 omhandlede bemyndigede organs ansvar dette organs identifikationsnummer på hvert produkt med digitale elementer, som opfylder kravene i bilag I, del I.

5.2. Fabrikanten udarbejder en skriftlig overensstemmelseserklæring for hver produktmodel og opbevarer den, så den står til rådighed for de nationale myndigheder i ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst. Det skal af overensstemmelseserklæringen fremgå, hvilken produktmodel den vedrører.

Et eksemplar af overensstemmelseserklæringen stilles efter anmodning til rådighed for de relevante myndigheder.

6. Fabrikanten skal, i mindst ti år efter at produktet med digitale elementer er blevet bragt i omsætning, eller i supportperioden, alt efter hvilket tidsrum der er længst, kunne forelægge de nationale myndigheder:

a) den i punkt 3.1 omhandlede tekniske dokumentation

b) den i punkt 3.1 omhandlede dokumentation vedrørende kvalitetsstyringssystemet

c) de i punkt 3.5 omhandlede ændringer som godkendt

d) de i punkt 3.5 og 4.3 omhandlede afgørelser og rapporter fra det bemyndigede organ.

7. Hvert bemyndiget organ skal underrette sine bemyndigende myndigheder om udstedte eller tilbagekaldte godkendelser af kvalitetsstyringssystemer og med jævne mellemrum eller efter anmodning stille en fortegnelse over afviste, suspenderede eller på anden måde begrænsede godkendelser af kvalitetsstyringssystemer til rådighed for sine bemyndigende myndigheder.

Hvert bemyndiget organ skal underrette de øvrige bemyndigede organer om afviste, suspenderede eller tilbagekaldte godkendelser af kvalitetsstyringssystemer og, efter anmodning, om udstedte godkendelser af kvalitetsstyringssystemer.

8. Bemyndiget repræsentant

Fabrikantens forpligtelser i henhold til punkt 3.1, 3.5, 5 og 6 kan opfyldes af den bemyndigede repræsentant på fabrikantens vegne og ansvar, forudsat at de relevante forpligtelser er angivet i fuldmagten.

Der er fremsat en erklæring/erklæringer vedrørende denne retsakt, og den kan findes i EUT C, C/2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj.