EUROPA-
KOMMISSIONEN

Bruxelles, den 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020

(EØS-relevant tekst)

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

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

Hardware- og softwareprodukter udsættes i stigende grad for vellykkede cyberangreb, og de samlede årlige omkostninger ved cyberkriminalitet beløb sig således til 5,5 mia. EUR i 2021. To store problemer knytter sig til disse produkter, som øger omkostningerne for brugerne og samfundet: 1) et lavt cybersikkerhedsniveau, der afspejles i udbredte sårbarheder og utilstrækkelig og inkonsekvent levering af sikkerhedsopdateringer til håndtering heraf, og 2) brugernes utilstrækkelige forståelse af og adgang til oplysninger, hvilket forhindrer dem i at vælge produkter med passende cybersikkerhedsegenskaber eller at anvende dem på en sikker måde. I et forbundet miljø kan en cybersikkerhedshændelse i ét produkt påvirke en hel organisation eller en hel forsyningskæde og spreder sig ofte over hele det indre markeds grænser inden for få minutter. Dette kan føre til alvorlige forstyrrelser af økonomiske og sociale aktiviteter eller endda blive livstruende.

Cybersikkerheden for produkter med digitale elementer har en stærk grænseoverskridende dimension, da produkter fremstillet i ét land ofte anvendes i hele det indre marked. Hændelser, der i første omgang berører en enkelt enhed eller en enkelt medlemsstat, spreder sig desuden ofte inden for få minutter i hele det indre marked.

Selv om den eksisterende lovgivning om det indre marked finder anvendelse på visse produkter med digitale elementer, er de fleste hardware- og softwareprodukter i øjeblikket ikke omfattet af EU-lovgivning om cybersikkerhed. EU's nuværende retlige ramme indeholder navnlig ikke bestemmelser om cybersikkerheden for ikkeindlejrede softwareprodukter, selv om cyberangreb i stigende grad er rettet mod sårbarheder i disse produkter, hvilket medfører betydelige samfundsmæssige og økonomiske omkostninger. Der er talrige eksempler på bemærkelsesværdige cyberangreb, der skyldes suboptimal produktsikkerhed, f.eks. ransomware-ormen WannaCry, som udnyttede en Windows-sårbarhed og ramte 200 000 computere i 150 lande i 2017 og forårsagede skader til flere milliarder amerikanske dollars, angrebet på Kaseya VSA-forsyningskæden, hvor Kaseyas netværksadministrationssoftware blev anvendt til at angribe over 1 000 virksomheder og tvang en supermarkedskæde til at lukke alle sine 500 butikker i hele Sverige, eller de mange hændelser, hvor bankapplikationer hackes for at stjæle penge fra intetanende forbrugere.

Der blev udpeget to hovedmål, som skal sikre et velfungerende indre marked: 1) skabe betingelser 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, og 2) skabe betingelser, der gør det muligt for brugerne at tage hensyn til cybersikkerhed, når de udvælger og anvender produkter med digitale elementer. Der blev fastsat fire specifikke mål: i) sikre, at fabrikanterne forbedrer sikkerheden af produkter med digitale elementer lige fra design- og udviklingsfasen og i hele livscyklussen, ii) sikre en sammenhængende ramme for cybersikkerhed, der letter hardware- og softwareproducenternes overholdelse af kravene, iii) øge gennemsigtigheden med hensyn til sikkerhedsegenskaber ved produkter med digitale elementer og iv) gøre det muligt for virksomheder og forbrugere at anvende produkter med digitale elementer på en sikker måde.

Den stærke grænseoverskridende karakter af cybersikkerhed og det stigende antal hændelser med afsmittende virkninger på tværs af grænser, sektorer og produkter betyder, at målene ikke kan opfyldes effektivt af medlemsstaterne alene. I betragtning af den globale karakter af

markederne for produkter med digitale elementer står medlemsstaterne over for de samme risici i forbindelse med det samme produkt med digitale elementer på deres område. Et kludetæppe af potentielt divergerende nationale regler risikerer at forhindre et åbent og konkurrencedygtigt indre marked for produkter med digitale elementer. En fælles indsats på EU-plan er derfor nødvendig for at øge tilliden blandt brugerne og gøre EU-produkter med digitale elementer mere attraktive. Det vil også gavne det indre marked ved at sikre retssikkerhed og lige vilkår for leverandører af produkter med digitale elementer, hvilket også blev fremhævet i den endelige rapport fra konferencen om Europas fremtid, hvor borgerne opfordrer EU til at spille en stærkere rolle i bekæmpelsen af cybersikkerhedstrusler.

- **Sammenhæng med de gældende regler på samme område**

EU-rammen omfatter flere horisontale retsakter, der dækker visse aspekter af cybersikkerhed fra forskellige vinkler (produkter, tjenester, krisestyring og kriminalitet). I 2013 trådte direktivet om angreb på informationssystemer[1], der harmoniserer kriminalisering og sanktioner for en række strafbare handlinger rettet mod informationssystemer, i kraft. I august 2016 trådte direktiv (EU) 2016/1148 om sikkerhed i net- og informationssystemer (NIS-direktivet)[2] i kraft som den første EU-retsakt om cybersikkerhed. I revisionen heraf, der er mundet ud i direktiv [direktiv XXX/XXXX (NIS2)], hæves EU's fælles ambitionsniveau. I 2019 trådte EU's forordning om cybersikkerhed[3] i kraft, og den havde til formål at øge sikkerheden i forbindelse med IKT-produkter, -tjenester og -processer gennem indførelse af en frivillig europæisk ramme for cybersikkerhedscertificering[4].

Cybersikkerhed i hele forsyningskæden kan kun sikres, hvis alle dele deraf er cybersikre. Ovennævnte EU-lovgivning har imidlertid betydelige mangler i denne henseende, da den ikke omfatter obligatoriske krav til sikkerheden af produkter med digitale elementer.

Selv om den foreslåede forordning om cyberrobusthed omfatter produkter med digitale elementer, der bringes i omsætning, har direktiv [direktiv XXX/XXXX (NIS2)] til formål at sikre et højt cybersikkerhedsniveau for tjenester, der udbydes af væsentlige og vigtige enheder. I henhold til direktiv [XXX/XXXX (NIS2)] skal medlemsstaterne sikre, at væsentlige og vigtige enheder inden for anvendelsesområdet såsom sundhedstjenesteydere eller cloududbydere og offentlige forvaltningsenheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske cybersikkerhedsforanstaltninger. Dette omfatter bl.a. et krav om at sikre sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder. I henhold til direktiv [XXX/XXXX (NIS2)] skal Kommissionen vedtage gennemførelsesretsakter, der fastlægger de tekniske og metodiske krav til disse foranstaltninger senest 21 måneder efter datoen for dette direktivs ikrafttræden for visse typer

[1] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

[2] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

[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] Forordningen om cybersikkerhed gør det muligt at udvikle særlige certificeringsordninger. Hver ordning indeholder henvisninger til relevante standarder, tekniske specifikationer eller andre cybersikkerhedskrav, der er defineret i ordningen. Beslutningen om at udvikle en cybersikkerhedscertificering er risikobaseret.

enheder såsom udbydere af cloud computing-tjenester. For alle andre enheder kan Kommissionen vedtage en gennemførelsesretsakt, der fastlægger de tekniske og metodiske krav samt sektorspecifikke krav. Denne ramme vil sikre, at der også gennemføres tekniske specifikationer og foranstaltninger, der opfylder de væsentlige cybersikkerhedskrav i forordningen om cyberrobusthed, med henblik på design og udvikling af og håndtering af sårbarheder i software, der leveres som en service (software-as-a-service). Dette kan f.eks. være et middel til at sikre et højt cybersikkerhedsniveau, f.eks. i forbindelse med elektroniske patientjournalsystemer (EPJ-systemer), herunder når softwaren leveres som software-as-a-service (SaaS) eller udvikles i sundhedsinstitutioner (internt) i overensstemmelse med forslaget til [forordning om det europæiske sundhedsdataområde].

- **Sammenhæng med Unionens politik på andre områder**

Som beskrevet i meddelelsen om Europas digitale fremtid i støbeskeen[5] er det afgørende, at EU høster alle fordelene ved den digitale tidsalder og styrker sin industri og innovationskapacitet inden for sikre og etiske grænser. I den europæiske strategi for data fastsættes der fire søjler — databeskyttelse, grundlæggende rettigheder, sikkerhed og cybersikkerhed — som væsentlige forudsætninger for et samfund, der styrkes ved brugen af data.

Den nuværende EU-ramme[6] for produkter, der også kan have digitale elementer, omfatter flere retsakter, herunder EU-lovgivning om specifikke produkter, der dækker sikkerhedsrelaterede aspekter, og generel lovgivning om produktansvar. Forslaget er i overensstemmelse med den nuværende produktrelaterede EU-lovramme samt med nylige lovgivningsforslag såsom Kommissionens forslag til forordning [forordningen om kunstig intelligens — AI-forordningen][7].

Den foreslåede forordning vil finde anvendelse på alt radioudstyr, der er omfattet af Kommissionens delegerede forordning (EU) 2022/30. Desuden omfatter kravene i denne forordning alle elementerne i de væsentlige krav, der er omhandlet i artikel 3, stk. 3, litra d), e) og f), i direktiv 2014/53/EU, herunder hovedelementerne i [Kommissionens gennemførelsesafgørelse XXX/2022 om en standardiseringsanmodning til de europæiske standardiseringsorganisationer] udstedt på grundlag af nævnte delegerede forordning. For at undgå overlapning af reglerne forventes det, at Kommissionen ophæver eller ændrer den delegerede forordning for så vidt angår radioudstyr, der er omfattet af den foreslåede forordning, således at sidstnævnte forordning finder anvendelse herpå, når den er trådt i kraft.

For at undgå dobbeltarbejde er det desuden hensigten, at Kommissionen og de europæiske standardiseringsorganisationer skal tage hensyn til det standardiseringsarbejde, der er udført i forbindelse med Kommissionens gennemførelsesafgørelse C (2022) 5637 om en standardiseringsanmodning i forbindelse med den delegerede forordning 2022/30 om radioudstyrsdirektivet, ved udarbejdelsen og udviklingen af harmoniserede standarder for at lette gennemførelsen af forordningen.

---

5 Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget — Europas digitale fremtid i støbeskeen (COM(2020) 67 final af 19.2.2020).

6 Primært den nye lovgivningsmæssige ramme.

7 Forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter af 21. april 2021 (COM(2021) 206 final).

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

- **Retsgrundlag**

Retsgrundlaget for dette forslag er artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), som indeholder bestemmelser om vedtagelse af foranstaltninger, der skal sikre det indre markeds oprettelse og funktion. Formålet med forslaget er at harmonisere cybersikkerhedskravene til produkter med digitale elementer i alle medlemsstater og fjerne hindringer for den frie bevægelighed for varer.

Artikel 114 i TEUF kan anvendes som retsgrundlag for at forhindre disse hindringer som følge af divergerende nationale love og tilgange til, hvordan retsusikkerheden og hullerne i de eksisterende retlige rammer kan afhjælpes[8]. Domstolen har desuden anerkendt, at anvendelse af heterogene tekniske krav kan være en gyldig grund til at udløse artikel 114 i TEUF[9].

EU's nuværende lovgivningsmæssige ramme for produkter med digitale elementer er baseret på artikel 114 i TEUF og omfatter flere retsakter, herunder om specifikke produkter og sikkerhedsrelaterede aspekter, eller generel lovgivning om produktansvar. Den dækker imidlertid kun visse aspekter i forbindelse med cybersikkerheden for håndgribelige digitale produkter og, hvor det er relevant, software indlejret i disse produkter. På nationalt plan er medlemsstaterne begyndt at træffe nationale foranstaltninger, der pålægger leverandører af digitale produkter at forbedre deres cybersikkerhed[10]. Cybersikkerheden for digitale produkter har samtidig en særlig stærk grænseoverskridende dimension, da produkter fremstillet i ét land ofte anvendes af organisationer og forbrugere i hele det indre marked. Hændelser, der i første omgang berører en enkelt enhed eller medlemsstat, spredes ofte inden for få minutter på tværs af organisationer, sektorer og flere medlemsstater.

De forskellige retsakter og initiativer, der er truffet indtil videre på EU-plan og nationalt plan, løser kun delvist de konstaterede problemer og risici og skaber et kludetæppe af lovgivning i det indre marked, øger retsusikkerheden for både leverandører og brugere af disse produkter og pålægger virksomhederne unødvendige byrder forbundet med opfyldelsen af en række krav til lignende produkttyper.

Den foreslåede forordning vil harmonisere og strømline EU's lovgivningsmæssige landskab ved at indføre cybersikkerhedskrav for produkter med digitale elementer og undgå overlappende krav i forskellige retsakter. Dette vil skabe større retssikkerhed for erhvervsdrivende og brugere i hele Unionen samt en bedre harmonisering af EU's indre marked, hvilket vil skabe mere levedygtige vilkår for operatører, der ønsker at komme ind på EU-markedet.

- **Nærhedsprincippet (for områder, der ikke er omfattet af enekompetence)**

Den stærke grænseoverskridende karakter af cybersikkerhed generelt og det stigende antal risici og hændelser med afsmittende virkninger på tværs af grænser, sektorer og produkter betyder, at målene for det nuværende tiltag ikke kan opfyldes effektivt af medlemsstaterne

---

8 Domstolens dom (Store Afdeling) af 3. december 2019, Den Tjekkiske Republik mod Europa-Parlamentet og Rådet for Den Europæiske Union, sag C-482/17, præmis 35.

9 Domstolens dom (Store Afdeling) af 2. maj 2006, Det Forenede Kongerige Storbritannien og Nordirland mod Europa-Parlamentet og Rådet for Den Europæiske Union, sag C-217/04, præmis 62-63.

10 Finland oprettede f.eks. i 2019 en mærkningsordning for IoT-enheder såsom intelligente fjernsyn, smartphones og legetøj baseret på ETSI-standarderne. Tyskland har for nylig indført et forbrugersikkerhedsmærke for bredbåndsroutere, intelligente fjernsyn, kameraer, højttalere, legetøj samt rengørings- og haverobotter.

alene. Nationale tilgange til løsning af problemerne, herunder navnlig indførelse af obligatoriske krav, vil skabe yderligere retsusikkerhed og juridiske hindringer. Der kan lægges hindringer i vejen for virksomhedernes ekspansion i andre medlemsstater, hvilket fratager brugerne fordelene ved deres produkter.

En fælles indsats på EU-plan er derfor nødvendig for at skabe en høj grad af tillid blandt brugerne og gøre EU-produkter med digitale elementer mere attraktive. Det vil også gavne det digitale indre marked og det indre marked generelt ved at sikre retssikkerhed og lige vilkår for fabrikanter af produkter med digitale elementer.

Endelig opfordrer Rådet i sine konklusioner af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition Kommissionen til at foreslå fælles cybersikkerhedskrav for forbundne enheder inden udgangen af 2022.

- **Proportionalitetsprincippet**

Med hensyn til proportionaliteten af den foreslåede forordning vil foranstaltningerne i de overvejede løsninger ikke gå ud over, hvad der er nødvendigt for at nå de generelle og specifikke mål, og de vil ikke medføre uforholdsmæssigt store omkostninger. Mere specifikt vil det påtænkte tiltag sikre, at produkter med digitale elementer sikres i hele deres livscyklus på en måde, der står i et rimeligt forhold til de pågældende risici, gennem målorienterede og teknologineutrale krav, der fortsat er rimelige og generelt svarer til de involverede enheders interesse.

De væsentlige cybersikkerhedskrav i forslaget bygger på almindeligt anvendte standarder, og der vil blive taget hensyn til produkternes tekniske specifikationer i den efterfølgende standardiseringsproces. Det betyder, at sikkerhedskontrollen vil blive tilpasset, hvor det er nødvendigt for et givet risikoniveau. Desuden vil de påtænkte horisontale regler kun omfatte tredjepartsvurdering af kritiske produkter. Dette vil kun omfatte en lille andel af markedet for produkter med digitale elementer. Virkningerne for SMV'er vil afhænge af deres tilstedeværelse på markedet for disse specifikke produktkategorier.

Med hensyn til proportionaliteten af omkostningerne til overensstemmelsesvurdering vil bemyndigede organer, der foretager tredjepartsvurderinger, tage hensyn til virksomhedens størrelse ved fastsættelsen af deres gebyrer. Der vil også blive fastsat en rimelig overgangsperiode på 24 måneder til at forberede gennemførelsen, hvilket giver de relevante markeder tid til at forberede sig, samtidig med at der udstikkes en klar kurs for FoU-investeringer. Virksomhedernes eventuelle overholdelsesomkostninger vil blive opvejet af fordelene ved et højere sikkerhedsniveau for produkter med digitale elementer og i sidste ende af en stigning i brugernes tillid til disse produkter.

- **Valg af retsakt**

Et reguleringstiltag ville indebære vedtagelse af en forordning og ikke et direktiv. Dette skyldes, at en forordning i forbindelse med denne særlige type produktlovgivning ville løse de konstaterede problemer mere effektivt og opfylde de formulerede mål, da der er tale om et indgreb, som fastsætter de betingelser på hvilke en meget bred kategori af produkter kan bringes i omsætning i det indre marked. I tilfælde af et direktiv kunne gennemførelsen af et sådant indgreb give for stort spillerum på nationalt plan, hvilket potentielt kunne føre til manglende ensartethed i visse væsentlige cybersikkerhedskrav, retsusikkerhed, yderligere fragmentering eller endda diskriminerende situationer på tværs af grænserne, så meget desto mere som de omfattede produkter kan have eller anvendes til flere formål, og fabrikanterne kan producere flere kategorier af sådanne produkter.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

- **Høringer af interesserede parter**

Kommissionen har hørt en lang række interesserede parter. Medlemsstaterne og interessenterne blev opfordret til at deltage i den åbne offentlige høring og i de undersøgelser og workshopper, der blev afholdt i forbindelse med en undersøgelse udført af et konsortium, der understøttede Kommissionens forberedende arbejde til konsekvensanalysen: Wavestone, Centre for European Policy Studies (CEPS) og ICF. De hørte interessenter omfattede nationale markedsovervågningsmyndigheder, EU-organer, der beskæftiger sig med cybersikkerhed, hardware- og softwarefabrikanter, importører og distributører af hardware og software, brancheorganisationer, forbrugerorganisationer og brugere af produkter med digitale elementer og borgere, forskere og den akademiske verden, bemyndigede organer og akkrediteringsorganer samt fagfolk inden for cybersikkerhedsindustrien.

Høringsaktiviteterne omfattede:

- En første undersøgelse udført af et konsortium bestående af ICF, Wavestone, Carsa og CEPS, som blev offentliggjort i december 2021[11]. Undersøgelsen afdækkede flere markedssvigt, og en række mulige reguleringstiltag blev vurderet.
- En åben offentlig høring rettet mod borgere, interessenter og cybersikkerhedseksperter. Der blev indsendt 176 svar. Disse bidrog til indsamlingen af forskellige holdninger og erfaringer fra alle interessentgrupper.
- De workshopper, der blev afholdt som led i undersøgelsen til støtte for Kommissionens forberedende arbejde med en retsakt om cyberrobusthed, samlede omkring 100 repræsentanter fra alle 27 medlemsstater, der repræsenterede forskellige interessenter.
- Der blev gennemført ekspertinterviews for at få en dybere forståelse af de aktuelle cybersikkerhedsudfordringer i forbindelse med produkter med digitale elementer og for at drøfte mulighederne for et reguleringstiltag.
- Der blev afholdt bilaterale drøftelser med nationale cybersikkerhedsmyndigheder, den private sektor og forbrugerorganisationer.
- Der blev taget målrettet kontakt til centrale SMV-interessenter.

- **Indhentning og brug af ekspertbistand**

Formålet med høringsaktiviteterne var at få input til de fem vigtigste evalueringskriterier baseret på EU's retningslinjer for bedre regulering (virkningsfuldhed, effektivitet, relevans, sammenhæng, EU-merværdi) samt de potentielle virkninger af mulige løsninger i fremtiden. Kontrahenten har ikke kun været i kontakt med de interessenter, der vil blive direkte berørt af den foreslåede forordning, men har også hørt en bred vifte af eksperter inden for cybersikkerhed.

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

- **Konsekvensanalyse**

Kommissionen har foretaget en konsekvensanalyse af dette forslag, som blev behandlet af Kommissionens Udvalg for Forskriftskontrol. Der blev afholdt et møde med Udvalget for Forskriftskontrol den 6. juli 2022, og der blev efterfølgende afgivet en positiv udtalelse. Konsekvensanalysen blev tilpasset for at tage højde for anbefalingerne og bemærkningerne fra Udvalget for Forskriftskontrol.

Kommissionen har undersøgt forskellige løsninger for at nå forslagets overordnede formål:

- En tilgang med blød lovgivning og frivillige foranstaltninger (løsning 1): Denne løsning omfatter ikke obligatoriske reguleringstiltag. Kommissionen vil i stedet udstede meddelelser, vejledning, henstillinger og eventuelt adfærdskodekser for at tilskynde til frivillige foranstaltninger. Nationale ordninger, frivillige eller obligatoriske, vil fortsat blive udviklet for at kompensere for manglen på horisontale EU-regler.
- Produktspecifikt ad hoc-reguleringstiltag i forbindelse med cybersikkerhed for håndgribelige produkter med digitale elementer og indlejret software (løsning 2): Denne løsning vil indebære et produktspecifikt ad hoc-reguleringstiltag, der vil være begrænset til at tilføje og/eller ændre cybersikkerhedskravene i den allerede eksisterende lovgivning eller indføre ny lovgivning, efterhånden som der opstår nye risici, herunder potentielt for ikkeindlejret software.

Løsning 3 og 4 indebærer et horisontalt reguleringstiltag, der varierer i omfang, og som i vid udstrækning følger den nye lovgivningsmæssige ramme. I denne ramme fastsættes væsentlige krav som en forudsætning for, at visse produkter kan bringes i omsætning i det indre marked. Den nye lovgivningsramme indeholder typisk også bestemmelser om overensstemmelsesvurdering, den proces, der udføres af fabrikanten for at påvise, om specifikke krav til et produkt er opfyldt.

- Blandet tilgang, herunder horisontale obligatoriske regler for cybersikkerhed for håndgribelige produkter med digitale elementer og indlejret software og en trinvis tilgang til ikkeindlejret software (løsning 3): Denne løsning vil indebære en forordning, der indfører horisontale cybersikkerhedskrav til alle håndgribelige produkter med digitale elementer og indlejret software som en forudsætning for, at produkterne kan bringes i omsætning, og vil omfatte to delløsninger med og uden obligatorisk tredjepartsvurdering (3i og 3ii). Ikkeindlejret software vil ikke blive reguleret.
- Et horisontalt reguleringstiltag med indførelse af cybersikkerhedskrav til en bred vifte af håndgribelige og ikkehåndgribelige produkter med digitale elementer, herunder ikkeindlejret software (løsning 4): Denne løsning ligner løsning 3, bortset fra anvendelsesområdet. Løsning 4 vil omfatte ikkeindlejret software (med to delløsninger, der kun omfatter kritisk software (4a) eller al software (4b)) inden for anvendelsesområdet for en potentiel forordning. For hver delløsning vil de samme delløsninger vedrørende overensstemmelsesvurdering som for løsning 3 blive overvejet.

Løsning 4 (med delløsninger, der omfatter al software og indebærer obligatorisk tredjepartsvurdering af kritiske produkter) fremstod som den foretrukne løsning baseret på en vurdering af effektiviteten i forhold til de specifikke mål og omkostningseffektiviteten. Denne løsningsmodel vil sikre, at der fastsættes specifikke horisontale cybersikkerhedskrav til alle produkter med digitale elementer, der bringes i omsætning eller gøres tilgængelige på det

indre marked, og vil være den eneste løsning, der dækker hele den digitale forsyningskæde. Ikkeindlejret software, der ofte er udsat for sårbarheder, vil også være omfattet af et sådant reguleringstiltag og dermed sikre en sammenhængende tilgang til alle produkter med digitale elementer med en klar ansvarsfordeling mellem forskellige erhvervsdrivende.

Denne løsning tilfører også merværdi ved at omfatte aspekter vedrørende pligt til at udvise rettidig omhu og livscyklus, når produkterne med digitale elementer er bragt i omsætning, bl.a. for at sikre tilvejebringelsen af relevante oplysninger om sikkerhedsstøtte og levering af sikkerhedsopdateringer. Denne løsning vil også mest effektivt supplere den seneste revision af NIS-rammen ved at sikre forudsætningerne for en styrket forsyningskædesikkerhed.

Den foretrukne løsning vil medføre betydelige fordele for de forskellige interessenter. For virksomhederne vil det forhindre divergerende sikkerhedsregler for produkter med digitale elementer og mindske omkostningerne til overholdelse af relateret lovgivning om cybersikkerhed. Det vil reducere antallet af cyberhændelser, omkostningerne til håndtering af hændelser og skade på omdømme. For hele EU anslås det, at initiativet kan føre til en omkostningsreduktion som følge af hændelser, der påvirker virksomheder, på ca. 180-290 mia. EUR om året. Det vil føre til en øget omsætning som følge af øget efterspørgsel efter produkter med digitale elementer. Det vil forbedre virksomhedernes globale omdømme og også føre til øget efterspørgsel uden for EU. For brugerne vil den foretrukne løsning øge gennemsigtigheden med hensyn til sikkerhedsegenskaberne og lette anvendelsen af produkter med digitale elementer. Forbrugere og borgere vil også få en bedre beskyttelse af deres grundlæggende rettigheder såsom privatlivets fred og databeskyttelse.

Da respondenterne i den offentlige høring blev bedt om at vurdere effektiviteten af de politiske tiltag, var de enige i, at løsning 4 ville være den mest effektive foranstaltning (4,08 på en skala fra 1 til 5). Dette omfatter forbrugerorganisationer (5,00), respondenter, der angav sig som brugere (4,22), bemyndigede organer (4,17), markedsovervågningsmyndigheder (5,00) og producenter af produkter med digitale elementer (3,85), herunder små og mellemstore producenter (4,05).

- **Målrettet regulering og forenkling**

Med dette forslag fastsættes krav, der vil gælde for software- og hardwarefabrikanter. Der er behov for at sikre retssikkerheden og undgå yderligere markedsfragmentering af produktrelaterede krav til cybersikkerhed på det indre marked, hvilket den brede støtte fra forskellige interessenter til et horisontalt tiltag viser. Forslaget vil minimere den regelbyrde, som en række retsakter om produktsikkerhed pålægger fabrikanterne. Tilpasningen til den nye lovgivningsmæssige ramme betyder, at tiltaget og håndhævelsen heraf vil fungere bedre. Forslaget strømliner beskyttelsesprocedurerne ved at inddrage fabrikanterne og medlemsstaterne inden Kommissionen underrettes. En stor del af de fabrikanter, der er omfattet af forslaget, er allerede fortrolige med den nye lovgivningsmæssige ramme, hvilket vil bidrage til forståelsen og gennemførelsen heraf. For forbrugere og virksomheder vil forslaget fremme tilliden til produkter med digitale elementer.

- **Grundlæggende rettigheder**

Alle løsninger forventes i et vist omfang at forbedre beskyttelsen af grundlæggende rettigheder og frihedsrettigheder såsom privatlivets fred, beskyttelse af personoplysninger, frihed til at oprette og drive egen virksomhed og beskyttelse af ejendom eller personlig værdighed og integritet. Den foretrukne løsning 4, der består af brede horisontale reguleringstiltag, vil navnlig være mest effektiv i denne henseende, da der er større sandsynlighed for, at den vil bidrage til at mindske antallet og alvoren af hændelser, herunder brud på persondatasikkerheden. Den vil også øge retssikkerheden og skabe lige vilkår for de

erhvervsdrivende, øge tilliden blandt brugerne og gøre EU-produkter med digitale elementer mere attraktive som helhed og dermed beskytte ejendomsretten og forbedre vilkårene for erhvervsdrivende.

De horisontale cybersikkerhedskrav vil bidrage til sikkerheden af personoplysninger ved at beskytte fortroligheden, integriteten og tilgængeligheden af oplysninger om produkter med digitale elementer. Overholdelse af disse krav vil gøre det lettere at overholde kravet om sikkerhed i forbindelse med behandling af personoplysninger i henhold til forordning (EU) 2016/679 (den generelle forordning om databeskyttelse)[12]. Forslaget vil øge gennemsigtigheden og informationen til brugerne, herunder brugere, der ikke har så mange cybersikkerhedsfærdigheder. Brugerne vil også blive bedre informeret om risici, kapaciteter og begrænsninger ved produkter med digitale elementer, hvilket vil give dem bedre forudsætninger for at træffe de nødvendige forebyggende og afbødende foranstaltninger for at reducere de resterende risici.

4. VIRKNINGER FOR BUDGETTET

For at kunne udføre opgaverne tildelt Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) i henhold til denne forordning, skal ENISA omfordele ressourcer på ca. 4.5 fuldtidsækvivalenter. Kommissionen skal tildele syv fuldtidsækvivalenter for at opfylde sine håndhævelsesforpligtelser i henhold til denne forordning.

En detaljeret oversigt over de omkostninger, der er forbundet hermed, findes i "finansieringsoversigten" til dette forslag.

5. ANDRE FORHOLD

- **Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering**

Kommissionen vil overvåge gennemførelsen, anvendelsen og overholdelsen af disse nye bestemmelser med henblik på at vurdere deres effektivitet. Forordningen vil indeholde krav om evaluering og revision fra Kommissionen og forelæggelse af en offentlig rapport herom for Europa-Parlamentet og Rådet senest 36 måneder efter datoen for forordningens anvendelse og hvert fjerde år derefter.

- **Nærmere redegørelse for de enkelte bestemmelser i forslaget**

Almindelige bestemmelser (kapitel I)

I denne foreslåede forordning fastsættes a) regler for omsætning af produkter med digitale elementer for at sikre cybersikkerheden for sådanne produkter, b) væsentlige krav 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 krav til de sårbarhedshåndteringsprocesser, som fabrikanterne skal indføre for at sikre cybersikkerheden for produkter med digitale elementer i hele deres livscyklus, og forpligtelser for erhvervsdrivende i forbindelse med disse processer, d) regler om markedsovervågning og håndhævelse af ovennævnte regler og krav.

[12] 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).

Den foreslåede forordning vil finde anvendelse på produkter med digitale elementer, hvis tilsigtede og med rimelighed forudsigelige anvendelse omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk.

Den foreslåede forordning finder ikke anvendelse på produkter med digitale elementer inden for anvendelsesområdet for forordning (EU) 2017/745 [medicinsk udstyr til human brug og tilbehør til sådant udstyr] og forordning (EU) 2017/746 [medicinsk udstyr til in vitro-diagnostik til human brug og tilbehør til sådant udstyr], da begge forordninger indeholder krav vedrørende udstyr, herunder om software og generelle forpligtelser for fabrikanter, der dækker hele produkternes livscyklus, samt overensstemmelsesvurderingsprocedurer. Denne forordning finder ikke anvendelse på produkter med digitale elementer, der er certificeret i overensstemmelse med forordning 2018/1139 [højt ensartet niveau for civil luftfartssikkerhed], eller på produkter, som forordning (EU) 2019/2144 finder anvendelse på [om krav til typegodkendelse af motorkøretøjer og påhængskøretøjer dertil samt systemer, komponenter og separate tekniske enheder til sådanne køretøjer].

Kritiske produkter med digitale elementer omfattes af specifikke overensstemmelsesvurderingsprocedurer og inddeles i klasse I og II som fastsat i bilag III, der afspejler deres cybersikkerhedsrisikoniveau, hvor klasse II udgør en større risiko. Et produkt med digitale elementer betragtes som kritisk og er derfor medtaget i bilag III under hensyntagen til virkningen af potentielle cybersikkerhedssårbarheder i produktet med digitale elementer. Den cybersikkerhedsrelaterede funktionalitet i produktet med digitale elementer og produktets tilsigtede anvendelse i følsomme miljøer såsom industrielle rammer tages i betragtning ved fastlæggelsen af cybersikkerhedsrisiciene.

Kommissionen tillægges også beføjelser til at vedtage delegerede retsakter med henblik på at supplere denne forordning ved at præcisere de kategorier af meget kritiske produkter med digitale elementer, for hvilke fabrikanterne skal indhente en europæisk cybersikkerhedsattest i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med de væsentlige krav i bilag I eller dele deraf. Ved fastlæggelsen af sådanne kategorier af højkritiske produkter med digitale elementer tager Kommissionen hensyn til cybersikkerhedsrisikoniveauet for kategorien af produkter med digitale elementer på grundlag af et eller flere af de kriterier, der overvejes for opførelse af kritiske produkter med digitale elementer i bilag III, samt vurderingen af, om denne produktkategori anvendes af de væsentlige enheder af den type, der er omhandlet i bilag [bilag I] til direktiv [direktiv XXX/XXXX (NIS2)], eller vil have potentiel fremtidig betydning for disse enheders aktiviteter, eller er relevant for modstandsdygtigheden i den samlede forsyningskæde for produkter med digitale elementer over for afbrydelser.

Erhvervsdrivendes forpligtelser (kapitel II)

Forslaget indeholder forpligtelser for fabrikanter, importører og distributører baseret på referencebestemmelserne i afgørelse 768/2008/EF. Ifølge de væsentlige cybersikkerhedskrav og -forpligtelser må alle produkter med digitale elementer kun gøres tilgængelige på markedet, hvis de er korrekt leveret, installeret og vedligeholdt og anvendes til det tilsigtede formål eller på betingelser, som med rimelighed kan forudses, og opfylder de væsentlige cybersikkerhedskrav, der er fastsat i denne forordning.

Ifølge de væsentlige krav og forpligtelser skal fabrikanterne til at tage højde for cybersikkerhed i forbindelse med design, udvikling og produktion af produkter med digitale elementer, udvise den fornødne omhu med hensyn til sikkerhedsaspekter i forbindelse med design og produktion af deres produkter, være åbne omkring cybersikkerhedsaspekter, som kunderne skal have kendskab til, sørge for sikkerhedsstøtte (opdateringer) på en forholdsmæssig måde og opfylde krav til håndtering af sårbarheder.

Der vil blive indført forpligtelser for erhvervsdrivende, lige fra fabrikanter til distributører og importører, i forbindelse med omsætning af produkter med digitale elementer, som er passende i forhold til deres rolle og ansvar i forsyningskæden.

Overensstemmelsen af produkter med digitale elementer (kapitel III)

Produktet med digitale elementer, som er i overensstemmelse med harmoniserede standarder eller dele heraf, hvis referencer er offentliggjort *i Den Europæiske Unions Tidende*, formodes at være i overensstemmelse med de væsentlige krav i denne foreslåede forordning. Hvis der ikke findes harmoniserede standarder, eller hvis de er utilstrækkelige, eller hvis der er unødige forsinkelser i standardiseringsproceduren, eller hvis Kommissionens anmodning ikke er blevet imødekommet af nogen af de europæiske standardiseringsorganisationer, kan Kommissionen vedtage fælles specifikationer ved hjælp af gennemførelsesretsakter.

Desuden formodes produkter med digitale elementer, der er blevet certificeret, eller for hvilke der er udstedt en EU-overensstemmelseserklæring eller attest i henhold til en europæisk cybersikkerhedscertificeringsordning i henhold til forordning (EU) 2019/881, og for hvilken Kommissionen har præciseret i en gennemførelsesretsakt, at den kan danne grundlag for formodning om overensstemmelse med denne forordning, at være i overensstemmelse med de væsentlige krav i denne forordning eller dele heraf, såfremt cybersikkerhedsattesten eller overensstemmelseserklæringen eller dele heraf dækker disse krav.

For at undgå unødige administrative byrder for fabrikanter bør Kommissionen endvidere, hvor det er relevant, præcisere, om en cybersikkerhedsattest, der er udstedt i henhold til en sådan europæisk cybersikkerhedscertificeringsordning, fritager fabrikanten fra forpligtelsen til at lade foretage en overensstemmelsesvurdering af tredjepart som omhandlet i denne forordning vedrørende tilsvarende krav .

Fabrikanten skal foretage en overensstemmelsesvurdering af produktet med digitale elementer og de sårbarhedshåndteringsprocesser, fabrikanter har indført, for at påvise overensstemmelse med de væsentlige krav i bilag I ved at følge en af de procedurer, der er fastsat i bilag VI. Fabrikanter af kritiske produkter i klasse I og II skal anvende de respektive moduler, der er nødvendige for at opfylde kravene. Fabrikanter af kritiske produkter i klasse II skal inddrage en tredjepart i deres overensstemmelsesvurdering.

Notifikation af overensstemmelsesvurderingsorganer (kapitel IV)

Velfungerende bemyndigede organer er af afgørende betydning for at sikre et højt cybersikkerhedsniveau og alle berørte parters tillid til systemet med den nye metode. I overensstemmelse afgørelse 768/2008/EF indeholder forslaget derfor en række krav til de nationale myndigheder med ansvar for overensstemmelsesvurderingsorganer (bemyndigede organer). Det endelige ansvar for udpegelsen og overvågningen af de bemyndigede organer overlades til medlemsstaterne. Medlemsstaterne udpeger en bemyndigende myndighed, som er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering og notifikation af overensstemmelsesvurderingsorganer og overvågning af bemyndigede organer.

Markedsovervågning og håndhævelse (kapitel V)

I overensstemmelse med forordning (EU) 2019/1020 udfører de nationale markedsovervågningsmyndigheder markedsovervågning i den pågældende medlemsstat. Medlemsstaterne kan vælge at udpege enhver eksisterende eller ny myndighed som markedsovervågningsmyndighed, herunder eksisterende nationale kompetente myndigheder som omhandlet i artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)], eller udpegede nationale cybersikkerhedscertificeringsmyndigheder som omhandlet i artikel 58 i forordning (EU) 2019/881. Erhvervsdrivende anmodes om at samarbejde fuldt ud med markedsovervågningsmyndighederne og andre kompetente myndigheder.

Delegerede beføjelser og udvalgsprocedure (kapitel VI)

For at sikre, at den lovgivningsmæssige ramme kan tilpasses om nødvendigt, delegeres Kommissionen beføjelse til at vedtage retsakter, jf. artikel 290 i TEUF, for så vidt angår opdatering af listen over kritiske produkter i klasse I og II og præcisering af definitionerne af disse produkter, præcisering af, om en begrænsning eller udelukkelse er nødvendig for produkter med digitale elementer, der er omfattet af andre EU-forskrifter, der fastlægger krav, som sikrer samme beskyttelsesniveau som denne forordning, tildeling af mandat til certificering af visse meget kritiske produkter med digitale elementer baseret på de kriterier, der er fastsat i denne forordning, præcisering af minimumsindholdet i EU-overensstemmelseserklæringen og supplering af de elementer, der skal indgå i den tekniske dokumentation.

Kommissionen tillægges desuden beføjelser til at vedtage gennemførelsesretsakter med henblik på at: præcisere formatet for eller elementerne i rapporteringsforpligtelserne og softwarekomponentlisten, præcisere de europæiske cybersikkerhedscertificeringsordninger, der kan anvendes til at påvise overensstemmelse med de væsentlige krav eller dele heraf som fastsat i denne forordning, vedtage fælles specifikationer, fastsætte tekniske specifikationer for anbringelse af CE-mærkningen; vedtage korrigerende eller restriktive foranstaltninger på EU-plan under ekstraordinære omstændigheder, der berettiger et hurtigt indgreb for at bevare et velfungerende indre marked.

Fortrolighed og sanktioner (kapitel VII)

Alle parter, der anvender denne forordning, skal overholde tavshedspligten for oplysninger og data, der indhentes under udførelsen af deres opgaver og arbejde.

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. På samme måde fastsættes der i denne forordning maksimumsniveauer for administrative bøder, som bør fastsættes i national lovgivning for manglende overholdelse af forpligtelserne i denne forordning.

Overgangsbestemmelser og afsluttende bestemmelser (kapitel VIII)

For at give fabrikanter, bemyndigede organer og medlemsstaterne tid til at tilpasse sig de nye krav vil den foreslåede forordning finde anvendelse [24 måneder] efter dens ikrafttræden, bortset fra fabrikanternes indberetningspligt, som finder anvendelse fra [12 måneder] efter ikrafttrædelsesdatoen.

2022/0272 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

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

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],

under henvisning til udtalelse fra Regionsudvalget[2],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) Det er nødvendigt at 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 passende cybersikkerhedsegenskaber eller at anvende dem på en sikker måde.

(2) Denne forordning har til formål at fastsætte grænsebetingelserne 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.

(3) Den relevante gældende EU-lovgivning omfatter flere sæt horisontale regler, der omhandler visse cybersikkerhedsaspekter fra forskellige vinkler, herunder foranstaltninger til forbedring af sikkerheden i den digitale forsyningskæde. Den eksisterende EU-lovgivning vedrørende cybersikkerhed, herunder [direktiv

[1] EUT C […] af […], s. […].
[2] EUT C […] af […], s. […].

XXX/XXXX (NIS2)] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[3], omfatter imidlertid ikke direkte obligatoriske krav til sikkerheden af produkter med digitale elementer.

(4) Selv om den eksisterende EU-lovgivning 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 er truffet indtil videre på EU-plan og nationalt plan, løser kun delvist de identificerede cybersikkerhedsrelaterede problemer og risici og skaber et kludetæppe af lovgivning i det indre marked, øger retsusikkerheden for både fabrikanter og brugere af disse produkter og pålægger virksomhederne unødvendige byrder forbundet med opfyldelsen af en række krav til lignende produkttyper. Cybersikkerheden for disse produkter har en særlig stærk grænseoverskridende dimension, da produkter fremstillet i ét land ofte anvendes af organisationer og forbrugere i hele det indre marked. Dette gør det nødvendigt at regulere området på EU-plan. Unionens lovgivningsmæssige landskab bør harmoniseres ved at indføre cybersikkerhedskrav til produkter med digitale elementer. Der bør desuden sikres større retssikkerhed for erhvervsdrivende og brugere i hele Unionen samt en bedre harmonisering af det europæiske indre marked, hvilket vil skabe mere levedygtige vilkår for operatører, der ønsker at komme ind på EU-markedet.

(5) På EU-plan er der i forskellige program- og politikdokumenter såsom EU's strategi for cybersikkerhed for det digitale årti[4], Rådets konklusioner af 2. december 2020 og 23. maj 2022 eller Europa-Parlamentets beslutning af 10. juni 2021[5] blevet opfordret til, at der indføres specifikke EU-cybersikkerhedskrav til digitale eller forbundne produkter, og en række lande rundt om i verden har indført foranstaltninger til at løse dette problem på eget initiativ. I den endelige rapport fra konferencen om Europas fremtid[6] opfordrede borgerne EU til "at spille en stærkere rolle i bekæmpelsen af cybersikkerhedstrusler".

(6) 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.

(7) 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 betragtes 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

---

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

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

6 *Conference on the Future of Europe – Report on the Final Outcome*, maj 2022, forslag 28(2). Konferencen blev afholdt mellem april 2021 og maj 2022. Det var en enestående, borgerstyret øvelse i samtaledemokrati på paneuropæisk plan med deltagelse af tusindvis af europæiske borgere samt politiske aktører, arbejdsmarkedets parter, repræsentanter for civilsamfundet og centrale interesserede parter.

i overensstemmelse med de væsentlige krav, der er fastsat i denne forordning. Dette omfatter både produkter, der kan forbindes fysisk via hardwaregrænseflader, og produkter, der er logisk forbundne, f.eks. via netstikdåser, rør, filer, applikationsprogrammeringsgrænseflader eller andre typer softwaregrænseflader. Da cybersikkerhedstrusler 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.

(8) Ved at fastsætte cybersikkerhedskrav til produkter med digitale elementer, der bringes i omsætning, vil disse produkters cybersikkerhed blive forbedret for både forbrugere og virksomheder. Dette omfatter også krav til produkter med digitale elementer beregnet til sårbare forbrugere, f.eks. legetøj og babyalarmer, der bringes i omsætning.

(9) Denne forordning sikrer et højt cybersikkerhedsniveau for produkter med digitale elementer. Den regulerer ikke tjenester såsom software-as-a-service (SaaS), bortset fra fjerndatabehandlingsløsninger vedrørende et produkt med digitale elementer forstået som enhver databehandling på afstand, som softwaren er designet og udviklet til af fabrikanten af det pågældende produkt eller under den pågældende fabrikants ansvar, hvis fravær ville forhindre et sådant produkt med digitale elementer i at udføre en af sine funktioner. I [direktiv XXX/XXXX (NIS2)] indføres krav om cybersikkerhed og underretning om hændelser til væsentlige og vigtige enheder såsom kritisk infrastruktur for at øge modstandsdygtigheden af de tjenester, de leverer. [Direktiv XXX/XXXX (NIS2)] finder anvendelse på cloud computing-tjenester og modeller for cloud-tjenester såsom SaaS. Alle enheder, der udbyder cloud computing-tjenester i Unionen, og som opfylder eller overskrider tærsklen for mellemstore virksomheder, er omfattet af nævnte direktivs anvendelsesområde.

(10) For ikke at hæmme innovation eller forskning bør gratis og open source-software, der ikke udvikles eller leveres som led i erhvervsvirksomhed, ikke være omfattet af denne forordning. Dette er navnlig tilfældet for software, herunder kildekode og ændrede versioner, der deles åbent og er frit tilgængelige, anvendelige, redigerbare og redistribuerbare. I forbindelse med software kan erhvervsvirksomhed ikke blot være kendetegnet ved opkrævning af en pris for et produkt, men også ved opkrævning af en pris for tekniske supporttjenester, ved tilrådighedsstillelse af en softwareplatform, hvorigennem fabrikanten tjener penge på andre tjenester, eller ved anvendelse af personoplysninger til andre formål end blot at forbedre softwarens sikkerhed, kompatibilitet eller interoperabilitet.

(11) Et sikkert internet er uundværligt for kritiske infrastrukturers funktion og for samfundet som helhed. [Direktiv XXX/XXXX (NIS2)] har til formål at sikre et højt cybersikkerhedsniveau for tjenester, der leveres af væsentlige og vigtige enheder, herunder udbydere af digital infrastruktur, der understøtter centrale funktioner i det åbne internet og sikrer internetadgang og 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 XXX/XXXX (NIS2)] 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.

(12) Europa-Parlamentets og Rådets forordning (EU) 2017/745[7] fastsætter regler om medicinsk udstyr, og Europa-Parlamentets og Rådets forordning (EU) 2017/746[8] fastsætter regler om medicinsk udstyr til in vitro-diagnostik. Begge 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 er software i sig selv. Visse former for ikkeindlejret software og livscyklustilgangen behandles også i disse forordninger. Disse krav giver fabrikanterne mandat til at udvikle og bygge deres produkter ud fra risikostyringsprincipper og ved at fastsætte krav vedrørende IT-sikkerhedsforanstaltninger og anvende tilsvarende overensstemmelsesvurderingsprocedurer. Desuden 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 disse forordninger for så vidt angår cybersikkerhed[9]. Produkter med digitale elementer, som en af disse forordninger finder anvendelse på, bør derfor ikke være omfattet af denne forordning.

(13) Ved Europa-Parlamentets og Rådets forordning (EU) 2019/2144[10] fastsættes krav til typegodkendelse af køretøjer og deres systemer og komponenter, herunder en række cybersikkerhedskrav, bl.a. vedrørende drift af et certificeret cybersikkerhedsstyringssystem, softwareopdateringer, der dækker organisationers politikker og processer for styring af cyberrisici i hele livscyklussen for køretøjer, udstyr og tjenester i overensstemmelse med de gældende FN-regulativer om tekniske specifikationer og cybersikkerhed[11], og der indføres specifikke overensstemmelsesvurderingsprocedurer. På luftfartsområdet er hovedformålet med Europa-Parlamentets og Rådets forordning (EU) 2018/1139[12] at fastlægge og opretholde et højt og ensartet sikkerhedsniveau for den civile luftfart i Unionen. Den

---

7 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).

8 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).

9 MDCG 2019-16, godkendt af Koordinationsgruppen for Medicinsk Udstyr (MDCG), der er nedsat ved artikel 103 i forordning (EU) 2017/745.

10 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).

11 FN-regulativ nr. 155 — Ensartede forskrifter for godkendelse af køretøjer for så vidt angår cybersikkerhed og systemer til forvaltning af cybersikkerhed [2021/387].

12 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 forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og Europa-Parlamentets og Rådets 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).

skaber en ramme for væsentlige krav til luftdygtighed for luftfartøjsmateriel, dele og udstyr, herunder software, hvor deres tages hensyn til forpligtelser til at beskytte mod trusler mod informationssikkerheden. Produkter med digitale elementer, som forordning (EU) 2019/2144 finder anvendelse på, og produkter, der er certificeret i overensstemmelse med forordning (EU) 2018/1139, er derfor ikke omfattet af de væsentlige krav og overensstemmelsesvurderingsprocedurerne i nærværende forordning. Certificeringsprocessen i henhold til forordning (EU) 2018/1139 sikrer det samme beskyttelsesniveau som det, der er fastsat i denne forordning.

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

(15) I delegeret forordning (EU) 2022/30 præciseres det, at de væsentlige krav i artikel 3, stk. 3, litra d) (skade på net og misbrug af netressourcer), litra e) (personoplysninger og privatliv) og litra f) (svig) i direktiv 2014/53/EU finder anvendelse på visse typer radioudstyr. I [Kommissionens gennemførelsesafgørelse XXX/2022 om en standardiseringsanmodning til de europæiske standardiseringsorganisationer] fastsættes krav til udviklingen af specifikke standarder med nærmere angivelse af, hvordan disse tre væsentlige krav bør håndteres. De væsentlige krav fastsat i denne 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. De væsentlige krav i denne forordning er desuden i overensstemmelse med målene for kravene til specifikke standarder, der er omfattet af denne standardiseringsanmodning. Hvis 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 tage hensyn til det standardiseringsarbejde, der er udført i forbindelse med Kommissionens gennemførelsesafgørelse C (2022) 5637 om en standardiseringsanmodning i forbindelse med den delegerede forordning 2022/30 om radioudstyrsdirektivet, ved udarbejdelsen og udviklingen af harmoniserede standarder for at lette gennemførelsen af forordningen.

(16) Direktiv 85/374/EØF[13] 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

[13] Rådets direktiv 85/374/EØF af 25. juli 1985 om tilnærmelse af medlemsstaternes administrativt eller ved lov fastsatte bestemmelser om produktansvar (EFT (OJ L 210, 7.8.1985)).

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.

(17) Denne forordning bør ikke berøre Europa-Parlamentets og Rådets forordning (EU) 2016/679[14], herunder bestemmelser om 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 denne 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 (EDPB) oprettet ved forordning (EU) 2016/679 og de nationale databeskyttelsestilsynsmyndigheder. Der bør også skabes synergier mellem denne forordning og EU's databeskyttelseslovgivning inden for markedsovervågning og håndhævelse. Med henblik herpå bør nationale markedsovervågningsmyndigheder udpeget i henhold til denne forordning samarbejde med myndigheder, der fører tilsyn med EU's databeskyttelseslovgivning. Sidstnævnte myndigheder bør også have adgang til oplysninger, der er relevante for udførelsen af deres opgaver.

(18) I det omfang deres produkter er omfattet af denne forordnings anvendelsesområde, bør udstedere af europæiske digitale ID-tegnebøger som omhandlet i artikel [artikel 6a, stk. 2, i forordning (EU) nr. 910/2014 som ændret ved forslag til forordning om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af en ramme for en europæisk digital identitet] opfylde både de horisontale væsentlige krav fastsat i denne forordning og de specifikke sikkerhedskrav fastsat i artikel [artikel 6a i forordning (EU) nr. 910/2014 som ændret ved forslag til forordning om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af en ramme for en europæisk digital identitet]. For at lette overholdelsen bør udstedere af tegnebøger kunne påvise, at europæiske digitale ID-tegnebøger opfylder de krav, der er fastsat i begge retsakter, 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 præciseret i en gennemførelsesretsakt, at den kan danne grundlag for formodning om overensstemmelse med denne forordning, såfremt attesten eller dele heraf dækker disse krav.

(19) Visse af de opgaver, der er fastsat i denne forordning, bør udføres af ENISA i overensstemmelse med artikel 3, stk. 2, i forordning (EU) 2019/881. ENISA bør navnlig modtage underretninger fra fabrikanter om aktivt udnyttede sårbarheder i

[14] 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 (den generelle forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

produkter med digitale elementer samt om hændelser, der indvirker på disse produkters sikkerhed. ENISA bør også videresende disse underretninger til de relevante enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), eller til de relevante centrale kontaktpunkter i medlemsstaterne, der er udpeget i overensstemmelse med artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)], og underrette de relevante markedsovervågningsmyndigheder om den anmeldte sårbarhed. På grundlag af de oplysninger, som agenturet indsamler, bør ENISA 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 omhandlet i direktiv [direktiv XXX/XXXX (NIS2)]. Endvidere bør ENISA i betragtning af sin ekspertise og sit mandat være i stand til at støtte processen for gennemførelse af denne forordning. Agenturet 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 samtidige, koordinerede kontrolaktioner. Under ekstraordinære omstændigheder bør ENISA efter anmodning fra Kommissionen kunne foretage evalueringer af specifikke produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, hvis der er behov for et hurtigt indgreb for at bevare et velfungerende indre marked.

(20) Produkter med digitale elementer bør være forsynet med CE-mærkning for 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.

(21) For at sikre, at fabrikanterne kan frigive software til testformål, inden deres produkter underkastes en overensstemmelsesvurdering, bør medlemsstaterne ikke forhindre, at ufærdig software såsom alfaversioner, betaversioner eller versioner, som er klar til frigivelse ("release candidates"), stilles til rådighed, så længe versionen kun stilles til rådighed i det tidsrum, der er nødvendigt for at teste den og indsamle feedback. Fabrikanterne bør sikre, at software, der stilles til rådighed under disse betingelser, kun 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 prøvningsformål.

(22) For at sikre, at produkter med digitale elementer, der bringes i omsætning, ikke indebærer cybersikkerhedsrisici for personer og organisationer, bør der fastsættes væsentlige krav til sådanne produkter. Hvis produkterne efterfølgende ændres fysisk eller digitalt på en måde, som fabrikanten ikke har forudset, og som kan indebære, at de ikke længere opfylder de relevante væsentlige krav, bør ændringen betragtes som væsentlig. Softwareopdateringer eller reparationer kan f.eks. sammenlignes med vedligeholdelse, såfremt de ikke ændrer et produkt, der allerede er bragt i omsætning, på en sådan måde, at det påvirker overholdelsen af de gældende krav, eller såfremt produktets tilsigtede anvendelse kan ændres. Som det er tilfældet med fysiske reparationer eller ændringer, bør et produkt med digitale elementer anses for at være væsentligt ændret ved en softwareændring, hvis softwareopdateringen ændrer produktets oprindelige funktioner, type eller ydeevne, og disse ændringer ikke var

forudset i den indledende risikovurdering, eller farens art har ændret sig, eller risikoniveauet er forøget som følge af softwareopdateringen.

(23) I overensstemmelse med det almindeligt anerkendte begreb væsentlig ændring for produkter, der er reguleret ved EU-harmoniseringslovgivning, bør det verificeres, om et produkt med digitale elementer overholder kravene, og i givet fald bør produktet underkastes en ny overensstemmelsesvurdering, når 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 ændringer, der kan føre til væsentlige ændringer.

(24) Istandsættelse, vedligeholdelse og reparation af et produkt med digitale elementer som defineret i forordningen [forordningen om miljøvenligt design] fører ikke nødvendigvis til en væsentlig ændring af produktet, f.eks. hvis den tilsigtede anvendelse og funktionalitet ikke ændres, og risikoniveauet ikke påvirkes. Fabrikantens opgradering af et produkt kan imidlertid føre til ændringer i produktets design og udvikling og kan derfor påvirke produktets tilsigtede anvendelse og opfyldelse af kravene i denne forordning.

(25) Produkter med digitale elementer bør betragtes som kritiske, hvis den negative indvirkning af udnyttelsen af potentielle cybersikkerhedssårbarheder i produktet kan være alvorlig, bl.a. på grund af den cybersikkerhedsrelaterede funktionalitet eller den tilsigtede anvendelse. Sårbarheder i produkter med digitale elementer, der har en cybersikkerhedsrelateret funktionalitet, f.eks. sikre elementer, kan navnlig skabe en lang række sikkerhedsproblemer i hele forsyningskæden. Indvirkningen af en cybersikkerhedshændelse kan også blive mere alvorlig, når der tages højde for den tilsigtede anvendelse af produktet, f.eks. i et industrielt miljø eller i forbindelse med en væsentlig enhed af den type, der er omhandlet i bilag [bilag I] til direktiv [direktiv XXX/XXXX (NIS2)], eller i forbindelse med udførelsen af kritiske eller følsomme funktioner såsom behandling af personoplysninger.

(26) Kritiske produkter med digitale elementer bør være underlagt strengere overensstemmelsesvurderingsprocedurer, samtidig med at der sikres en forholdsmæssig tilgang. Med henblik herpå bør kritiske produkter med digitale elementer inddeles i to klasser, der afspejler cybersikkerhedsrisikoniveauet for disse produktkategorier. En potentiel cyberhændelse, der involverer produkter i klasse II, kan have større negative virkninger end en hændelse, der involverer produkter i klasse I, f.eks. på grund af karakteren af deres cybersikkerhedsrelaterede funktion eller tilsigtede anvendelse i følsomme miljøer, og bør derfor underkastes en strengere overensstemmelsesvurderingsprocedure.

(27) De kategorier af kritiske produkter med digitale elementer, der er omhandlet i bilag III til denne forordning, bør forstås som de produkter, hvis væsentligste funktion er af den type, der er opført i bilag III til denne forordning. F.eks. indeholder bilag III til denne forordning en liste over produkter, der defineres ud fra deres væsentligste funktion som mikroprocessorer til generelle formål i klasse II. Som følge heraf er mikroprocessorer til generelle formål underkastet obligatorisk overensstemmelsesvurdering udført af tredjepart. Dette er ikke tilfældet for andre produkter, der ikke udtrykkeligt er nævnt i bilag III til denne forordning, og som kan integrere en mikroprocessor til generelle formål. Kommissionen bør vedtage delegerede retsakter [senest 12 måneder efter denne forordnings ikrafttræden] for at

præcisere definitionerne af de produktkategorier, der er omfattet af kategori I og II, jf. bilag III.

(28) Denne forordning har en målrettet tilgang til cybersikkerhedsrisici. Produkter med digitale elementer kan imidlertid indebære andre sikkerhedsrisici, som ikke vedrører cybersikkerhed. Disse risici bør fortsat reguleres af anden relevant EU-produktlovgivning. Hvis ingen anden EU-harmoniseringslovgivning finder anvendelse, bør de være omfattet af forordning [forordningen om produktsikkerhed i almindelighed]. Uanset artikel 2, stk. 1, tredje afsnit, litra b), i forordning [forordningen om produktsikkerhed i almindelighed] bør kapitel III, afdeling 1, kapitel V og VII og kapitel IX-XI i forordning [forordningen om produktsikkerhed i almindelighed] i lyset af denne forordnings målrettede karakter derfor finde anvendelse på produkter med digitale elementer for så vidt angår sikkerhedsrisici, der ikke er omfattet af denne forordning, hvis disse produkter ikke er omfattet af specifikke krav i anden EU-harmoniseringslovgivning som defineret i [artikel 3, nr. 25), i forordningen om produktsikkerhed i almindelighed].

(29) Produkter med digitale elementer, der er klassificeret som højrisiko-AI-systemer i henhold til artikel 6 i forordning[15] [AI-forordningen], og som falder ind under denne forordnings anvendelsesområde, bør opfylde de væsentlige krav, der er fastsat i denne forordning. Når disse højrisiko-AI-systemer opfylder de væsentlige krav i denne forordning, bør de anses for at være i overensstemmelse med cybersikkerhedskravene i artikel [artikel 15] i forordning [AI-forordningen], såfremt disse krav er omfattet af EU-overensstemmelseserklæringen eller dele heraf udstedt i henhold til denne forordning. For så vidt angår overensstemmelsesvurderingsprocedurerne vedrørende de væsentlige cybersikkerhedskrav til et produkt med digitale elementer, der er omfattet af denne forordning og klassificeret som et højrisiko-AI-system, bør de relevante bestemmelser i artikel 43 i forordning [AI-forordningen] som hovedregel finde anvendelse i stedet for de respektive bestemmelser i denne forordning. Denne regel bør dog ikke resultere i en reduktion af den nødvendige grad af sikkerhed for kritiske produkter med digitale elementer omfattet af denne forordning. Uanset denne regel bør højrisiko-AI-systemer, der er omfattet af anvendelsesområdet for forordning [AI-forordningen] og også betragtes som kritiske produkter med digitale elementer i henhold til denne forordning, og som overensstemmelsesvurderingsproceduren baseret på intern kontrol som omhandlet i bilag VI til forordning [AI-forordningen] finder anvendelse på, derfor være omfattet af bestemmelserne om overensstemmelsesvurdering i denne forordning for så vidt angår de væsentlige krav i denne forordning. I dette tilfælde bør de respektive bestemmelser om overensstemmelsesvurdering på grundlag af intern kontrol, der er fastsat i bilag VI til forordning [AI-forordningen], finde anvendelse på alle andre aspekter, der er omfattet af forordning [AI-forordningen].

(30) Maskinprodukter omfattet af anvendelsesområdet for forordning [forslaget til maskinforordning], der er produkter med digitale elementer som defineret i denne forordning, og for hvilke der er udstedt en overensstemmelseserklæring i henhold til denne forordning, bør formodes at være i overensstemmelse med de væsentlige sikkerheds- og sundhedskrav i [bilag III, punkt 1.1.9 og 1.2.1] til forordning [forslaget til maskinforordning], for så vidt angår beskyttelse mod korruption og kontrolsystemernes sikkerhed og pålidelighed, såfremt overensstemmelsen med disse

[15] Forordning [AI-forordningen].

krav dokumenteres ved en EU-overensstemmelseserklæring udstedt i henhold til denne forordning.

(31) Forordning [forslaget til forordning om det europæiske sundhedsdataområde] supplerer de væsentlige krav, der er fastsat i denne forordning. De elektroniske patientjournalsystemer ("EPJ-systemer") omfattet af anvendelsesområdet for forordning [forslaget til forordning om det europæiske sundhedsdataområde], der er produkter med digitale elementer som defineret i denne forordning, bør derfor også opfylde de væsentlige krav, der er fastsat i denne forordning. Fabrikanterne af disse systemer bør påvise overensstemmelse som krævet i forordning [forslaget til forordning om det europæiske sundhedsdataområde]. For at lette overholdelsen kan fabrikanterne udarbejde en samlet teknisk dokumentation, som indeholder de elementer, der kræves i begge retsakter. Da denne forordning ikke omfatter SaaS som sådan, er EPJ-systemer, der tilbydes gennem SaaS-licens- og leveringsmodellen, ikke omfattet af denne forordnings anvendelsesområde. Tilsvarende er EPJ-systemer, der udvikles og anvendes internt, ikke omfattet af denne forordnings anvendelsesområde, da de ikke bringes i omsætning.

(32) For at sikre, at produkter med digitale elementer er sikre både på det tidspunkt, hvor de bringes i omsætning, og i hele deres livscyklus, er det nødvendigt at fastsætte væsentlige krav til sårbarhedshåndtering og væsentlige cybersikkerhedskrav vedrørende egenskaberne ved produkter med digitale elementer. Fabrikanterne bør opfylde alle væsentlige krav vedrørende håndtering af sårbarheder og sikre, at alle deres produkter leveres uden kendte sårbarheder, der kan udnyttes, og de bør afgøre, hvilke andre væsentlige krav vedrørende produktegenskaberne der er relevante for den pågældende produkttype. 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 krav og for på passende vis at anvende relevante harmoniserede standarder eller fælles specifikationer.

(33) For at forbedre sikkerheden af produkter med digitale elementer, der bringes i omsætning i det indre marked, er det nødvendigt at fastsætte væsentlige krav. Disse væsentlige krav bør ikke berøre de koordinerede EU-risikovurderinger af kritiske forsyningskæder indført ved [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)][16], hvor der tages hensyn til både tekniske og, hvor det er relevant, ikketekniske risikofaktorer såsom et tredjelands utilbørlige indflydelse på leverandører. Det 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 henstilling (EU) 2019/534, i den EU-dækkende koordinerede risikovurdering af 5G-netsikkerhed og i EU-værktøjskassen om 5G-cybersikkerhed, som NIS-samarbejdsgruppen er nået til enighed om, jf. [direktiv XXX/XXXX (NIS2)].

(34) For at sikre, at de nationale CSIRT'er og det centrale kontaktpunkt, der er udpeget i overensstemmelse med artikel [artikel X] i direktiv [direktiv XX/XXXX (NIS2)], får de oplysninger, der er nødvendige for, at de kan udføre deres opgaver og øge det overordnede cybersikkerhedsniveau for væsentlige og vigtige enheder, og for at sikre, at markedsovervågningsmyndighederne fungerer effektivt, bør fabrikanter af

[16] Europa-Parlamentets og Rådets direktiv XXX af [dato] [om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 (EUT L xx af dato, s. x)].

produkter med digitale elementer underrette ENISA om sårbarheder, der udnyttes aktivt. Da de fleste produkter med digitale elementer markedsføres i hele det indre marked, bør enhver udnyttet sårbarhed i et produkt med digitale elementer betragtes som en trussel mod det indre markeds funktion. Fabrikanterne bør også overveje at offentliggøre afhjulpne sårbarheder i den europæiske sårbarhedsdatabase, der er oprettet i henhold til direktiv [direktiv XX/XXXX (NIS2)] og forvaltes af ENISA, eller i en anden offentligt tilgængelig sårbarhedsdatabase.

(35) Fabrikanterne bør også underrette ENISA om enhver hændelse, der indvirker på sikkerheden af produktet med digitale elementer. Uanset forpligtelserne til underretning om hændelser i direktiv [XXX/XXXX (NIS2)] for væsentlige og vigtige enheder er det afgørende for ENISA, de centrale kontaktpunkter, der er udpeget af medlemsstaterne i overensstemmelse med artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)], og markedsovervågningsmyndighederne at modtage oplysninger fra fabrikanter af produkter med digitale elementer, der gør det muligt for dem at vurdere disse produkters sikkerhed. For at sikre, at brugerne kan reagere hurtigt på hændelser, der har indvirkning på sikkerheden af deres produkter med digitale elementer, bør fabrikanterne også underrette deres brugere om en sådan hændelse og, hvor det er relevant, 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 hvis fabrikanten har mulighed for at kontakte brugerne, ved at kontakte brugerne direkte, hvis risiciene berettiger det.

(36) 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. En 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. 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 (såkaldte "bug bounty-programmer").

(37) 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, og den gør det navnlig lettere for fabrikanter og brugere at spore kendte nyligt opståede sårbarheder og risici. Det er særlig vigtigt for fabrikanterne at sikre, at deres produkter ikke indeholder sårbare komponenter udviklet af tredjeparter.

(38) 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 krav i denne forordning til detaljerede tekniske specifikationer og er vedtaget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU)

nr. 1025/2012[17]. Forordning (EU) nr. 1025/2012 fastsætter bestemmelser om en procedure for indsigelse mod harmoniserede standarder i tilfælde, hvor disse standarder ikke fuldt ud opfylder kravene i denne forordning.

(39) Ved forordning (EU) 2019/881 oprettes en frivillig europæisk ramme for cybersikkerhedscertificering af IKT-produkter, -processer og -tjenester. Europæiske cybersikkerhedscertificeringsordninger kan omfatte produkter med digitale elementer omfattet af denne forordning. Denne forordning bør skabe synergier med forordning (EU) 2019/881. For at lette vurderingen af overensstemmelsen med kravene i denne forordning formodes produkter med digitale elementer, der er certificeret, eller for hvilke der er udstedt en overensstemmelseserklæring i henhold til en cybersikkerhedsordning i henhold til forordning (EU) 2019/881, og som Kommissionen har identificeret i en gennemførelsesretsakt, at være i overensstemmelse med de væsentlige krav i denne forordning, såfremt cybersikkerhedsattesten eller overensstemmelseserklæringen eller dele heraf dækker disse krav. Behovet for nye europæiske cybersikkerhedscertificeringsordninger for produkter med digitale elementer bør vurderes i lyset af denne forordning. I sådanne fremtidige europæiske cybersikkerhedscertificeringsordninger, der dækker produkter med digitale elementer, bør der tages hensyn til de væsentlige krav i denne forordning, og de bør lette overholdelsen af denne forordning. Kommissionen bør tillægges beføjelser til ved hjælp af gennemførelsesretsakter at præcisere de europæiske cybersikkerhedscertificeringsordninger, der kan anvendes til at påvise overensstemmelse med de væsentlige krav i denne forordning. For at undgå unødige administrative byrder for fabrikanter bør Kommissionen endvidere, hvor det er relevant, præcisere, om en cybersikkerhedsattest, der er udstedt i henhold til sådanne europæiske cybersikkerhedscertificeringsordninger, fritager fabrikanten fra forpligtelsen til at lade foretage en overensstemmelsesvurdering af tredjepart vedrørende tilsvarende krav som omhandlet denne forordning.

(40) Ved gennemførelsesretsaktens ikrafttræden [Kommissionens gennemførelsesforordning (EU) nr. …/... af XXX om den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier] (EUCC) vedrørende hardwareprodukter omfattet af denne forordning såsom hardwaresikkerhedsmoduler og mikroprocessorer kan Kommissionen ved hjælp af en gennemførelsesretsakt præcisere, hvordan EUCC giver formodning om overensstemmelse med de væsentlige krav i bilag I til denne forordning eller dele heraf. Desuden kan en sådan gennemførelsesretsakt præcisere, hvordan en attest udstedt i henhold til EUCC fritager fabrikanterne fra forpligtelsen til at lade foretage en tredjepartsvurdering som krævet i denne forordning vedrørende tilsvarende krav.

(41) Hvis der ikke vedtages harmoniserede standarder, eller hvis de harmoniserede standarder ikke i tilstrækkelig grad opfylder de væsentlige krav i denne forordning, bør Kommissionen kunne vedtage fælles specifikationer ved hjælp af gennemførelsesretsakter. Begrundelsen for at udvikle sådanne fælles specifikationer i stedet for at basere sig på harmoniserede standarder kan være, at ingen af de europæiske standardiseringsorganisationer har imødekommet

[17] 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 316 af 14.11.2012, s. 12).

standardiseringsanmodningen, unødige forsinkelser i udarbejdelsen af passende harmoniserede standarder eller udviklede standarders manglende overholdelse af kravene i denne forordning eller af en anmodning fra Kommissionen. Med henblik på at gøre det lettere at vurdere overensstemmelsen med de væsentlige krav 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.

(42) Fabrikanterne bør udfærdige en EU-overensstemmelseserklæring for at afgive de efter denne forordning krævede oplysninger om overensstemmelsen af produkter med digitale elementer med de væsentlige krav i denne forordning og, hvor det er relevant, med anden relevant EU-harmoniseringslovgivning, som produktet er omfattet af. Fabrikanter kan også blive pålagt at udarbejde en EU-overensstemmelseserklæring i henhold til anden EU-lovgivning. 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 en sådan enkelt EU-overensstemmelseserklæring at tage form af et dossier bestående af de relevante individuelle overensstemmelseserklæringer.

(43) 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[18]. Der bør i denne 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 denne forordning.

(44) For at gøre det muligt for erhvervsdrivende at påvise overensstemmelse med de væsentlige krav 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[19] fastsætter moduler for overensstemmelsesvurderingsprocedurer alt efter risikoniveauet og det krævede sikkerhedsniveau. For at sikre kohærens mellem de forskellige sektorer og undgå ad hoc-varianter er der blevet indført passende overensstemmelsesvurderingsprocedurer til kontrol af, om produkter med digitale elementer er i overensstemmelse med de væsentlige krav i denne forordning, 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, prøvning og vedligeholdelse af produktet.

(45) Som hovedregel bør overensstemmelsesvurderingen af produkter med digitale elementer foretages af fabrikanten på eget ansvar i henhold til proceduren baseret på modul A i afgørelse 768/2008/EF. Fabrikanten bør have fleksibilitet til at vælge en

---

[18] 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).

[19] 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).

strengere overensstemmelsesvurderingsprocedure, der involverer en tredjepart. Hvis produktet er klassificeret som et kritisk produkt i klasse I, kræves der yderligere sikkerhed for at påvise overensstemmelse med de væsentlige krav i denne forordning. Fabrikanten bør anvende harmoniserede standarder, fælles specifikationer eller cybersikkerhedscertificeringsordninger 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 cybersikkerhedscertificeringsordninger, bør fabrikanten lade foretage en overensstemmelsesvurdering af tredjepart. 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 + C eller modul H i afgørelse 768/2008/EF blevet valgt som værende mest hensigtsmæssige til at vurdere overensstemmelsen af kritiske produkter med digitale elementer på en forholdsmæssig og effektiv måde. Den fabrikant, der lader tredjepart foretage overensstemmelsesvurderingen, kan vælge den procedure, der passer bedst til fabrikantens design- og produktionsproces. I betragtning af den endnu større cybersikkerhedsrisiko forbundet med anvendelsen af produkter, der er klassificeret som kritiske klasse II-produkter, bør overensstemmelsesvurderingen altid involvere en tredjepart.

(46) 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 betragtes som aktiviteter, der svarer til produktion, når de relevante overensstemmelsesvurderingsmoduler anvendes til at verificere produktets overensstemmelse med de væsentlige krav i denne forordning i hele design-, udviklings- og produktionsfasen.

(47) Med henblik på af tredjeparter foretagne overensstemmelsesvurderinger 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 interessekonflikter.

(48) 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, notifikation og overvågning af bemyndigede organer. Den ordning, der fastsættes i 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 anvendelsen heraf også omfatte notifikationsformål.

(49) De nationale offentlige myndigheder i hele Unionen bør betragte en gennemsigtig akkreditering, jf. forordning (EF) nr. 765/2008, der sikrer den fornødne tillid til overensstemmelsesattester, som det foretrukne middel til dokumentation af overensstemmelsesvurderingsorganers tekniske kompetence. De nationale myndigheder kan imidlertid mene, 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.

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

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

(52) Da 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 en eventuel tvivl eller usikkerhed om overensstemmelsesvurderingsorganers kompetence kan afklares, før de påbegynder deres aktiviteter som bemyndigede organer.

(53) 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, må det sikres, at den tekniske anvendelse af overensstemmelsesvurderingsprocedurer er ensartet. Dette kan bedst opnås gennem koordinering og samarbejde mellem de bemyndigede organer.

(54) Markedsovervågning er et væsentligt instrument til at sikre en korrekt og ensartet anvendelse af EU-lovgivningen. Der bør derfor skabes juridiske rammer, inden for hvilke markedsovervågningen kan foretages på en passende måde. Bestemmelserne om EU-markedsovervågning og kontrol af produkter, der indføres på EU-markedet, i Europa-Parlamentets og Rådets forordning (EU) 2019/1020[20] finder anvendelse på produkter med digitale elementer, der er omfattet af denne forordning.

(55) I overensstemmelse med forordning (EU) 2019/1020 udfører markedsovervågningsmyndighederne markedsovervågning i den pågældende medlemsstat. Denne forordning bør ikke hindre medlemsstaterne i at udvælge de kompetente myndigheder, der skal udføre disse opgaver. Hver medlemsstat bør udpege en eller flere markedsovervågningsmyndigheder på dens område. Medlemsstaterne kan vælge at udpege enhver eksisterende eller ny myndighed som markedsovervågningsmyndighed, herunder nationale kompetente myndigheder som omhandlet i artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)], eller udpegede nationale cybersikkerhedscertificeringsmyndigheder som omhandlet i

[20] 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).

artikel 58 i forordning (EU) 2019/881. Erhvervsdrivende bør samarbejde fuldt ud med markedsovervågningsmyndighederne 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 overvågningsopgaverne i forbindelse med denne 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.

(56) Der bør oprettes en særlig administrativ samarbejdsgruppe (ADCO) med henblik på ensartet gennemførelse af denne forordning i henhold til artikel 30, stk. 2, i forordning (EU) 2019/1020. Denne 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 artikel 10 i forordning (EU) 2019/1020 og en valgfri national ekspert, formændene for ADCO'erne og repræsentanter for Kommissionen. Kommissionen bør deltage i netværkets møder, dets undergrupper og den pågældende ADCO. Den bør også bistå denne ADCO med et administrativt sekretariat, der yder teknisk og logistisk støtte.

(57) For at sikre rettidige, forholdsmæssige og effektive foranstaltninger i forbindelse med produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, bør der fastsættes en EU-beskyttelsesprocedure, hvorved de 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, hvis det er nødvendigt. Når 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.

(58) I visse tilfælde kan et produkt med digitale elementer, der opfylder kravene i 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 af den type, der er omhandlet i [bilag I til direktiv XXX/XXXX (NIS2)], eller for andre samfundsinteresser. 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 en risiko, eller at det tilbagekaldes eller trækkes tilbage, afhængigt af risikoen. Når en markedsovervågningsmyndighed således begrænser eller forbyder den frie bevægelighed for et produkt, bør medlemsstaten straks underrette Kommissionen og de øvrige medlemsstater om de foreløbige foranstaltninger og angive begrundelserne for afgørelsen. Hvis en markedsovervågningsmyndighed vedtager sådanne

foranstaltninger over for produkter, der udgør en risiko, bør Kommissionen rådføre sig med medlemsstaterne og den eller de relevante erhvervsdrivende og evaluere den nationale foranstaltning. På grundlag af resultaterne af denne vurdering bør Kommissionen træffe afgørelse om, hvorvidt den nationale foranstaltning er berettiget eller ej. Kommissionen bør rette sin afgørelse til alle medlemsstaterne og straks meddele den til disse og til den eller de relevante erhvervsdrivende. Hvis foranstaltningen anses for at være berettiget, kan Kommissionen også overveje at vedtage forslag til revision af den pågældende EU-lovgivning.

(59) For produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, og hvor der er grund til at tro, at disse ikke opfylder kravene i denne forordning, eller for produkter, som opfylder kravene i denne forordning, men indebærer andre betydelige risici såsom risici for menneskers sundhed eller sikkerhed, grundlæggende rettigheder eller tjenester, der leveres af væsentlige enheder af den type, der er omhandlet i [bilag I til direktiv XXX/XXXX (NIS2)], kan Kommissionen anmode ENISA om at foretage en evaluering. På grundlag af denne evaluering kan Kommissionen ved hjælp af gennemførelsesretsakter vedtage korrigerende eller restriktive foranstaltninger på EU-plan, herunder påbud om at trække de pågældende produkter tilbage fra markedet eller tilbagekalde dem inden for en rimelig tidsfrist, som den fastsætter i forhold til risikoens art. Kommissionen kan kun foretage et sådant indgreb under ekstraordinære omstændigheder, der berettiger et hurtigt indgreb for at bevare et velfungerende indre marked, og kun hvis tilsynsmyndighederne ikke har truffet effektive foranstaltninger til at rette op på situationen. Sådanne ekstraordinære omstændigheder kan være nødsituationer, f.eks. hvor et produkt, der ikke opfylder kravene, gøres bredt tilgængeligt af fabrikanten i flere medlemsstater og også anvendes af enheder i nøglesektorer omfattet af [direktiv XXX/XXXX (NIS2)], selv om det indeholder kendte sårbarheder, der udnyttes af ondsindede aktører, og som fabrikanten ikke udsender rettelser til. Kommissionen kan kun gribe ind i sådanne nødsituationer, så længe de ekstraordinære omstændigheder er til stede, og hvis den manglende overholdelse af denne forordning eller de betydelige risici forbundet hermed fortsat er til stede.

(60) I tilfælde, 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.

(61) Samtidige koordinerede kontrolaktioner er specifikke håndhævelsesforanstaltninger truffet af markedsovervågningsmyndighederne, som kan forbedre produktsikkerheden. Kontrolaktioner bør navnlig foretages, hvis markedstendenser, forbrugerklager eller andre forhold tyder på, at visse produktkategorier ofte viser sig at udgøre en cybersikkerhedsrisiko. ENISA bør indsende forslag til produktkategorier, for hvilke der kan tilrettelægges kontrolaktioner, til markedsovervågningsmyndighederne, bl.a. på grundlag af de underretninger om produktsårbarheder og hændelser, som agenturet modtager.

(62) For at sikre, at den lovgivningsmæssige ramme kan tilpasses om nødvendigt, bør Kommissionen delegeres beføjelse til at vedtage retsakter, jf. artikel 290 i TEUF, for så vidt angår opdateringer af listen over kritiske produkter i bilag III og præcisering af definitionerne af disse produktkategorier. Kommissionen bør tillægges beføjelse til at vedtage retsakter 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. Kommissionen bør tillægges beføjelse til at vedtage retsakter i overensstemmelse med nævnte artikel for så vidt angår potentiel tildeling af mandat til certificering af visse meget kritiske produkter med digitale elementer baseret på de kriterier, der er fastsat i denne forordning, samt for så vidt angår præcisering af minimumsindholdet i EU-overensstemmelseserklæringen og supplering af 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[21]. 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 forberedelsen af delegerede retsakter.

(63) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser til at præcisere formatet for og elementerne i softwarekomponentlisten, præcisere typen af oplysninger, formatet og proceduren for underretninger om aktivt udnyttede sårbarheder og hændelser indgivet af fabrikanterne til ENISA, præcisere de europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til forordning (EU) 2019/881, som kan anvendes til at påvise overensstemmelse med de væsentlige krav eller dele heraf som fastsat i bilag I til nærværende forordning, vedtage fælles specifikationer for de væsentlige krav i bilag I, fastsætte tekniske specifikationer for piktogrammer eller andre mærker vedrørende sikkerheden af produkter med digitale elementer og mekanismer til at fremme deres anvendelse og træffe afgørelse om korrigerende eller restriktive 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[22].

(64) 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.

(65) 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 lovgivning 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 andre markedsovervågningsmyndigheder allerede har pålagt den samme erhvervsdrivende administrative bøder for lignende overtrædelser. Sådanne omstændigheder kan enten

[21] EUT L 123 af 12.5.2016, s. 1.

[22] 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).

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.

(66) Når personer, 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.

(67) I sine forbindelser med tredjelande tilstræber EU at fremme den internationale handel med regulerede produkter. Der kan anvendes en lang række foranstaltninger til at fremme handelen, 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 Den Europæiske Union og tredjelande, der er på samme tekniske udviklingsniveau og har en forenelig tilgang til overensstemmelsesvurdering. Disse aftaler er baseret på gensidig accept af certifikater, overensstemmelsesmærkninger og prøvningsrapporter udstedt af parternes overensstemmelsesvurderingsorganer i overensstemmelse med den anden parts lovgivning. I øjeblikket er der indgået aftaler om gensidig anerkendelse med flere lande. Aftalerne er indgået i en række specifikke sektorer, der varierer fra land til land. 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 partnerlande 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 EU.

(68) Kommissionen bør regelmæssigt tage denne forordnings bestemmelser op til fornyet overvejelse efter høring af interesserede parter, navnlig med henblik på at afgøre, om der er behov for ændringer i lyset af skiftende samfundsmæssige, politiske eller teknologiske vilkår eller markedsvilkår.

(69) Økonomiske aktører bør have tilstrækkelig tid til at tilpasse sig kravene i denne forordning. Denne forordning bør anvendes [24 måneder] fra dens ikrafttræden med undtagelse af rapporteringsforpligtelserne vedrørende aktivt udnyttede sårbarheder og hændelser, som bør finde anvendelse [12 måneder] fra denne forordnings ikrafttræden.

(70) Målet for denne forordning kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens 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.

(71) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725[23] og afgav udtalelse den […] —

VEDTAGET DENNE FORORDNING—

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand

Ved denne forordning fastsættes:

(a) regler for omsætning af produkter med digitale elementer for at sikre cybersikkerheden for sådanne produkter

(b) væsentlige krav 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 krav til sårbarhedshåndteringsprocesser, som fabrikanterne skal indføre for at sikre cybersikkerheden for produkter med digitale elementer i hele deres livscyklus, og forpligtelser for erhvervsdrivende i forbindelse med disse processer

(d) regler om markedsovervågning og håndhævelse af ovennævnte regler og krav.

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på produkter med digitale elementer, hvis tilsigtede og med rimelighed 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. 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

[23] 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).

risici, som er omfattet af de væsentlige krav 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 beskyttelsesniveau som det, der er fastsat i denne forordning.

Kommissionen tillægges beføjelse til i overensstemmelse med artikel 50 at vedtage delegerede retsakter om ændring af denne forordning for at præcisere, om en sådan begrænsning eller udelukkelse er nødvendig, de pågældende produkter og regler samt begrænsningens anvendelsesområde, hvis det er relevant.

5. Denne forordning finder ikke anvendelse på produkter med digitale elementer, der udelukkende udvikles til nationale sikkerhedsformål eller militære formål, eller på produkter, der er specifikt designet til at behandle klassificerede oplysninger.

Artikel 3

Definitioner

I denne forordning forstås ved:

(1) "produkt med digitale elementer": ethvert software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der skal bringes i omsætning separat

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

(3) "kritisk produkt med digitale elementer": et produkt med digitale elementer, der udgør en cybersikkerhedsrisiko i henhold til kriterierne i artikel 6, stk. 2, og hvis væsentligste funktion er fastsat i bilag III

(4) "meget kritisk produkt med digitale elementer": et produkt med digitale elementer, der udgør en cybersikkerhedsrisiko i henhold til kriterierne i artikel 6, stk. 5

(5) "operationel teknologi": programmerbare digitale systemer eller enheder, der interagerer med det fysiske miljø eller styrer enheder, der interagerer med det fysiske miljø

(6) "software": den del af et elektronisk informationssystem, der består af maskinkode

(7) "hardware": et fysisk elektronisk informationssystem eller dele heraf, der kan behandle, lagre eller overføre digitale data

(8) "komponent": software eller hardware, der er beregnet til integration i et elektronisk informationssystem

(9) "elektronisk informationssystem": ethvert system, herunder elektrisk eller elektronisk udstyr, der kan behandle, lagre eller overføre digitale data

(10) "logisk forbindelse": virtuel gengivelse af en dataforbindelse via en softwaregrænseflade

(11) "fysisk forbindelse": enhver forbindelse mellem elektroniske informationssystemer eller komponenter, der implementeres ved hjælp af fysiske midler, herunder via elektriske eller mekaniske grænseflader, kabler eller radiobølger

(12) "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

(13) "privilegium": en adgangsret, der tildeles bestemte brugere eller programmer med henblik på udførelse af sikkerhedsrelevante operationer i et elektronisk informationssystem

(14) "forhøjet privilegium": en adgangsret, der tildeles bestemte brugere eller programmer med henblik på udførelse af et udvidet sæt sikkerhedsrelevante operationer i et elektronisk informationssystem, der — hvis den misbruges eller kompromitteres — kan give en ondsindet aktør mulighed for at få bredere adgang til et systems eller en organisations ressourcer

(15) "endepunkt": enhver enhed, der er tilsluttet et netværk og fungerer som indgangspunkt til dette netværk

(16) "netværks- eller databehandlingsressourcer": data- eller hardware- eller softwarefunktioner, der er tilgængelige enten lokalt eller gennem et netværk eller en anden forbundet enhed

(17) "erhvervsdrivende": fabrikanten, den bemyndigede repræsentant, importøren, distributøren eller enhver anden fysisk eller juridisk person, der er underlagt forpligtelser i henhold til denne forordning

(18) "fabrikant": enhver fysisk eller juridisk person, som udvikler eller fremstiller produkter med digitale elementer eller får produkter med digitale elementer designet, udviklet eller fremstillet og markedsfører dem under eget navn eller varemærke mod eller uden vederlag

(19) "bemyndiget repræsentant": enhver 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

(20) "importør": enhver fysisk eller juridisk person, der er etableret i Unionen, og som bringer et produkt med digitale elementer, som bærer en uden for Unionen etableret fysisk eller juridisk persons navn eller varemærke, i omsætning

(21) "distributør": enhver fysisk eller juridisk person i forsyningskæden ud over fabrikanten eller importøren, som gør et produkt med digitale elementer tilgængeligt på EU-markedet uden at have indflydelse på dets egenskaber

(22) "bringe i omsætning": første tilgængeliggørelse af et produkt med digitale elementer på EU-markedet

(23) "gøre tilgængelig på markedet": enhver levering af et produkt med digitale elementer med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed mod eller uden vederlag

(24) "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, reklame- eller salgsmaterialet eller reklame- og salgserklæringerne samt i den tekniske dokumentation

(25) "anvendelse, der med rimelighed kan forudses": anvendelse, som ikke nødvendigvis er det tilsigtede formål, som fabrikanten har angivet i brugsanvisningerne, 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

(26) "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

(27) "bemyndigende myndighed": den nationale myndighed, der er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering, udpegelse og notifikation af overensstemmelsesvurderingsorganer og for overvågning heraf

(28) "overensstemmelsesvurdering": en proces til verificering af, om de væsentlige krav i bilag I er opfyldt

(29) "overensstemmelsesvurderingsorgan": et organ som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008

(30) "bemyndiget organ": et overensstemmelsesvurderingsorgan, der er udpeget i overensstemmelse med artikel 33 i denne forordning og anden relevant EU-harmoniseringslovgivning

(31) "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 krav i bilag I, punkt 1, eller medfører en ændring af den tilsigtede anvendelse af produktet med digitale elementer

(32) "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 krav i bilag I og anden gældende EU-lovgivning om harmonisering af betingelserne for markedsføring af produkter ("EU-harmoniseringslovgivning") om anbringelse af denne mærkning

(33) "markedsovervågningsmyndighed": myndighed som defineret i artikel 3, nr. 4), i forordning (EU) 2019/1020

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

(35) "cybersikkerhedsrisiko": risiko som defineret i artikel [artikel X] i direktiv [XXX/XXXX (NIS2)]

(36) "væsentlig cybersikkerhedsrisiko": en cybersikkerhedsrisiko, hvor der som følge af dens tekniske egenskaber 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

(37) "softwarekomponentliste" (SBOM — software bill of materials): en formel fortegnelse med nærmere oplysninger om og forsyningskæderelationer for komponenter, der indgår i softwareelementerne i et produkt med digitale elementer

(38) "sårbarhed": sårbarhed som defineret i artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)]

(39) "aktivt udnyttet sårbarhed": en sårbarhed, hvor der er pålidelig dokumentation for, at en aktør har installeret ondsindet kode på et system uden tilladelse fra systemejeren

(40) "personoplysninger": oplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679.

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 og udstillinger samt ved demonstrationer eller lignende begivenheder præsenteres og anvendes et produkt med digitale elementer, der ikke er i overensstemmelse med denne forordning.

3. Medlemsstaterne må ikke forhindre tilgængeliggørelse af ufærdig software, der ikke er i overensstemmelse med denne forordning, såfremt softwaren kun gøres tilgængelig i et begrænset tidsrum, der er nødvendigt til prøvningsformål, og det ved synlig skiltning klart er anført, at den pågældende software ikke er i overensstemmelse med denne forordning og ikke vil være tilgængelig på markedet til andre formål end prøvning.

Artikel 5

Krav til produkter med digitale elementer

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

(1) de opfylder de væsentlige krav i bilag I, punkt 1, forudsat at de er korrekt installeret og vedligeholdt og anvendes til det tilsigtede formål eller på betingelser, som med rimelighed kan forudses, og opdateres, hvor det er relevant

(2) de processer, som fabrikanten har indført, opfylder de væsentlige krav i bilag I, punkt 2.

Artikel 6

Kritiske produkter med digitale elementer

1. Produkter med digitale elementer, der tilhører en kategori, som er opført i bilag III, betragtes som kritiske produkter med digitale elementer. Produkter, hvis væsentligste funktion henhører under en kategori opført i bilag III til denne forordning, anses for at falde ind under denne kategori. Kategorier af kritiske produkter med digitale elementer inddeles i klasse I og klasse II som fastsat i bilag III, der afspejler cybersikkerhedsniveauet for disse produkter.

2. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 50 med henblik på at ændre bilag III ved at føje en ny kategori til eller fjerne en eksisterende kategori fra listen over kategorier af kritiske produkter med digitale elementer. Ved vurderingen af behovet for at ændre listen i bilag III tager Kommissionen hensyn til cybersikkerhedsrisikoniveauet for kategorien af produkter med digitale elementer. Ved fastsættelsen af cybersikkerhedsrisikoniveauet tages et eller flere af følgende kriterier i betragtning:

(a) den cybersikkerhedsrelaterede funktionalitet i produktet med digitale elementer, og hvorvidt produktet med digitale elementer har mindst én af følgende egenskaber:

(i) det er designet til at køre med forhøjet privilegium eller forvalte privilegier

(ii) det har direkte eller privilegeret adgang til netværks- eller computerressourcer

(iii) det er designet til at kontrollere adgangen til data eller operationel teknologi

(iv) det udfører en funktion, der er afgørende for tilliden, navnlig sikkerhedsfunktioner såsom netkontrol, endepunktssikkerhed og netværksbeskyttelse.

(b) den tilsigtede anvendelse i følsomme miljøer, herunder i industrielle miljøer eller af væsentlige enheder af den type, der er omhandlet i bilag [bilag I] til direktiv [direktiv XXX/XXXX (NIS2)]

(c) den tilsigtede anvendelse af kritiske eller følsomme funktioner såsom behandling af personoplysninger

(d) det potentielle omfang af en negativ indvirkning, navnlig med hensyn til alvorlighed og mulighed for påvirkning af flere personer

(e) i hvilket omfang anvendelsen af produkter med digitale elementer allerede har forårsaget materielle eller immaterielle tab eller forstyrrelser eller har givet anledning til betydelig bekymring med hensyn til forekomsten af en negativ indvirkning.

3. Kommissionen tillægges beføjelser til at vedtage en delegeret retsakt i overensstemmelse med artikel 50 med henblik på at supplere denne forordning ved at præcisere definitionerne af produktkategorierne i kategori I og kategori II som fastsat i bilag III. Den delegerede retsakt vedtages den [*senest 12 måneder efter datoen for denne forordnings ikrafttræden*].

4. Kritiske produkter med digitale elementer er omfattet af de overensstemmelsesvurderingsprocedurer, der er omhandlet i artikel 24, stk. 2 og 3.

5. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 50 med henblik på at supplere denne forordning ved at præcisere de kategorier af meget kritiske produkter med digitale elementer, for hvilke fabrikanterne skal indhente en europæisk cybersikkerhedsattest i henhold til en europæisk cybersikkerhedscertificeringsordning i henhold til forordning (EU) 2019/881 for at påvise overensstemmelse med de væsentlige krav i bilag I eller dele deraf. Ved fastlæggelsen af sådanne kategorier af meget kritiske produkter med digitale elementer tager Kommissionen hensyn til cybersikkerhedsrisikoniveauet for kategorien af produkter med digitale elementer på grundlag af et eller flere af kriterierne i stk. 2 samt vurderingen af, om denne produktkategori:

(a) anvendes af de væsentlige enheder af den type, der er omhandlet i bilag [bilag I] til direktiv [direktiv XXX/XXXX (NIS2)], eller vil have potentiel fremtidig betydning for disse enheders aktiviteter eller

(b) er relevant for modstandsdygtigheden i den samlede forsyningskæde for produkter med digitale elementer over for afbrydelser.

Artikel 7

Produktsikkerhed i almindelighed

Uanset artikel 2, stk. 1, tredje afsnit, litra b), i forordning [forordningen om produktsikkerhed i almindelighed] finder kapitel III, afdeling 1, kapitel V og VII og kapitel IX-XI i forordning [forordningen om produktsikkerhed i almindelighed] anvendelse på produkter med digitale elementer for så vidt angår sikkerhedsrisici, der ikke er omfattet af denne forordning, såfremt disse produkter ikke er omfattet af specifikke krav i anden EU-harmoniseringslovgivning som defineret i [artikel 3, nr. 25), i forordningen om produktsikkerhed i almindelighed].

Artikel 8

Højrisiko-AI-systemer

1. Produkter med digitale elementer klassificeret som højrisiko-AI-systemer i overensstemmelse med artikel [artikel 6] i forordning [AI-forordningen], som falder ind under denne forordnings anvendelsesområde og opfylder de væsentlige krav i bilag I, punkt 1, i denne forordning, og processer indført af fabrikanten, som er i overensstemmelse med de væsentlige krav i bilag I, punkt 2, anses for at være i overensstemmelse med cybersikkerhedskravene i artikel [artikel 15] i forordning [AI-forordningen], uden at dette berører de øvrige krav til nøjagtighed og robusthed i ovennævnte artikel, og for så vidt som opnåelsen af det påkrævede beskyttelsesniveau i henhold til disse krav dokumenteres ved en EU-overensstemmelseserklæring udstedt i henhold til denne forordning.

2. For de i stk. 1 nævnte produkter og cybersikkerhedskrav finder den relevante overensstemmelsesvurderingsprocedure som omhandlet i artikel [artikel 43] i forordning [AI-forordningen] anvendelse. Med henblik på denne vurdering har bemyndigede organer, der er blevet bemyndiget til at kontrollere højrisiko-AI-systemernes overensstemmelse i henhold til forordning (AI-forordningen), også ret til at kontrollere, at højrisiko-AI-systemerne inden for nærværende forordnings anvendelsesområde opfylder kravene i nærværende forordnings bilag I, forudsat at disse bemyndigede organers overholdelse af kravene i nærværende forordnings artikel 29 er blevet vurderet i forbindelse med bemyndigelsesproceduren i henhold til forordning [AI-forordningen].

3. Uanset stk. 2 er kritiske produkter med digitale elementer opført i bilag III til denne forordning, der er omfattet af overensstemmelsesvurderingsprocedurerne i artikel 24, stk. 2, litra a) og b), og artikel 24, stk. 3, litra a) og b), i denne forordning, og som også er klassificeret som højrisiko-AI-systemer i henhold til artikel [artikel 6] i forordning [AI-forordningen], og på hvilke overensstemmelsesvurderingsproceduren baseret på intern kontrol som omhandlet i bilag [bilag VI] til forordning [AI-forordningen] finder anvendelse, omfattet af overensstemmelsesvurderingsprocedurerne i henhold til denne forordning for så vidt angår de væsentlige krav i denne forordning.

Artikel 9

Maskinprodukter

Maskinprodukter omfattet af anvendelsesområdet for forordning [forslaget til maskinforordning], der er produkter med digitale elementer som defineret i denne forordning, og for hvilke der er udstedt en EU-overensstemmelseserklæring i henhold til denne

forordning, formodes at være i overensstemmelse med de væsentlige sikkerheds- og sundhedskrav i bilag [bilag III, punkt 1.1.9 og 1.2.1] til forordning [forslaget til maskinforordning], for så vidt angår beskyttelse mod korruption og kontrolsystemernes sikkerhed og pålidelighed, og for så vidt som opnåelsen af det påkrævede beskyttelsesniveau i henhold til disse krav dokumenteres ved en EU-overensstemmelseserklæring udstedt i henhold til denne forordning.

KAPITEL II

ERHVERVSDRIVENDES FORPLIGTELSER

Artikel 10

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 krav i bilag I, punkt 1.

2. Med henblik på at opfylde forpligtelsen i 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 sikkerhedshændelser og minimere virkningerne af sådanne hændelser, herunder i forbindelse med brugernes sundhed og sikkerhed.

3. Når et produkt med digitale elementer bringes i omsætning, medtager fabrikanten en cybersikkerhedsrisikovurdering i den tekniske dokumentation, jf. artikel 23 og bilag V. For produkter med digitale elementer som omhandlet i artikel 8 og artikel 24, stk. 4, der også er omfattet af andre EU-retsakter, kan cybersikkerhedsrisikovurderingen indgå i den risikovurdering, der kræves i henhold til disse respektive EU-retsakter. Hvis visse væsentlige krav ikke finder anvendelse på det markedsførte produkt med digitale elementer, medtager fabrikanten en klar begrundelse i denne dokumentation.

4. Med henblik på at opfylde forpligtelsen i stk. 1 skal fabrikanten udvise rettidig omhu ved integreringen af komponenter fra tredjeparter i produkter med digitale elementer. Fabrikanten sikrer, at sådanne komponenter ikke bringer sikkerheden af produktet med digitale elementer i fare.

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

6. Når et produkt med digitale elementer bringes i omsætning, sikrer fabrikanten i produktets forventede levetid eller i en periode på fem år efter, at produktet er bragt i omsætning, alt efter hvilken periode der er kortest, at det pågældende produkts sårbarheder håndteres effektivt og i overensstemmelse med de væsentlige krav i bilag I, punkt 2.

   Fabrikanten indfører passende politikker og procedurer, herunder politikker for koordineret offentliggørelse af sårbarheder, jf. bilag I, punkt 2, nr. 5, til håndtering

og afhjælpning af potentielle sårbarheder i produktet med digitale elementer indberettet fra interne eller eksterne kilder.

7. Inden et produkt med digitale elementer bringes i omsætning, udarbejder fabrikanten den tekniske dokumentation, der er omhandlet i artikel 23.

   Fabrikanten gennemfører eller får gennemført de valgte overensstemmelsesvurderingsprocedurer i artikel 24.

   Når det ved en af disse overensstemmelsesvurderingsprocedurer er blevet dokumenteret, at produktet med digitale elementer overholder de væsentlige krav i bilag I, punkt 1, og at de processer, som fabrikanten har indført, overholder de væsentlige krav i bilag I, punkt 2, udarbejder fabrikanten EU-overensstemmelseserklæringen i overensstemmelse med artikel 20 og anbringer CE-mærkningen i overensstemmelse med artikel 22.

8. Fabrikanten opbevarer den tekniske dokumentation og EU-overensstemmelseserklæringen, hvor det er relevant, så den i ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, står til rådighed for de nationale markedsovervågningsmyndigheder.

9. 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, i designet af produktet med digitale elementer eller i produktets egenskaber og til ændringer i de harmoniserede standarder, europæiske cybersikkerhedscertificeringsordninger eller de fælles specifikationer omhandlet i artikel 19, 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.

10. Fabrikanten sikrer, at produkter med digitale elementer ledsages af oplysningerne og anvisningerne i bilag II i elektronisk eller fysisk form. Sådanne oplysninger og anvisninger affattes på et for brugerne letforståeligt sprog. De skal være klare, forståelige og letlæselige. De skal muliggøre sikker installation, drift og anvendelse af produkter med digitale elementer.

11. Fabrikanten udleverer enten EU-overensstemmelseserklæringen sammen med produktet med digitale elementer eller angiver den internetadresse, hvor der er adgang til EU-overensstemmelseserklæringen, i brugsanvisningerne og oplysningerne i bilag II.

12. Når et produkt med digitale elementer er bragt i omsætning, træffer fabrikanten i produktets forventede levetid eller i en periode på fem år efter, at produktet er bragt i omsætning, alt efter hvilken periode der er kortest, hvis fabrikanten 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 krav i bilag I, straks de nødvendige korrigerende foranstaltninger til at bringe produktet med digitale elementer eller fabrikantens processer i overensstemmelse eller til at tilbagetrække eller tilbagekalde produktet, alt efter hvad der er relevant.

13. 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 krav 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.

14. En fabrikant, der indstiller driften og derfor ikke er i stand til at opfylde de forpligtelser, der er fastsat i 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 pågældende produkter med digitale elementer, der er bragt i omsætning.

15. Kommissionen kan ved hjælp af gennemførelsesretsakter præcisere formatet for og elementerne i den softwarekomponentliste, der er fastsat i bilag I, punkt 2, nr. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 51, stk. 2.

Artikel 11

Fabrikantens rapporteringsforpligtelser

1. Fabrikanten underretter uden unødig forsinkelse og under alle omstændigheder senest 24 timer efter at have fået kendskab hertil ENISA om enhver aktivt udnyttet sårbarhed i produktet med digitale elementer. Underretningen skal indeholde nærmere oplysninger om denne sårbarhed og, hvis det er relevant, eventuelle korrigerende eller afbødende foranstaltninger, der er truffet. ENISA videresender uden unødig forsinkelse, medmindre der foreligger begrundede årsager vedrørende cybersikkerhedsrisici, underretningen til den CSIRT, der er udpeget med henblik på koordineret offentliggørelse af sårbarheder i overensstemmelse med artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)] i de berørte medlemsstater, efter modtagelsen og underretter markedsovervågningsmyndigheden om den anmeldte sårbarhed.

2. Fabrikanten underretter uden unødig forsinkelse og under alle omstændigheder senest 24 timer efter at have fået kendskab hertil ENISA om enhver hændelse, der indvirker på sikkerheden af produktet med digitale elementer. ENISA videresender uden unødig forsinkelse, medmindre der foreligger begrundede årsager vedrørende cybersikkerhedsrisici, underretningerne til det centrale kontaktpunkt, der er udpeget i overensstemmelse med artikel [artikel X] i de berørte medlemsstaters direktiv [direktiv XXX/XXXX (NIS2)], og underretter markedsovervågningsmyndigheden om de anmeldte hændelser. Underretningen om hændelsen skal indeholde oplysninger om hændelsens alvor og konsekvenser og, hvor det er relevant, angives det, om fabrikanten har mistanke om, at hændelsen skyldes ulovlige eller ondsindede handlinger, eller om fabrikanten mener, at den har en grænseoverskridende virkning.

3. ENISA forelægger det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe), der er oprettet ved artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)], oplysninger, der er meddelt i henhold til stk. 1 og 2, hvis sådanne oplysninger er relevante for den koordinerede forvaltning af væsentlige cybersikkerhedshændelser og -kriser på operationelt plan.

4. Fabrikanten underretter uden unødig forsinkelse og efter at være blevet bekendt hermed brugerne af produktet med digitale elementer om hændelsen og om nødvendigt om korrigerende foranstaltninger, som brugeren kan træffe for at afbøde virkningen af hændelsen.

5. Kommissionen kan ved hjælp af gennemførelsesretsakter yderligere præcisere typen af oplysninger, formatet og proceduren for underretninger indgivet i henhold til stk. 1 og 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 51, stk. 2.

6. ENISA udarbejder på grundlag af de underretninger, der er modtaget i henhold til stk. 1 og 2, hvert andet år en teknisk rapport om nye tendenser med hensyn til cybersikkerhedsrisici forbundet med produkter med digitale elementer og forelægger den for den samarbejdsgruppe, der er omhandlet i artikel [artikel X] i direktiv [direktiv XXX/XXXX (NIS2)]. Den første rapport forelægges senest 24 måneder efter, at forpligtelserne i stk. 1 og 2 begynder at finde anvendelse.

7. 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 vedligeholder komponenten.

Artikel 12

Bemyndigede repræsentanter

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

2. Forpligtelserne i artikel 10, stk. 1-7, første led, og artikel 10, stk. 9, er ikke en del af den bemyndigede repræsentants fuldmagt.

3. En bemyndiget repræsentant udfører de opgaver, der er fastsat i den fuldmagt, denne har modtaget fra fabrikanten. Fuldmagten skal som minimum sætte den bemyndigede repræsentant i stand til:

   (a) at opbevare den i artikel 20 omhandlede EU-overensstemmelseserklæring og den i artikel 23 omhandlede tekniske dokumentation, så den i ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, 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 overholder lovgivningen

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

Artikel 13

Importørens forpligtelser

1. Importøren må kun bringe produkter med digitale elementer, der opfylder de væsentlige krav i bilag I, afsnit 1, i omsætning, og hvor de processer, der er indført af fabrikanten, er i overensstemmelse med de væsentlige krav i bilag I, punkt 2.

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

   (a) at fabrikanten har gennemført de i artikel 24 omhandlede relevante overensstemmelsesvurderingsprocedurer

   (b) at fabrikanten har udarbejdet den tekniske dokumentation

(c) at produktet med digitale elementer er forsynet med CE-mærkning, jf. artikel 22, og er ledsaget af oplysninger og brugsanvisninger, jf. bilag II.

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 de væsentlige krav i bilag I, må importøren ikke bringe produktet i omsætning, før produktet eller de processer, som fabrikanten har indført, er blevet bragt i overensstemmelse med de væsentlige krav i bilag I. Hvis produktet med digitale elementer udgør en væsentlig cybersikkerhedsrisiko, underretter importøren endvidere fabrikanten og markedsovervågningsmyndighederne herom.

4. Importørens navn, registrerede firmanavn eller registrerede varemærke, postadresse og e-mailadresse skal fremgå af produktet med digitale elementer, eller hvis dette ikke er muligt, af emballagen eller af et dokument, der ledsager produktet med digitale elementer. Kontaktoplysningerne angives på et for brugere og markedsovervågningsmyndigheder letforståeligt sprog.

5. Importøren sikrer, at produktet med digitale elementer ledsages af anvisninger og oplysninger, jf. bilag II, på et for slutbrugerne letforståeligt sprog.

6. Hvis importøren ved eller har grund til at tro, at et produkt med digitale elementer, som importøren har bragt i omsætning, eller de processer, der er indført af fabrikanten, ikke er i overensstemmelse med de væsentlige krav i bilag I, træffer importøren straks de nødvendige korrigerende foranstaltninger til at bringe produktet med digitale elementer eller de processer, som fabrikanten har indført, i overensstemmelse med de væsentlige krav i bilag I eller til at tilbagetrække eller tilbagekalde produktet, hvis det er relevant.

   Hvis importøren har identificeret en sårbarhed i produktet med digitale elementer, underretter importøren uden unødig forsinkelse fabrikanten om denne sårbarhed. Hvis produktet med digitale elementer udgør en væsentlig cybersikkerhedsrisiko, underretter importøren endvidere straks markedsovervågningsmyndighederne i de medlemsstater, hvor importøren har gjort produktet med digitale elementer tilgængeligt på markedet, herom og giver nærmere oplysninger, navnlig om den manglende overensstemmelse med lovgivningen og de trufne afhjælpende foranstaltninger.

7. Importøren opbevarer i ti år efter, at produktet med digitale elementer er blevet bragt i omsætning, 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.

8. 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 krav i bilag I, punkt 1, og at de processer, der er indført af fabrikanten, er i overensstemmelse med de væsentlige krav i bilag I, punkt 2, 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.

9. Når 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 14

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 10, stk. 10 og 11, og artikel 13, stk. 4.

3. Hvis en distributør 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 krav 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. Hvis produktet med digitale elementer udgør en væsentlig cybersikkerhedsrisiko, underretter distributøren endvidere markedsovervågningsmyndighederne herom.

4. Hvis distributøren 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 de væsentlige krav i bilag I, træffer distributøren straks 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 har identificeret en sårbarhed i produktet med digitale elementer, underretter distributøren uden unødig forsinkelse fabrikanten om denne sårbarhed. Hvis produktet med digitale elementer udgør en væsentlig cybersikkerhedsrisiko, underretter distributøren endvidere straks markedsovervågningsmyndighederne i de medlemsstater, hvor distributøren har gjort produktet med digitale elementer tilgængeligt på markedet, herom og giver nærmere oplysninger, navnlig om den manglende overensstemmelse med lovgivningen 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 de væsentlige krav i bilag I, 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 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 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 15

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 underlagt de samme forpligtelser som fabrikanten, jf. artikel 10 og artikel 11, stk. 1, 2, 4 og 7, når 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 16

Andre tilfælde, hvor fabrikantens forpligtelser finder anvendelse

En fysisk eller juridisk person, bortset fra fabrikanten, importøren eller distributøren, som foretager en væsentlig ændring af produktet med digitale elementer, anses for at være fabrikant i denne forordnings forstand.

Denne person er underlagt fabrikantens forpligtelser som fastsat i artikel 10 og artikel 11, stk. 1, 2, 4 og 7, for den del af produktet, 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 17

Identifikation af erhvervsdrivende

1. Erhvervsdrivende giver efter anmodning, og hvis oplysningerne er tilgængelige, markedsovervågningsmyndighederne følgende oplysninger:

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

   (b) 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.

KAPITEL III

OVERENSSTEMMELSEN AF PRODUKTER MED DIGITALE ELEMENTER

Artikel 18

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 krav, der er omfattet af disse standarder eller dele deraf, jf. bilag I.

2. Produkter med digitale elementer og processer indført af fabrikanten, som er i overensstemmelse med de fælles specifikationer, der er omhandlet i artikel 19, formodes at være i overensstemmelse med de væsentlige krav, der er fastsat i bilag I, for så vidt de nævnte fælles specifikationer omfatter disse krav.

3. 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 henhold til forordning (EU) 2019/881, og som er præciseret i stk. 4, formodes at være i overensstemmelse med de væsentlige krav i bilag I, såfremt EU-overensstemmelseserklæringen eller cybersikkerhedsattesten eller dele heraf dækker disse krav.

4. Kommissionen tillægges beføjelser til ved hjælp af gennemførelsesretsakter at præcisere de europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til forordning (EU) 2019/881, som kan anvendes til at påvise overensstemmelse med de væsentlige krav eller dele deraf som fastsat i bilag I. Kommissionen præciserer desuden, hvor det er relevant, om en cybersikkerhedsattest udstedt i henhold til sådanne ordninger fritager fabrikanten fra forpligtelsen til at lade foretage en overensstemmelsesvurdering af tredjepart vedrørende de tilsvarende krav, jf. artikel 24, stk. 2, litra a), b), og artikel 24, stk. 3, litra a) og b). Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 51, stk. 2.

Artikel 19

Fælles specifikationer

I tilfælde, hvor der ikke findes harmoniserede standarder som omhandlet i artikel 18, eller hvis Kommissionen ikke finder, at de relevante harmoniserede standarder er tilstrækkelige til at opfylde kravene i denne forordning eller Kommissionens standardiseringsanmodning, eller hvis der er unødige forsinkelser i standardiseringsproceduren, eller hvis Kommissionens anmodning om harmoniserede standarder ikke er blevet imødekommet af nogen af de europæiske standardiseringsorganisationer, tillægges Kommissionen beføjelser til ved hjælp af gennemførelsesretsakter at vedtage fælles specifikationer for så vidt angår de væsentlige krav i bilag I. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 51, stk. 2.

Artikel 20

EU-overensstemmelseserklæring

1. EU-overensstemmelseserklæringen skal udfærdiges af fabrikanten i overensstemmelse med artikel 10, stk. 7, og det skal af EU-overensstemmelseserklæringen fremgå, at det er blevet dokumenteret, at de gældende væsentlige krav i bilag I er opfyldt.

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

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 står fabrikanten inde for, at produktet opfylder de gældende krav.

5. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 50 med henblik på at supplere denne forordning ved at tilføje elementer til minimumsindholdet af EU-overensstemmelseserklæringen, jf. bilag IV, for at tage hensyn til den teknologiske udvikling.

Artikel 21

Generelle principper for CE-mærkningen

CE-mærkningen som defineret i artikel 3, nr. 32), er underkastet de generelle principper i artikel 30 i forordning (EF) nr. 765/2008.

Artikel 22

Regler og betingelser for anbringelse af CE-mærkning

1. CE-mærkningen anbringes på produktet med digitale elementer, så den er synlig, let læselig og ikke kan slettes. Hvis produktet med digitale elementer er af en sådan art, at dette ikke er muligt eller berettiget, anbringes den på emballagen og på EU-overensstemmelseserklæringen omhandlet i artikel 20, der ledsager produktet med digitale elementer. For produkter med digitale elementer i form af software anbringes CE-mærkningen enten på den i artikel 20 omhandlede EU-overensstemmelseserklæring eller på webstedet for softwareproduktet.

2. CE-mærkning på produktet med digitale elementer kan, hvis arten af produktet med digitale elementer nødvendiggør det, være lavere end 5 mm, forudsat at den 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 risiko- eller brugskategori som fastsat i de gennemførelsesretsakter, der er omhandlet i stk. 6.

4. Efter CE-mærkningen anføres identifikationsnummeret på det bemyndigede organ, hvis dette organ deltager i overensstemmelsesvurderingsproceduren på grundlag af fuld kvalitetssikring (baseret på modul H), jf. artikel 24.

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

5. Medlemsstaterne benytter sig af eksisterende mekanismer til sikring af, 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-lovgivning, som også indeholder bestemmelser om anbringelse af CE-mærkning, skal CE-mærkningen angive, at produktet ligeledes opfylder kravene i denne anden lovgivning.

6. Kommissionen kan ved hjælp af gennemførelsesretsakter fastsætte tekniske specifikationer for piktogrammer eller andre mærker vedrørende sikkerheden af

produkter med digitale elementer og mekanismer til at fremme af deres anvendelse. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 51, stk. 2.

Artikel 23

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 krav i bilag I. Den skal som minimum indeholde de i bilag V fastsatte elementer.

2. Den tekniske dokumentation udarbejdes, inden produktet med digitale elementer bringes i omsætning, og ajourføres løbende, hvis det er relevant, i løbet af produktets forventede levetid eller i en periode på fem år efter, at produktet er bragt i omsætning, alt efter hvilken periode der er kortest.

3. For produkter med digitale elementer som omhandlet i artikel 8 og artikel 24, stk. 4, der også er omfattet af andre EU-retsakter, udarbejdes der en samlet teknisk dokumentation, som indeholder de oplysninger, der er omhandlet i bilag V til denne forordning, og de oplysninger, der kræves i henhold til disse respektive 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 50 med henblik på at supplere denne forordning med de elementer, der skal indgå i den tekniske dokumentation, jf. bilag V, for at tage hensyn til den teknologiske udvikling samt udviklingen i forbindelse med gennemførelsen af denne forordning.

Artikel 24

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 krav i bilag I er opfyldt. Fabrikanten eller dennes bemyndigede repræsentant påviser overensstemmelse med de væsentlige krav ved brug af en af følgende procedurer:

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

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

   (c) overensstemmelsesvurdering grundlag af fuld kvalitetssikring (baseret på modul H) som fastsat i bilag VI.

2. Hvis fabrikanten eller dennes bemyndigede repræsentant ved vurderingen af overensstemmelsen af det kritiske produkt med digitale elementer i klasse I, jf. bilag III, og de processer, der er indført af fabrikanten, ikke har anvendt eller kun delvist har anvendt harmoniserede standarder, fælles specifikationer eller europæiske

cybersikkerhedscertificeringsordninger som omhandlet i artikel 18, 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 krav en af følgende procedurer:

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

(b) overensstemmelsesvurdering grundlag af fuld kvalitetssikring (baseret på modul H) som fastsat i bilag VI.

3. Hvis produktet er et kritisk produkt med digitale elementer i klasse II, jf. bilag III, påviser fabrikanten eller dennes bemyndigede repræsentant overensstemmelse med de væsentlige krav i bilag I ved brug af en af følgende procedurer:

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

(b) overensstemmelsesvurdering grundlag af fuld kvalitetssikring (baseret på modul H) som fastsat i bilag VI.

4. Fabrikanter af produkter med digitale elementer, der er klassificeret som EPJ-systemer omfattet af anvendelsesområdet for forordning [forordningen om det europæiske sundhedsdataområde], påviser overensstemmelse med de væsentlige krav i bilag I til denne forordning ved brug af den relevante overensstemmelsesvurderingsprocedure som omhandlet i forordning [kapitel III i forordningen om det europæiske sundhedsdataområde].

5. Bemyndigede organer tager hensyn til små og mellemstore virksomheders særlige interesser og behov, når de fastsætter gebyrerne for overensstemmelsesvurdering, og reducerer disse gebyrer i forhold til deres særlige interesser og behov.

KAPITEL IV

NOTIFIKATION AF OVERENSSTEMMELSESVURDERINGSORGANER

Artikel 25

Notifikation

Medlemsstaterne underretter Kommissionen og de øvrige medlemsstater om, hvilke overensstemmelsesvurderingsorganer der er bemyndiget til at udføre overensstemmelsesvurderingsopgaver i henhold til denne forordning.

Artikel 26

Bemyndigende myndigheder

1. Medlemsstaterne udpeger en bemyndigende myndighed, som er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering og notifikation af overensstemmelsesvurderingsorganer og overvågningen af bemyndigede organer, herunder overholdelse af artikel 31.

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

Artikel 27

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 notifikation af et overensstemmelsesvurderingsorgan 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 28

Oplysningskrav for bemyndigende myndigheder

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

2. Kommissionen offentliggør disse oplysninger.

Artikel 29

Krav til bemyndigede organer

1. I forbindelse med notifikation skal et overensstemmelsesvurderingsorgan opfylde kravene i stk. 2-12.

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

3. Et overensstemmelsesvurderingsorgan skal være et tredjepartsorgan, der er uafhængigt af den organisation eller det produkt, 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 organ.

4. Overensstemmelsesvurderingsorganet, dets øverste ledelse og det personale, der er ansvarligt for at foretage overensstemmelsesvurdering, må ikke være designer, udvikler, fabrikant, leverandør, montør, køber, ejer, bruger eller reparatør af det produkt med digitale elementer, der vurderes, 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, markedsføring, montering, anvendelse eller vedligeholdelse af disse produkter eller repræsentere parter, der er involveret i disse aktiviteter. Organet må ikke deltage i aktiviteter, som kan være i strid med dets objektivitet og integritet i forbindelse med de overensstemmelsesvurderingsopgaver, organet er notificeret til at udføre. Dette gælder navnlig rådgivningstjenester.

   Overensstemmelsesvurderingsorganet skal sikre, at dets dattervirksomheders eller underentreprenørers aktiviteter ikke påvirker fortroligheden, objektiviteten og uvildigheden af dets overensstemmelsesvurderingsaktiviteter.

5. Overensstemmelsesvurderingsorganet og dets 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 og 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 kunne gennemføre alle de overensstemmelsesvurderingsopgaver, der er nævnt i bilag VI, og for hvilke det er blevet notificeret, uanset om disse opgaver udføres af overensstemmelsesvurderingsorganet selv eller på dets vegne og på dets ansvar.

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

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

   (b) beskrivelser af de procedurer, i henhold til hvilke overensstemmelsesvurderingen 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 virksomhedernes størrelse, den sektor, som organet opererer i, strukturen, den pågældende produktteknologis kompleksitet og produktionsprocessens karakter af masse- eller serieproduktion.

   Det 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 notifikation dækker

   (b) tilstrækkeligt kendskab til kravene vedrørende de vurderinger, de foretager, og den nødvendige bemyndigelse til at udføre sådanne vurderinger

   (c) et tilstrækkeligt kendskab til og en tilstrækkelig forståelse af de væsentlige krav, de gældende harmoniserede standarder og de relevante bestemmelser i EU-harmoniseringslovgivning og gennemførelsesretsakter

   (d) færdighed i at udarbejde attester, redegørelser 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 hvordan vurderingerne falder ud.

9. Overensstemmelsesvurderingsorganet skal tegne en ansvarsforsikring, medmindre staten 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 VI 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 40, 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 og rimelige vilkår og betingelser, særlig under hensyntagen til SMV'ernes interesser for så vidt angår gebyrer.

Artikel 30

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 29, for så vidt som de gældende harmoniserede standarder dækker disse krav.

Artikel 31

Dattervirksomheder og underentreprise i tilknytning til bemyndigede organer

1. Hvis et bemyndiget organ giver bestemte opgaver i forbindelse med overensstemmelsesvurderingen i underentreprise eller anvender en dattervirksomhed,

skal det sikre, at underentreprenøren eller dattervirksomheden opfylder kravene i artikel 29, og underretter den bemyndigende myndighed herom.

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

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

4. De bemyndigede organer skal kunne stille de relevante dokumenter vedrørende vurderingen af underentreprenørens eller dattervirksomhedens kvalifikationer og det arbejde, som de har udført i henhold til denne forordning, til rådighed for den bemyndigende myndighed.

Artikel 32

Ansøgning om notifikation

1. Et overensstemmelsesvurderingsorgan skal indgive en ansøgning om notifikation 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, som organet hævder at være kompetent til, samt af et eventuelt akkrediteringscertifikat udstedt af et nationalt akkrediteringsorgan, hvor det attesteres, at overensstemmelsesvurderingsorganet opfylder kravene i artikel 29.

3. Hvis det pågældende overensstemmelsesvurderingsorgan ikke kan forelægge et akkrediteringscertifikat, forelægger det den bemyndigede myndighed den dokumentation, der er nødvendig for at kontrollere, anerkende og regelmæssigt overvåge, at det opfylder kravene i artikel 29.

Artikel 33

Notifikationsprocedure

1. De bemyndigende myndigheder må kun notificere overensstemmelsesvurderingsorganer, som opfylder kravene i artikel 29.

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

3. Notifikationen skal indeholde fyldestgørende oplysninger om overensstemmelsesvurderingsaktiviteterne, det eller de pågældende overensstemmelsesvurderingsmoduler og det eller de pågældende produkter og den relevante dokumentation for kompetencen.

4. Hvis en notifikation ikke er baseret på et akkrediteringscertifikat som anført i artikel 32, stk. 2, skal den bemyndigende myndighed forelægge Kommissionen og de øvrige medlemsstater den dokumentation, der attesterer overensstemmelsesvurderingsorganets kompetence, og oplysninger om 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 29 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 notifikation baseret på et akkrediteringscertifikat eller inden for to måneder efter en notifikation, 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 underrettes om enhver relevant efterfølgende ændring af notifikationen.

Artikel 34

Identifikationsnumre for og lister over bemyndigede organer

1. Kommissionen tildeler bemyndigede organer 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 35

Ændringer af notifikationer

1. Hvis en bemyndigende myndighed har konstateret eller er blevet underrettet om, at et bemyndiget organ ikke længere opfylder kravene i artikel 29, eller at det ikke opfylder sine forpligtelser, begrænser, suspenderer eller inddrager den bemyndigende myndighed notifikationen, alt efter hvad der er mest hensigtsmæssigt, og afhængigt af i hvor høj grad kravene eller forpligtelserne ikke er blevet opfyldt. Den underretter straks Kommissionen og de øvrige medlemsstater herom.

2. Hvis en notifikation 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 står til rådighed for de ansvarlige bemyndigende myndigheder og markedsovervågningsmyndigheder efter disses anmodning.

Artikel 36

Anfægtelse af bemyndigede organers kompetence

1. Kommissionen undersøger alle sager, 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 notifikationen eller fastholdelsen af det bemyndigede organs kompetence.

3. Kommissionen sikrer, at alle følsomme oplysninger, som 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 notifikation, underretter Kommissionen den bemyndigende medlemsstat herom og anmoder den om at træffe de nødvendige korrigerende foranstaltninger, herunder om nødvendigt inddragelse af notifikationen.

Artikel 37

Bemyndigede organers proceduremæssige forpligtelser

1. Bemyndigede organer foretager overensstemmelsesvurdering i overensstemmelse med de overensstemmelsesvurderingsprocedurer, der er fastsat i artikel 24 og bilag VI.

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, den sektor, som de opererer inden for, deres struktur, den pågældende produktteknologis kompleksitet og produktionsprocessens karakter af masse- eller serieproduktion.

3. I denne forbindelse respekterer de dog den grad af strenghed og det beskyttelsesniveau, der kræves for, at produktet opfylder kravene i denne forordning.

4. Hvis et bemyndiget organ finder, at fabrikanten ikke har opfyldt de krav, der er fastsat i bilag I eller i de dertil svarende harmoniserede standarder eller i de fælles specifikationer som omhandlet i artikel 19, skal det anmode fabrikanten om at træffe afhjælpende foranstaltninger, og det udsteder ikke en overensstemmelsesattest.

5. Hvis et bemyndiget organ i forbindelse med overensstemmelsesovervågning, efter at der er udstedt en attest, finder, at et produkt ikke længere opfylder kravene i denne forordning, anmoder det fabrikanten om at afhjælpe dette og suspenderer eller inddrager om nødvendigt attesten.

6. Hvis der ikke træffes afhjælpende foranstaltninger, eller hvis disse ikke har den ønskede virkning, skal det bemyndigede organ begrænse, suspendere eller inddrage eventuelle attester, alt efter hvad der er mest hensigtsmæssigt.

Artikel 38

Oplysningskrav til bemyndigede organer

1. De bemyndigede organer skal oplyse 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 notifikationen

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

   (d) efter anmodning, overensstemmelsesvurderingsaktiviteter, der er udført på det område, som deres notifikation gælder for, og enhver anden udført aktivitet, herunder grænseoverskridende aktiviteter og underentreprise.

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

Artikel 39

Erfaringsudveksling

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

Artikel 40

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 41

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

1. Forordning (EU) 2019/1020 finder anvendelse på produkter med digitale elementer inden for denne 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 fungere som markedsovervågningsmyndighed i henhold til denne forordning.
3. 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. Med hensyn til tilsynet med gennemførelsen af rapporteringsforpligtelserne i henhold til artikel 11 i denne forordning samarbejder de udpegede markedsovervågningsmyndigheder med ENISA.
4. Markedsovervågningsmyndighederne samarbejder, hvor det er relevant, med andre markedsovervågningsmyndigheder, der er udpeget på grundlag af anden EU-harmoniseringslovgivning for andre produkter, og udveksler regelmæssigt oplysninger.
5. Markedsovervågningsmyndighederne samarbejder, hvor det er relevant, med de myndigheder, der fører tilsyn med EU's databeskyttelseslovgivning. Et sådant samarbejde omfatter underretning af disse myndigheder om ethvert resultat, der er relevant for udøvelsen af deres beføjelser, herunder i forbindelse med vejledning og

rådgivning i henhold til denne artikels stk. 8, hvis sådan vejledning og rådgivning vedrører behandling af personoplysninger.

De myndigheder, der fører tilsyn med EU's databeskyttelseslovgivning, 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.

6. Medlemsstaterne sikrer, at de udpegede markedsovervågningsmyndigheder modtager tilstrækkelige finansielle og menneskelige ressourcer til at udføre deres opgaver i henhold til denne forordning.

7. Kommissionen letter udvekslingen af erfaringer mellem de udpegede markedsovervågningsmyndigheder.

8. Markedsovervågningsmyndighederne kan yde vejledning og rådgivning til erhvervsdrivende om gennemførelsen af denne forordning med støtte fra Kommissionen.

9. 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's konkurrenceregler, til Kommissionen og de relevante nationale konkurrencemyndigheder.

10. For produkter med digitale elementer inden for denne forordnings anvendelsesområde, der er klassificeret som højrisiko-AI-systemer i henhold til artikel [artikel 6] i forordning [AI-forordningen], er de markedsovervågningsmyndigheder, der er udpeget med henblik på forordning [AI-forordningen], de myndigheder, der er ansvarlige for de markedsovervågningsaktiviteter, der skal udføres i henhold til denne forordning. De markedsovervågningsmyndigheder, der er udpeget i henhold til forordning [AI-forordningen], samarbejder, hvor det er relevant, med de markedsovervågningsmyndigheder, der er udpeget i henhold til nærværende forordning, og med ENISA om tilsynet med gennemførelsen af rapporteringsforpligtelserne i henhold til artikel 11. Markedsovervågningsmyndigheder udpeget i henhold til forordning [AI-forordningen] 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 denne forordning.

11. Der oprettes en særlig administrativ samarbejdsgruppe (ADCO) med henblik på ensartet gennemførelse af denne forordning i henhold til artikel 30, stk. 2, i forordning (EU) 2019/1020. Denne ADCO skal bestå af repræsentanter fra de udpegede markedsovervågningsmyndigheder og, hvis det er relevant, repræsentanter fra centrale forbindelseskontorer.

Artikel 42

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 krav i bilag I, tildeles markedsovervågningsmyndighederne efter begrundet anmodning adgang til de data, der er nødvendige for at vurdere designet, udviklingen, produktionen og sårbarhedshåndteringen af sådanne produkter, herunder den relevante interne dokumentation fra den pågældende erhvervsdrivende.

Artikel 43

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 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 foranstaltninger for at bringe produktet i overensstemmelse med disse krav, trække produktet tilbage fra markedet eller tilbagekalde det inden for en rimelig tidsfrist, som den fastsætter i forhold til risikoens art.

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

2. Hvis markedsovervågningsmyndigheden finder, at den manglende overensstemmelse ikke er begrænset til den pågældende medlemsstats område, underretter de Kommissionen og de øvrige medlemsstater om resultaterne af evalueringen og om de foranstaltninger, som de har pålagt den erhvervsdrivende at træffe.

3. Fabrikanten sikrer, at der træffes de fornødne afhjælpende foranstaltninger over for alle de pågældende produkter med digitale elementer, som fabrikanten har gjort tilgængelige på EU-markedet.

4. Hvis fabrikanten af et produkt med digitale elementer ikke træffer de fornødne afhjælpende foranstaltninger 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 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 sådanne foranstaltninger.

5. De i stk. 4 omhandlede oplysninger skal indeholde alle tilgængelige oplysninger, navnlig hvad angår de nødvendige data til identifikation af de produkter 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 eller de processer, som fabrikanten har indført, ikke opfylder de væsentlige krav i bilag I

(b) at der er mangler ved de harmoniserede standarder, cybersikkerhedscertificeringsordninger eller fælles specifikationer omhandlet i artikel 18.

6. De øvrige medlemsstater ud over den medlemsstat, der har indledt proceduren, underretter straks Kommissionen og de øvrige medlemsstater om de trufne foranstaltninger og om yderligere oplysninger, som de måtte råde over, om det pågældende produkts manglende overensstemmelse med kravene, og om deres indsigelser, hvis de ikke er indforstået med den meddelte nationale foranstaltning.

7. Hvis der ikke inden for tre måneder efter modtagelsen af de i stk. 4 omhandlede oplysninger 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 pågældende erhvervsdrivendes procedurerettigheder i henhold til artikel 18 i forordning (EU) 2019/1020.

8. Markedsovervågningsmyndighederne i alle medlemsstaterne sikrer, at der straks træffes de fornødne restriktive foranstaltninger med hensyn til det pågældende produkt, f.eks. tilbagetrækning af produktet fra deres marked.

Artikel 44

Beskyttelsesprocedure på EU-plan

1. Hvis en medlemsstat inden for tre måneder efter modtagelsen af den i artikel 43, stk. 4, omhandlede underretning gør indsigelse mod en medlemsstats foranstaltning, eller hvis 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 vurderer den nationale foranstaltning. På grundlag af resultaterne af denne vurdering træffer Kommissionen senest ni måneder efter den i artikel 43, stk. 4, 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 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 anses for at være uberettiget, trækker den pågældende medlemsstat foranstaltningen tilbage.

3. Hvis 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 10 i forordning (EU) nr. 1025/2012.

4. Hvis 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 18, tager Kommissionen stilling til, om den i artikel 18, stk. 4, omhandlede

gennemførelsesretsakt, der fastsætter formodningen om overensstemmelse for den pågældende certificeringsordning, skal ændres eller ophæves.

5. Hvis 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 19, tager Kommissionen stilling til, om den i artikel 19 omhandlede gennemførelsesretsakt, der fastsætter disse fælles specifikationer, skal ændres eller ophæves.

Artikel 45

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

1. Hvis 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, kan den anmode de relevante markedsovervågningsmyndigheder om at foretage en evaluering af overensstemmelsen og følge de procedurer, der er omhandlet i artikel 43.

2. Under ekstraordinære 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 fortsat ikke opfylder kravene i denne forordning, og de relevante markedsovervågningsmyndigheder ikke har truffet effektive foranstaltninger, kan Kommissionen anmode ENISA om at foretage en evaluering af overensstemmelsen. Kommissionen underretter de relevante markedsovervågningsmyndigheder herom. De relevante erhvervsdrivende samarbejder i nødvendigt omfang med ENISA.

3. På grundlag af ENISA's evaluering 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.

4. På grundlag af den i stk. 3 omhandlede høring kan Kommissionen vedtage gennemførelsesretsakter med henblik på at træffe afgørelse om korrigerende eller restriktive foranstaltninger på EU-plan, herunder påbud om at trække produktet tilbage fra markedet eller tilbagekalde det inden for en rimelig tidsfrist, som den fastsætter i forhold til risikoens art. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 51, stk. 2.

5. Kommissionen meddeler omgående den i stk. 4 omhandlede afgørelse til den eller de relevante erhvervsdrivende. Medlemsstaterne gennemfører straks de i stk. 4 omhandlede retsakter og underretter Kommissionen herom.

6. Stk. 2-5 finder anvendelse, indtil den ekstraordinære situation, der begrundede Kommissionens indgreb, ikke længere er til stede, og indtil det pågældende produkt er bragt i overensstemmelse med denne forordning.

Artikel 46

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

1. Hvis en medlemsstats markedsovervågningsmyndighed efter at have foretaget en evaluering i henhold til artikel 43 finder, at et produkt med digitale elementer og de processer, som fabrikanten har indført, selv om de opfylder kravene i denne

forordning, udgør en væsentlig cybersikkerhedsrisiko og desuden udgør 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 af den type, der er omhandlet i [bilag I til direktiv XXX/XXXX (NIS2)], eller for andre samfundsinteresser, pålægger medlemsstaten den relevante erhvervsdrivende at træffe alle nødvendige foranstaltninger for at sikre, at produktet med digitale elementer og de processer, som den pågældende fabrikant har indført, når produktet bringes i omsætning, ikke længere udgør en risiko, eller for at trække produktet med digitale elementer tilbage fra markedet eller kalde det tilbage inden for en rimelig tidsfrist, som den fastsætter i forhold til risikoens art.

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 markedsovervågningsmyndighed, jf. stk. 1.

3. Den pågældende medlemsstat underretter straks Kommissionen og de øvrige medlemsstater om de foranstaltninger, der er truffet i henhold til stk. 1. Denne underretning skal omfatte alle tilgængelige oplysninger, særlig hvad angår de nødvendige data 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 pågældende erhvervsdrivende og vurderer de trufne nationale foranstaltninger. På grundlag af resultaterne af denne vurdering træffer Kommissionen afgørelse om, hvorvidt foranstaltningen er berettiget eller ej, og foreslår om nødvendigt passende foranstaltninger.

5. Kommissionen retter sin afgørelse til medlemsstaterne.

6. Hvis Kommissionen har tilstrækkelig grund til at antage, herunder på grundlag af oplysninger fra ENISA, at et produkt med digitale elementer, selv om det opfylder kravene i denne forordning, udgør de i stk. 1 omhandlede risici, kan den anmode den eller de relevante markedsovervågningsmyndigheder om at foretage en evaluering af overensstemmelsen og følge de procedurer, der er omhandlet i artikel 43 og i stk. 1, 2 og 3 i denne artikel.

7. Under ekstraordinære 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 fortsat udgør de i stk. 1 omhandlede risici, og de relevante nationale markedsovervågningsmyndigheder ikke har truffet effektive foranstaltninger, kan Kommissionen anmode ENISA om at foretage en evaluering af risiciene forbundet med det pågældende produkt, og Kommissionen underretter de relevante markedsovervågningsmyndigheder herom. De relevante erhvervsdrivende samarbejder i nødvendigt omfang med ENISA.

8. På grundlag af ENISA's evaluering, jf. 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 stk. 8 omhandlede høring kan Kommissionen vedtage gennemførelsesretsakter med henblik på at træffe afgørelse om korrigerende eller

restriktive foranstaltninger på EU-plan, herunder påbud om at trække produktet tilbage fra markedet eller tilbagekalde det inden for en rimelig tidsfrist, som den fastsætter i forhold til risikoens art. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 51, stk. 2.

10. Kommissionen meddeler omgående den i stk. 9 omhandlede afgørelse til den eller de relevante erhvervsdrivende. Medlemsstaterne gennemfører sådanne retsakter 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 fortsat udgør de i stk. 1 omhandlede risici.

Artikel 47

Formel manglende overensstemmelse

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

   (a) overensstemmelsesmærkningen er anbragt i strid med artikel 21 22

   (b) overensstemmelsesmærkningen 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 manglende overensstemmelse som omhandlet i stk. 1 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 48

Markedsovervågningsmyndighedernes fælles aktiviteter

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

2. Kommissionen eller ENISA kan foreslå 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, der er omfattet af denne forordning, muligvis ikke overholdes i flere medlemsstater.

3. Markedsovervågningsmyndigheden og Kommissionen, hvis det er relevant, 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, som stammer fra de aktiviteter, der gennemføres som led i en undersøgelse, som den iværksætter.

5. Den pågældende markedsovervågningsmyndighed og Kommissionen, hvis det er relevant, gør aftalen om fælles aktiviteter, herunder de involverede parters navne, tilgængelig for offentligheden.

Artikel 49

Kontrolaktioner

1. Markedsovervågningsmyndighederne kan beslutte at gennemføre samtidige, koordinerede kontrolaktioner af bestemte produkter med digitale elementer eller kategorier heraf for at kontrollere overensstemmelse med eller afsløre overtrædelser af denne forordning.

2. Medmindre andet aftales af de involverede markedsovervågningsmyndigheder, koordinerer Kommissionen kontrolaktionerne. Kontrolaktionens koordinator kan efter omstændighederne gøre de samlede resultater offentligt tilgængelige.

3. ENISA kan i forbindelse med udførelsen af sine opgaver, herunder på grundlag af underretningerne modtaget i henhold til artikel 11, stk. 1 og 2, identificere de produktkategorier, for hvilke der kan tilrettelægges kontrolaktioner. Forslaget om kontrolaktioner indgives til den potentielle koordinator, der er omhandlet i stk. 2, med henblik på markedstilsynsmyndighedernes vurdering.

4. Ved gennemførelsen af kontrolaktioner kan de involverede kontrolovervågningsmyndigheder gøre brug af undersøgelsesbeføjelserne i artikel 41-47 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 50

Udøvelse af 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. 4, artikel 6, stk. 2, artikel 6, stk. 3, artikel 6, stk. 5, artikel 20, stk. 5, og artikel 23, stk. 5, tillægges Kommissionen.

3. Den i artikel 2, stk. 4, artikel 6, stk. 2, artikel 6, stk. 3, artikel 6, stk. 5, artikel 20, stk. 5, og artikel 23, 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 vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016.

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. 4, artikel 6, stk. 2, artikel 6, stk. 3, artikel 6, stk. 5, artikel 20, stk. 5, og artikel 23, 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 51

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, anvendes artikel 5 i forordning (EU) nr. 182/2011.

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 52

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 2016/943[24],

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

[24] 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).

(c) offentlige og nationale sikkerhedsinteresser

(d) strafferetlige eller administrative procedurers integritet.

2. Oplysninger, der udveksles på fortrolig basis mellem markedsovervågningsmyndighederne og mellem markedsovervågningsmyndighederne og Kommissionen, må ikke videregives uden forudgående tilladelse fra den oprindelige markedsmyndighed, jf. dog stk. 1.

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 straffelovgivning.

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 53

Sanktioner

1. Medlemsstaterne fastsætter bestemmelser om sanktioner for erhvervsdrivendes overtrædelse af denne forordning og træffer alle nødvendige foranstaltninger til at sikre håndhævelsen heraf. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

2. Medlemsstaterne giver straks Kommissionen meddelelse om disse regler og foranstaltninger og underretter den straks om senere ændringer, der berører dem.

3. Manglende opfyldelse af de væsentlige cybersikkerhedskrav i bilag I og forpligtelserne i artikel 10 og 11 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.

4. Manglende overholdelse af andre forpligtelser i henhold til denne forordning 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.

5. 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.

6. 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 andre markedsovervågningsmyndigheder allerede har pålagt den samme erhvervsdrivende administrative bøder for en lignende overtrædelse

(c) størrelsen på den erhvervsdrivende, der har begået overtrædelsen, og dens markedsandel.

7. Markedsovervågningsmyndigheder, der pålægger administrative bøder, deler disse oplysninger med markedsovervågningsmyndighederne i andre medlemsstater gennem det informations- og kommunikationssystem, der er omhandlet i artikel 34 i forordning (EU) 2019/1020.

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

9. 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 disse regler i disse medlemsstater har tilsvarende virkning.

10. 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.

KAPITEL VIII

OVERGANGSBESTEMMELSER OG AFSLUTTENDE BESTEMMELSER

Artikel 54

Ændring af forordning (EU) 2019/1020

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

"71. [forordning XXX] [forordning om cyberrobusthed]".

Artikel 55

Overgangsbestemmelser

1. Udstedte EU-typeafprøvningsattester og afgørelser om godkendelse vedrørende cybersikkerhedskrav til produkter med digitale elementer, der er omfattet af anden EU-harmoniseringslovgivning, forbliver gyldige indtil [42 måneder efter datoen for denne forordnings ikrafttræden], medmindre de udløber inden denne dato, eller medmindre andet er foreskrevet i anden EU-lovgivning, i hvilket tilfælde de forbliver gyldige som omhandlet i den pågældende EU-lovgivning.

2. Produkter med digitale elementer, der er bragt i omsætning inden den [datoen for denne forordnings anvendelse, jf. artikel 57], er kun omfattet af kravene i denne forordning, hvis disse produkter fra denne dato er genstand for væsentlige ændringer af deres design eller tilsigtede formål.

3. Uanset stk. 2 finder de forpligtelser, der er fastsat i artikel 11, anvendelse på alle produkter med digitale elementer inden for denne forordnings anvendelsesområde, som er bragt i omsætning inden den [datoen for denne forordnings anvendelse, jf. artikel 57].

Artikel 56

Evaluering og revision

Senest [36 måneder efter datoen for denne forordnings anvendelse] og hvert fjerde år derefter forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision af denne forordning. Rapporten offentliggøres.

Artikel 57

Ikrafttræden og anvendelsesdato

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

Den finder anvendelse fra den [24 måneder efter datoen for denne forordnings ikrafttræden]. Artikel 11 anvendes dog fra [12 måneder efter datoen for denne forordnings ikrafttræden].

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

Udfærdiget i Bruxelles, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

1.2. Berørt(e) politikområde(r)

1.3. Forslaget/initiativet vedrører:

1.4. Mål

1.4.1. Generelt/generelle mål

1.4.2. Specifikt/specifikke mål

1.4.3. Forventet/forventede resultat(er) og virkning(er)

1.4.4. Resultatindikatorer

1.5. Begrundelse for forslaget/initiativet

1.5.1. Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet

1.5.2. Merværdien ved et EU-tiltag (f.eks. som følge af koordineringsfordele, retssikkerhed, større effekt eller komplementaritet). For så vidt angår dette punkt skal der ved "Merværdien ved en indsats fra EU's side" forstås merværdien af EU's intervention i forhold til den værdi, der ellers ville være opnået med medlemsstaternes foranstaltninger på egen hånd.

1.5.3. Erfaringer fra tidligere foranstaltninger af lignende art

1.5.4. Forenelighed med den flerårige finansielle ramme og mulige synergivirkninger med andre relevante instrumenter

1.5.5. Vurdering af de forskellige finansieringsmuligheder, der er til rådighed, herunder muligheden for omfordeling

1.6. Forslagets/initiativets varighed og finansielle virkninger

1.7. Planlagt(e) forvaltningsmetode(r)

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om overvågning og rapportering

2.2. Forvaltnings- og kontrolsystem(er)

2.2.1. Begrundelse for den/de påtænkte forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

2.2.2. Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

2.2.3. Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftsområde(r) i den flerårige finansielle ramme og udgiftspost(er) på budgettet

3.2. Forslagets anslåede finansielle virkninger for bevillingerne

3.2.1. Sammenfatning af de anslåede virkninger for aktionsbevillingerne

3.2.2. Anslåede resultater finansieret med aktionsbevillinger

3.2.3. Sammenfatning af de anslåede virkninger for administrationsbevillingerne

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

3.2.5. Bidrag fra tredjemand

3.3. Anslåede virkninger for indtægterne

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

Forslag til forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer (forordning om cyberrobusthed)

1.2. Berørt(e) politikområde(r)

Kommunikationsnet, indhold og teknologi

1.3. Forslaget/initiativet vedrører:

× en ny foranstaltning

☐ en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning[37]

☐ en forlængelse af en eksisterende foranstaltning

☐ en sammenlægning eller en omlægning af en eller flere foranstaltninger til en anden/en ny foranstaltning

1.4. Mål

1.4.1. Generelt/generelle mål

Forslaget har to hovedmål, som skal sikre et velfungerende indre marked: 1) **skabe betingelser 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 og 2) **skabe betingelser, der gør det muligt for brugerne at tage hensyn til cybersikkerhed, når de udvælger og anvender produkter med digitale elementer**.

1.4.2. Specifikt/specifikke mål

Der blev fastsat **fire specifikke mål** i forslaget: i) sikre, at fabrikanterne forbedrer sikkerheden ved produkter med digitale elementer fra design- og udviklingsfasen og i hele livscyklussen, ii) sikre en sammenhængende ramme for cybersikkerhed, der letter hardware- og softwareproducenternes overholdelse af kravene, iii) øge gennemsigtigheden med hensyn til sikkerhedsegenskaber ved produkter med digitale elementer og iv) gøre det for muligt for virksomheder og forbrugere at anvende produkter med digitale elementer på en sikker måde.

Forventet/forventede resultat(er) og virkning(er)

Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgruppen.

Forslaget vil medføre betydelige fordele for de forskellige interessenter. For virksomhederne vil det forhindre divergerende sikkerhedsregler for produkter med digitale elementer og mindske omkostningerne til overholdelse af relateret lovgivning om cybersikkerhed. Det vil reducere antallet af cyberhændelser, omkostningerne til håndtering af hændelser og skade på omdømme. For hele EU

[37] Jf. finansforordningens artikel 58, stk. 2, litra a) hhv. b).

anslås det, at initiativet kan føre til en omkostningsreduktion som følge af hændelser, som påvirker virksomheder, på ca. 180-290 mia. EUR om året[38]. Det vil føre til en øget omsætning som følge af øget efterspørgsel efter produkter med digitale elementer. Det vil forbedre virksomhedernes globale omdømme og også føre til øget efterspørgsel uden for EU. For brugerne vil den foretrukne løsning øge gennemsigtigheden med hensyn til sikkerhedsegenskaberne og lette anvendelsen af produkter med digitale elementer. Forbrugere og borgere vil også få en bedre beskyttelse af deres grundlæggende rettigheder såsom privatlivets fred og databeskyttelse.

Forslaget vil samtidig medføre yderligere overholdelses- og håndhævelsesomkostninger for virksomheder, bemyndigede organer og offentlige myndigheder, herunder akkrediterings- og markedsovervågningsmyndigheder. For softwareudviklere og hardwarefabrikanter vil det medføre yderligere direkte overholdelsesomkostninger forbundet med nye sikkerhedskrav, overensstemmelsesvurdering og dokumentations- og rapporteringsforpligtelser, hvilket vil bringe de samlede overholdelsesomkostninger på op til ca. 29 mia. EUR for en anslået markedsværdi på op til 1 1485 mia. EUR i omsætning[39]. Brugere, herunder erhvervsbrugere, forbrugere og borgere, vil kunne opleve højere priser på produkter med digitale elementer. De skal dog ses på baggrund af de betydelige fordele, der er beskrevet ovenfor.

1.4.3. Resultatindikatorer

Angiv indikatorerne til overvågning af fremskridt og resultater.

For at teste, om fabrikanterne forbedrer sikkerheden af deres produkter med digitale elementer i design- og udviklingsfasen og i hele produkternes livscyklus, kan en række indikatorer tages i betragtning. Disse kan være antallet af væsentlige hændelser i Unionen som følge af sårbarheder, andelen af hardware- og softwarefabrikanter, der følger en systematisk sikker udviklingslivscyklus, en kvalitativ analyse af sikkerheden af produkter med digitale elementer, en kvantitativ og kvalitativ vurdering af sårbarhedsdatabaser, hyppigheden af sikkerhedsrettelser, der stilles til rådighed af fabrikanterne, eller det gennemsnitlige antal dage mellem opdagelse af sårbarhed og levering af sikkerhedsrettelser.

En indikator for en sammenhængende ramme for cybersikkerhed kunne være manglen på målrettet produktspecifik national lovgivning om cybersikkerhed.

En indikator for øget gennemsigtighed med hensyn til sikkerhedsegenskaberne ved produkter med digitale elementer kunne være andelen af produkter med digitale elementer, der leveres med oplysninger om sikkerhedsegenskaber. Andelen af produkter med digitale elementer, der leveres med brugsanvisninger om sikker anvendelse, kan desuden anvendes som en indikator for, om organisationer og forbrugere har mulighed for at anvende produkter med digitale elementer sikkert.

Med hensyn til overvågningen af forordningens virkninger vil bestemte indikatorer indgå i Kommissionens overvejelser, eventuelt med støtte fra ENISA. Afhængigt af det operationelle mål, der skal nås, er nogle af de overvågningsindikatorer, på

[38] Se [arbejdsdokument fra Kommissionens tjenestegrene om konsekvensanalyse, der ledsager forslaget til forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer].

[39] Se [arbejdsdokument fra Kommissionens tjenestegrene om konsekvensanalyse, der ledsager forslaget til forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer].

grundlag af hvilke opfyldelsen af de horisontale cybersikkerhed vil blive vurderet, følgende:

I forbindelse med vurdering af cybersikkerhedsniveauet for produkter med digitale elementer:

— Statistikker og kvalitative analyser af hændelser, der påvirker produkter med digitale elementer, og af hvordan disse er blevet håndteret. Disse kan indsamles og vurderes af Kommissionen med støtte fra ENISA.

— Lister over kendte sårbarheder og analyser af, hvordan disse er blevet håndteret. En sådan analyse kan foretages af ENISA på grundlag af den europæiske sårbarhedsdatabase oprettet i henhold til [direktiv XXX/XXXX (NIS2)].

— Undersøgelser blandt fabrikanter af hardware og software med henblik på overvågning af fremskridt.

I forbindelse med vurdering af informationsniveauet for sikkerhedselementer, sikkerhedsstøtte, udtjente produkter og pligt til at udvise rettidig omhu: Resultater af undersøgelser, der skal gennemføres af Kommissionen med støtte fra ENISA, for både brugere og virksomheder.

I forbindelse med vurdering af gennemførelsen vil Kommissionen bestræbe sig på at sikre, at overensstemmelsesvurderingerne gennemføres effektivt. Med henblik herpå vil der blive fremsat en standardiseringsanmodning, og dens gennemførelse vil blive fulgt. Kommissionen vil også kontrollere de bemyndigede organers og, hvis det er relevant, certificeringsorganernes kapacitet.

Med hensyn til anvendelsen vil Kommissionen på grundlag af medlemsstaternes rapporter kontrollere, at nationale initiativer ikke vedrører aspekter, der er omfattet af forordningen.

1.5. Begrundelse for forslaget/initiativet

1.5.1. Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet

Forordningen bør finde fuld anvendelse 24 måneder efter dens ikrafttræden. Elementer i forvaltningsstrukturen bør dog være på plads inden da. Medlemsstaterne skal navnlig have udpeget eksisterende myndigheder og/eller oprettet nye myndigheder til at udføre de i lovgivningen omhandlede opgaver.

1.5.2. Merværdien ved et EU-tiltag (f.eks. som følge af koordineringsfordele, retssikkerhed, større effekt eller komplementaritet). For så vidt angår dette punkt skal der ved "Merværdien ved en indsats fra EU's side" forstås merværdien af EU's intervention i forhold til den værdi, der ellers ville være opnået med medlemsstaternes foranstaltninger på egen hånd.

Den stærke grænseoverskridende karakter af cybersikkerhed og det stigende antal hændelser med afsmittende virkninger på tværs af grænser, sektorer og produkter betyder, at målene ikke kan opfyldes effektivt af medlemsstaterne alene. I betragtning af den globale karakter af produkter med digitale elementer står medlemsstaterne over for de samme risici i forbindelse med det samme produkt med digitale elementer på deres område. Et kludetæppe af potentielt divergerende nationale regler risikerer også at forhindre et åbent og konkurrencedygtigt indre

marked for produkter med digitale elementer. En fælles indsats på EU-plan er derfor nødvendig for at øge tilliden blandt brugerne og gøre EU-produkter med digitale elementer mere attraktive. Det vil også gavne det indre marked ved at sikre retssikkerhed og lige vilkår for leverandører af produkter med digitale elementer.

1.5.3. Erfaringer fra tidligere foranstaltninger af lignende art

Forordningen om cyberrobusthed er den første forordning af sin art, som indfører cybersikkerhedskrav til produkter med digitale elementer, der bringes i omsætning. Den bygger imidlertid på den nye lovgivningsmæssige ramme og de erfaringer, der er gjort i forbindelse med gennemførelsen af eksisterende EU-harmoniseringslovgivning for en række produkter, navnlig med forberedelsen af gennemførelsen, herunder aspekter som udarbejdelse af harmoniserede standarder.

1.5.4. Forenelighed med den flerårige finansielle ramme og mulige synergivirkninger med andre relevante instrumenter

I forordningen om horisontale cybersikkerhedskrav til produkter med digitale elementer fastsættes nye cybersikkerhedskrav til alle produkter med digitale elementer, der bringes i omsætning på EU-markedet, som går videre end de krav, der er fastsat i den eksisterende lovgivning. Forslaget bygger samtidig på den eksisterende nye lovgivningsmæssige ramme. Den vil derfor bygge på eksisterende strukturer og procedurer i den nye lovgivningsmæssige ramme såsom samarbejde mellem bemyndigede organer og markedsovervågning, overensstemmelsesvurderingsmoduler og udvikling af harmoniserede standarder. Det nye forslag vil også bygge på strukturer udviklet i henhold til anden cybersikkerhedslovgivning såsom direktiv 2016/1148 (NIS-direktivet), [direktiv XXX/XXXX (NIS2)] eller forordning 2019/881 (forordningen om cybersikkerhed).

1.5.5. Vurdering af de forskellige finansieringsmuligheder, der er til rådighed, herunder muligheden for omfordeling

Forvaltningen af de indsatsområder, der er tildelt ENISA, ligger inden for rammerne af agenturets eksisterende mandat og generelle opgaver. Disse indsatsområder kan kræve særlige profiler eller nye opgaver, men disse vil ikke være mærkbare og kan finansieres ved brug af ENISA's eksisterende ressourcer og ved omfordeling eller sammenkobling af forskellige opgaver. Et af de vigtigste indsatsområder, som ENISA har fået tildelt, vedrører f.eks. indsamling og behandling af underretninger fra fabrikanter om udnyttede produktsårbarheder. I henhold til [direktiv XXX/XXXX (NIS2)] har ENISA til opgave at oprette en europæisk sårbarhedsdatabase, hvor offentligt kendte sårbarheder kan offentliggøres og registreres på frivillig basis for at give brugerne mulighed for at træffe passende afhjælpende foranstaltninger. Ressourcer, der er afsat til dette formål, kan også anvendes til de nye ovennævnte opgaver vedrørende underretninger om produktsårbarheder. Dette kan sikre en effektiv anvendelse af eksisterende ressourcer og vil også skabe de nødvendige synergier mellem sådanne opgaver og således et bedre grundlag for ENISA's analyser af cybersikkerhedsrisici og -trusler.

1.6. Forslagets/initiativets varighed og finansielle virkninger

☐ **begrænset varighed**

– ☐ gældende fra [DD/MM]ÅÅÅÅ til [DD/MM]ÅÅÅÅ

– ☐ finansielle virkninger fra ÅÅÅÅ til ÅÅÅÅ for forpligtelsesbevillinger og fra ÅÅÅÅ til ÅÅÅÅ for betalingsbevillinger

× **ubegrænset varighed**

– Iværksættelse med en indkøringsperiode fra 2025.

– derefter gennemførelse i fuldt omfang

1.7. Planlagt(e) forvaltningsmetode(r)[40]

☐ **Direkte forvaltning** ved Kommissionen

– × i dens tjenestegrene, herunder ved dens personale i EU's delegationer

– ☐ i forvaltningsorganerne

☐ **Delt forvaltning** i samarbejde med medlemsstaterne

☐ **Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:

– ☐ tredjelande eller organer, som tredjelande har udpeget

– ☐ internationale organisationer og deres agenturer (angives nærmere)

– ☐ Den Europæiske Investeringsbank og Den Europæiske Investeringsfond

– ☐ de organer, der er omhandlet i finansforordningens artikel 70 og 71

– ☐ offentligretlige organer

– ☐ privatretlige organer, der har fået overdraget offentlige tjenesteydelsesopgaver, i det omfang de har fået stillet tilstrækkelige finansielle garantier

– ☐ privatretlige organer, undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som har fået stillet tilstrækkelige finansielle garantier

– ☐ personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er anført i den relevante basisretsakt

– *Hvis der angives flere forvaltningsmetoder, gives der en nærmere forklaring i afsnittet "Bemærkninger".*

Bemærkninger

Ved denne forordning tillægges ENISA visse opgaver i overensstemmelse med dets eksisterende mandat, navnlig artikel 3, stk. 2, i forordning (EU) 2019/881, hvori det hedder, at ENISA udfører de opgaver, det tillægges ved EU-retsakter, der fastsætter foranstaltninger med henblik på indbyrdes tilnærmelse af de af medlemsstaternes love og administrative bestemmelser, der vedrører cybersikkerhed. ENISA har navnlig til opgave at modtage underretninger fra fabrikanter om aktivt udnyttede sårbarheder i produkter med digitale elementer samt om hændelser, der indvirker på disse produkters sikkerhed. ENISA bør også

[40] Forklaringer vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: https://myintracomm.ec.europa.eu/budgweb/DA/man/budgmanag/Pages/budgmanag.aspx.

videresende disse underretninger til de relevante CSIRT'er eller til de relevante centrale kontaktpunkter i medlemsstaterne, der er udpeget i overensstemmelse med artikel [artikel X] direktiv [direktiv XXX/XXXX (NIS2)], og underrette markedsovervågningsmyndighederne. På grundlag af de oplysninger, som agenturet indsamler, bør ENISA hvert andet år udarbejde en teknisk rapport om nye tendenser med hensyn til cybersikkerhedsrisici forbundet med produkter med digitale elementer og forelægge den for NIS-samarbejdsgruppen. I betragtning af ENISA's ekspertise, indsamlede oplysninger og trusselsanalyser kan ENISA desuden støtte processen for gennemførelse af denne forordning ved at foreslå fælles aktiviteter, der skal gennemføres af nationale markedsovervågningsmyndigheder, 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 kan tilrettelægges samtidige, koordinerede kontrolaktioner. Kommissionen kan anmode ENISA om at foretage evalueringer af specifikke produkter under ekstraordinære omstændigheder i forbindelse med produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, og hvor et hurtigt indgreb er nødvendigt for at bevare et velfungerende indre marked.

Alle disse opgaver anslås til ca. 4,5 fuldtidsækvivalenter fra ENISA's eksisterende ressourcer og bygger på eksisterende ekspertise og det forberedende arbejde, som ENISA udfører i øjeblikket, bl.a. til støtte for den kommende gennemførelse af [direktiv XXX/XXXX (NIS2)], hvortil ENISA's ressourcer blev suppleret.

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om overvågning og rapportering

Angiv hyppighed og betingelser.

Senest 36 måneder efter datoen for denne forordnings anvendelse og hvert fjerde år derefter forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision. Rapporten offentliggøres.

2.2. Forvaltnings- og kontrolsystem(er)

2.2.1. Begrundelse for den/de påtænkte forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

Ved denne forordning fastlægges en ny politik for harmoniserede cybersikkerhedskrav til produkter med digitale elementer, der bringes i omsætning i det indre marked, gennem hele deres livscyklus. Retsakten vil blive fulgt op af anmodninger fra Kommissionen til de europæiske standardiseringsorganer om at udvikle standarder.

For at kunne løse disse nye opgaver er det nødvendigt at afsætte tilstrækkelige ressourcer til Kommissionens tjenestegrene. Håndhævelsen af den nye forordning anslås at kræve 7 FTE'er (heraf én UNE) til varetagelse af følgende opgaver:

- Udarbejdelse af standardiseringsanmodningen og/eller fælles specifikationer ved hjælp af gennemførelsesretsakter, hvis der ikke er en vellykket standardiseringsproces
- Udarbejdelse af en delegeret retsakt [inden for 12 måneder efter forordningens ikrafttræden], der præciserer definitionerne af kritiske produkter med digitale elementer
- Eventuel udarbejdelse af delegerede retsakter med henblik på opdatering af listen over kritiske produkter i klasse I og II, præcisering af, om en begrænsning eller udelukkelse er nødvendig for produkter med digitale elementer, der er omfattet af andre EU-forskrifter, der fastlægger krav, som sikrer samme beskyttelsesniveau som denne forordning, tildeling af mandat til certificering af visse meget kritiske produkter med digitale elementer baseret på de kriterier, der er fastsat i denne forordning, præcisering af minimumsindholdet i EU-overensstemmelseserklæringen og supplering af de elementer, der skal indgå i den tekniske dokumentation
- Eventuel udarbejdelse af gennemførelsesretsakter vedrørende formatet for eller elementerne i rapporteringsforpligtelserne, softwarekomponentlisten, de fælles specifikationer eller anbringelsen af CE-mærkning
- Eventuel forberedelse af et hurtigt indgreb med henblik på at indføre korrigerende eller restriktive foranstaltninger under ekstraordinære omstændigheder for at bevare et velfungerende indre marked, herunder udarbejdelse af en gennemførelsesretsakt
- Tilrettelæggelse og koordinering af medlemsstaternes notifikation af bemyndigede organer og koordinering af de bemyndigede organer
- Støtte af koordineringen af medlemsstaternes markedsovervågningsmyndigheder.

2.2.2. Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

For at sikre, at bemyndigede organer og markedsovervågningsmyndigheder udveksler oplysninger og samarbejder godt, er Kommissionen ansvarlig for deres koordinering. For så vidt angår teknisk og markedsrelateret ekspertise vil der blive nedsat en ekspertgruppe.

2.2.3. Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

2.3. I betragtning af den lave værdi pr. transaktion (f.eks. godtgørelse af rejseudgifter for en delegeret i forbindelse med et møde) synes standardkontrolprocedurerne for mødeudgifter at være tilstrækkelige. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger, f.eks. fra strategien til bekæmpelse af svig.

Kommissionens eksisterende foranstaltninger til forebyggelse af svig vil dække de supplerende bevillinger, der er nødvendige for denne forordning.

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftsområde(r) i den flerårige finansielle ramme og udgiftspost(er) på budgettet

- Eksisterende budgetposter

Skema

- Nye budgetposter, som der anmodes om

Ikke relevant

3.2. Forslagets anslåede finansielle virkninger for bevillingerne

3.2.1. Sammenfatning af de anslåede virkninger for aktionsbevillingerne

– ☑ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☐ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

Udgiftsområde i den flerårige finansielle ramme	Nummer	

GD: <…….>			År **N**[41]	År **n+1**	År **n+2**	År **n+3**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)			**I ALT**
•Aktionsbevillinger										
Budgetpost[42]	Forpligtelser	(1a)								
	Betalinger	(2a)								
Budgetpost	Forpligtelser	(1b)								
	Betalinger	(2b)								
Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer[43]										
Budgetpost		(3)								
Bevillinger I ALT	Forpligtelser	=1a+1b +3								

41 År n er det år, hvor gennemførelsen af forslaget/initiativet påbegyndes. Erstat "n" med det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de efterfølgende år.

42 Ifølge den officielle budgetkontoplan.

43 Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller foranstaltninger (tidligere BA-poster), indirekte forskning, direkte forskning.

til GD <…….>	Betalinger	=2a+2b +3								

• Aktionsbevillinger I ALT	Forpligtelser	(4)								
	Betalinger	(5)								
• Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT		(6)								
Bevillinger I ALT Under UDGIFTSOMRÅDE<….> i den flerårige finansielle ramme	Forpligtelser	=4+ 6								
	Betalinger	=5+ 6								

<u>Hvis flere aktionsrelaterede udgiftsområder berøres af forslaget/initiativet, indsættes der et tilsvarende afsnit for hvert udgiftsområde</u>

• Aktionsbevillinger I ALT (alle aktionsrelaterede udgiftsområder)	Forpligtelser	(4)								
	Betalinger	(5)								
Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT (alle aktionsrelaterede udgiftsområder)		(6)								
Bevillinger I ALT under UDGIFTSOMRÅDE 1-6 i den flerårige finansielle ramme (referencebeløb)	Forpligtelser	=4+ 6								
	Betalinger	=5+ 6								

Udgiftsområde i den flerårige finansielle ramme	7	"Administrationsudgifter"

Dette afsnit skal udfyldes ved hjælp af arket vedrørende administrative budgetoplysninger, der først skal indføres i bilaget til finansieringsoversigten (bilag V til de interne regler), som uploades til DECIDE med henblik på høring af andre tjenestegrene.

i mio. EUR (tre decimaler)

		År 2024	År 2025	År 2026	År 2027	I ALT
GD: CNECT						
• Menneskelige ressourcer		1,030	1,030	1,030	1,030	**4,120**
• Andre administrationsudgifter		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
I ALT GD CNECT	Bevillinger	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Bevillinger I ALT under UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	(Forpligtelser i alt = betalinger i alt)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

i mio. EUR (tre decimaler)

		År 2024	År 2025	År 2026	År 2027	I ALT
Bevillinger I ALT under UDGIFTSOMRÅDE 1-7 i den flerårige finansielle ramme	Forpligtelser	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Betalinger	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Anslåede resultater finansieret med aktionsbevillinger

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv mål og resultater ⇩			År **n**		År **n+1**		År **n+2**		År **n+3**		Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)						**I ALT**	
	RESULTATER																	
	Type 44	Gnsntl. omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal resultater i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[45]																		
— Resultat																		
— Resultat																		
— Resultat																		
Subtotal for specifikt mål nr. 1																		
SPECIFIKT MÅL NR. 2																		
— Resultat																		
Subtotal for specifikt mål nr. 2																		
I ALT																		

44 Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks.: antal finansierede studenterudvekslinger, antal km bygget vej osv.).

45 Som beskrevet i punkt 1.4.2 "Specifikt/specifikke mål ...".

3.2.3. Sammenfatning af de anslåede virkninger for administrationsbevillingerne

– ☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

– ☑ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År **2024**	År **2025**	År **2026**	År **2027**	
UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme					
Menneskelige ressourcer	1,030	1,030	1,030	1,030	**4,120**
Andre administrationsudgifter	0,222	0,222	0,222	0,222	**0,888**
Subtotal UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	1,252	1,252	1,252	1,252	**5,008**

Uden for UDGIFTSOMRÅDE 7[46] i den flerårige finansielle ramme					
Menneskelige ressourcer					
Andre udgifter Andre administrationsudgifter					
Subtotal uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme					

I ALT	1,252	1,252	1,252	1,252	**5,008**

Bevillingerne til menneskelige ressourcer og andre administrationsudgifter vil blive dækket ved hjælp af de bevillinger, som generaldirektoratet allerede har afsat til forvaltning af foranstaltningen, og/eller ved intern omfordeling i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

[46] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller aktioner (tidligere BA-poster), indirekte forskning, direkte forskning.

3.2.3.1. Anslået behov for menneskelige ressourcer

– ☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

– ☑ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

Overslag angives i årsværk

		År **2024**	År **2025**	År **2026**	År **2027**
20 01 02 01 (i hovedsædet og i Kommissionens repræsentationskontorer)		6	6	6	6
20 01 02 03 (i delegationerne)					
01 01 01 01 (indirekte forskning)					
01 01 01 11 (direkte forskning)					
Andre budgetposter (skal angives)					
• Eksternt personale (i årsværk)[47]					
20 02 01 (KA, UNE, V under den samlede bevillingsramme)		1	1	1	1
20 02 03 (KA, LA, UNE, V og JMD i delegationerne)					
XX 01 xx **yy zz** [48]	— i hovedsædet				
	– i delegationerne				
01 01 01 02 (KA, UNE, V – indirekte forskning)					
01 01 01 12 (KA, UNE, V — direkte forskning)					
Andre budgetposter (skal angives)					
I ALT		**7**	**7**	**7**	**7**

XX angiver det berørte politikområde eller budgetafsnit.

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til forvaltning af foranstaltningen, og/eller ved interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte 6 årsværk x 157 000 EUR/år = 942 000 EUR	Som beskrevet i punkt 2.2.1: – Udarbejdelse af standardiseringsanmodningen og/eller fælles specifikationer ved hjælp af gennemførelsesretsakter, hvis der ikke er en vellykket standardiseringsproces – Udarbejdelse af en delegeret retsakt [inden for 12 måneder efter forordningens ikrafttræden], der præciserer definitionerne af kritiske produkter med digitale elementer – Eventuel udarbejdelse af delegerede retsakter med henblik på opdatering af listen over kritiske produkter i klasse I og II, præcisering af, om en begrænsning eller udelukkelse er nødvendig for produkter med digitale elementer, der er omfattet af andre EU-forskrifter, der fastlægger krav, som sikrer samme beskyttelsesniveau som denne forordning, tildeling af mandat til certificering af visse meget kritiske produkter med digitale elementer baseret på de kriterier, der er fastsat i denne forordning, præcisering af minimumsindholdet i EU-overensstemmelseserklæringen og supplering af

[47] KA: kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JMD: juniormedarbejdere i delegationerne.

[48] Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

	de elementer, der skal indgå i den tekniske dokumentation – Eventuel udarbejdelse af gennemførelsesretsakter vedrørende formatet for eller elementerne i rapporteringsforpligtelserne, softwarekomponentlisten, de fælles specifikationer eller anbringelsen af CE-mærkning – Eventuel forberedelse af et hurtigt indgreb med henblik på at indføre korrigerende eller restriktive foranstaltninger under ekstraordinære omstændigheder for at bevare et velfungerende indre marked, herunder udarbejdelse af en gennemførelsesretsakt – Tilrettelæggelse og koordinering af medlemsstaternes notifikation af bemyndigede organer og koordinering af de bemyndigede organer – Støtte af koordineringen af medlemsstaternes markedsovervågningsmyndigheder.
Eksternt personale 1 UNE x 88 000 EUR/år	Som beskrevet i punkt 2.2.1: – Udarbejdelse af standardiseringsanmodningen og/eller fælles specifikationer ved hjælp af gennemførelsesretsakter, hvis der ikke er en vellykket standardiseringsproces – Udarbejdelse af en delegeret retsakt [inden for 12 måneder efter forordningens ikrafttræden], der præciserer definitionerne af kritiske produkter med digitale elementer – Eventuel udarbejdelse af delegerede retsakter med henblik på opdatering af listen over kritiske produkter i klasse I og II, præcisering af, om en begrænsning eller udelukkelse er nødvendig for produkter med digitale elementer, der er omfattet af andre EU-forskrifter, der fastlægger krav, som sikrer samme beskyttelsesniveau som denne forordning, tildeling af mandat til certificering af visse meget kritiske produkter med digitale elementer baseret på de kriterier, der er fastsat i denne forordning, præcisering af minimumsindholdet i EU-overensstemmelseserklæringen og supplering af de elementer, der skal indgå i den tekniske dokumentation – Eventuel udarbejdelse af gennemførelsesretsakter vedrørende formatet for eller elementerne i rapporteringsforpligtelserne, softwarekomponentlisten, de fælles specifikationer eller anbringelsen af CE-mærkning – Eventuel forberedelse af et hurtigt indgreb med henblik på at indføre korrigerende eller restriktive foranstaltninger under ekstraordinære omstændigheder for at bevare et velfungerende indre marked, herunder udarbejdelse af en gennemførelsesretsakt – Tilrettelæggelse og koordinering af medlemsstaternes notifikation af bemyndigede organer og koordinering af de bemyndigede organer – Støtte af koordineringen af medlemsstaternes markedsovervågningsmyndigheder.

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

Forslaget/initiativet:

– x kan finansieres fuldt ud gennem omfordeling inden for det relevante udgiftsområde i den flerårige finansielle ramme (FFR).

Der kræves ikke omlægning.

– ☐ kræver anvendelse af den uudnyttede margen under det relevante udgiftsområde i FFR og/eller anvendelse af særlige instrumenter som fastlagt i FFR-forordningen

—

– ☐ kræver en revision af FFR

—

3.2.5. Bidrag fra tredjemand

Forslaget/initiativet:

– x indeholder ikke bestemmelser om samfinansiering med tredjemand

– ☐ indeholder bestemmelser om samfinansiering med tredjemand, jf. følgende overslag:

Bevillinger i mio. EUR (tre decimaler)

	År **N**[49]	År **n+1**	År **n+2**	År **n+3**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)			I alt
Angiv det organ, der deltager i samfinansieringen								
Samfinansierede bevillinger I ALT								

[49] År n er det år, hvor gennemførelsen af forslaget/initiativet påbegyndes. Erstat "n" med det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de efterfølgende år.

3.3. Anslåede virkninger for indtægterne

– ☐ Forslaget/initiativet har ingen finansielle virkninger for indtægterne

– ☐ Forslaget/initiativet har følgende finansielle virkninger:

– ☐ for egne indtægter

– ☐ for andre indtægter

– Angiv, om indtægterne er formålsbestemte ☐

i mio. EUR (tre decimaler)

Indtægtspost på budgettet:	Bevillinger til rådighed i indeværende regnskabsår	Forslagets/initiativets virkninger[50]						
		År **n**	År **n+1**	År **n+2**	År **n+3**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)		
Artikel …								

For indtægter, der er formålsbestemte, angives det, hvilke af budgettets udgiftsposter der berøres.

Andre bemærkninger (f.eks. om hvilken metode, der er benyttet til at beregne virkningerne for indtægterne).

[50] Med hensyn til EU's traditionelle egne indtægter (told og sukkerafgifter) opgives beløbene netto, dvs. bruttobeløb, hvorfra der er trukket opkrævningsomkostninger på 20 %.