C/2026/6013

17.11.2026

MEDDELELSE FRA KOMMISSIONEN

Kommissionens vejledning til anvendelse af forordning (EU) 2024/2847 (forordningen om cyberrobusthed)

(C/2026/6013)

Indholdsfortegnelse

Side

1. INDLEDNING 3
   - 1.1. Forordningen om cyberrobusthed 3
   - 1.2. Vejledningens formål 3
2. ANVENDELSESOMRÅDE 4
   - 2.1. Markedsføring 4
   - 2.2. Software som et produkt med digitale elementer 5
   - 2.3. Computerkode 6
   - 2.4. Kombination af hardware og software, der udgør et produkt med digitale elementer 7
   - 2.5. Dataforbindelse 8
   - 2.6. Komplekse systemer 8
   - 2.7. Produkter med digitale elementer, der er udformet før CRA begyndte at finde anvendelse 9
3. FRI OG OPEN SOURCE-SOFTWARE 11
   - 3.1. Fastlæggelse af, om fri og open source-software hører under en persons ansvar 12
   - 3.2. Fastlæggelse af, om fri og open source-software bringes i omsætning på EU-markedet 13
     - 3.2.1. Opkrævning af en pris 13
     - 3.2.2. Indtjening på andre tjenester eller krav om behandling af personoplysninger 13
     - 3.2.3. Støttetjenester 14
     - 3.2.4. Donationer 15
     - 3.2.5. Finansiering af fri og open source-software 15
     - 3.2.6. Almennyttige enheder oprettet med henblik på almennyttige mål 16
     - 3.2.7. Integration foretaget af andre fabrikanter 16
   - 3.3. Open source-software-forvaltere 16
     - 3.3.1. Vedvarende støtte og sikring af levedygtigheden af en FOSS 17
   - 3.4. Bidragydere og anvendelser downstream 18
   - 3.5. Illustrative scenarier 19
4. VÆSENTLIGE ÆNDRINGER OG RESERVEDELE 21
   - 4.1. Fysiske reparationer 22
   - 4.2. Reservedele 23
   - 4.3. Softwareopdateringer som væsentlige ændringer 24

4.4. Konsekvenser af en væsentlig ændring 27
4.4.1. Væsentlige ændringer foretaget af en anden person end den oprindelige fabrikant 28
4.4.2. Væsentlige ændringer foretaget af den oprindelige fabrikant 29
5. VEDLIGEHOLDELSESPERIODE 29
5.1. Væsentlige ændringer og vedligeholdelsesperioden 31
6. VIGTIGE OG KRITISKE PRODUKTER MED DIGITALE ELEMENTER 32
6.1. Kernefunktionalitet 33
6.2. Overensstemmelsesvurdering af vigtige og kritiske produkter med digitale elementer 36
6.3. Betydning for formodningen om overensstemmelse 38
7. CYBERSIKKERHEDSRISIKOVURDERING OG INTEGRATION AF PRODUKTER MED DIGITALE ELEMENTER OG KOMPONENTER 41
7.1. Om vurdering og behandling af cybersikkerhedsrisici 41
7.2. Om design, udvikling og produktion af produkter med digitale elementer på en sådan måde, at de sikrer et passende cybersikkerhedsniveau på grundlag af risiciene 42
7.3. Risikovurdering og due diligence i forbindelse med eksterne afhængigheder og integrerede komponenter 42
7.4. Genbrug af risikovurderinger og overensstemmelsesdokumentation for familier af produkter med digitale elementer 44
8. FJERNDATABEHANDLING 44
8.1. Hvad anses for at være en fjerndatabehandlingsløsning for et produkt med digitale elementer? 45
8.1.1. Begrebet »eksternt« 46
8.1.2. Ville fraværet af en sådan databehandling forhindre produktet med digitale elementer i at udføre en af funktionerne? 46
8.1.3. Er softwaren designet og udviklet af fabrikanten eller under dennes ansvar? 47
8.2. Praktiske og tekniske konsekvenser af fjerndatabehandlingsløsninger og afhængighed af tredjepartsløsninger 49
8.3. Anvendelsestilfælde for fjerndatabehandlingsløsninger 50
8.3.1. Mobilbankapplikation 51
8.3.2. Intelligent termostat 52
8.3.3. E-bogslæser 53
8.3.4. Industrirobot 53
8.3.5. Mobilnet 53
9. YDERLIGERE ELEMENTER 54
9.1. Indberetningsforpligtelser 54
9.2. Håndtering af sårbarheder 56
9.2.1. Indberetning upstream og deling af rettelser af sikkerhedsfejl 56
9.2.2. Kendte sårbarheder, der kan udnyttes 57
9.2.3. Effektive og regelmæssige test og gennemgange 58
9.3. Samspil med anden lovgivning 59
9.3.1. Forordning (EU) 2019/2144 og forordning (EU) nr. 168/2013 59
9.3.2. EU-typeafprøvningsattesters gyldighed (artikel 69, stk. 1) 59

1. **INDLEDNING**

1.1. **Forordningen om cyberrobusthed**

1. Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) ([1]) trådte i kraft den 10. december 2024. Forordningen har til formål at styrke EU's tilgang til cybersikkerhed, sikre cyberrobusthed på EU-plan og forbedre det indre markeds funktion ved at fastlægge en ensartet retlig ramme for væsentlige cybersikkerhedskrav ved afsætning af produkter med digitale elementer på EU's marked samt i hele livscyklussen for et produkt med digitale elementer.

2. Forordningen om cyberrobusthed (CRA) bygger på EU's nye lovgivningsmæssige ramme (NLF), der er fastsat i Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93 og 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 ([2]).

3. Markedsovervågning og håndhævelse varetages af de nationale markedsovervågningsmyndigheder. Produkter med digitale elementer, som er omfattet af anvendelsesområdet for CRA, er omfattet af 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. Kommissionen og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) understøtter de økonomiske aktører og medlemsstaterne i anvendelsen af CRA.

1.2. **Vejledningens formål**

4. I henhold til artikel 26, stk. 1, i CRA skal Kommissionen offentliggøre en vejledning med henblik på at bistå de økonomiske aktører med at anvende forordningen og med særligt fokus på at lette mikrovirksomheders og små og mellemstore virksomheders (SMV'ers) overholdelse af forordningen. I artikel 26, stk. 2, fastsættes de minimumsaspekter, der bør behandles i vejledningen. Disse omfatter bl.a.: i) anvendelsesområdet for CRA (med særligt fokus på fjerndatabehandlingsløsninger og fri og open source-software), ii) begrebet »vedligeholdelsesperioder«, iii) samspillet mellem CRA og anden EU-lovgivning, iv) begrebet »væsentlig ændring«.

5. Den 3. december 2025 offentliggjorde Kommissionen en række ofte stillede spørgsmål (OSS), hvor formålet var at hjælpe økonomiske aktører med at forberede sig på gennemførelsen af CRA ([3]).

6. Denne vejledning har til formål at hjælpe økonomiske aktører med at overholde CRA og at understøtte markedsovervågningsmyndigheders, notificerende myndigheders og bemyndigede organers aktiviteter med henblik på at sikre en harmoniseret håndhævelse af CRA i hele Unionen. Denne vejledning har ikke til formål at dække hele anvendelsesområdet for CRA, men snarere at præcisere begrundelserne for udvalgte centrale bestemmelser, samt hvordan disse gennemføres i praksis. Denne vejledning vedrører CRA og finder ikke anvendelse på anden EU-lovgivning.

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

([2]) I Kommissionens arbejdsprogram for 2026 forventes det, at der fremlægges en »europæisk produktretsakt«, hvorved NLF og reglerne om markedsovervågning og standardisering ajourføres: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:52025DC0870.

([3]) OSS-listen kan downloades via Kommissionens websted om gennemførelse af CRA under Ofte stillede spørgsmål.

7. Der blev foretaget brede interessenthøringer i forbindelse med udarbejdelsen af denne vejledning, herunder Ekspertgruppen om cybersikkerhed for produkter med digitale elementer ([4]), samt en offentlig høring i perioden 3. marts-13. april 2026 ([5]).

8. Denne vejledning er ikke bindende for økonomiske aktører eller andre aktører, der er omfattet af CRA. En autoritativ fortolkning af CRA kan kun gives af Den Europæiske Unions Domstol. Ikke desto mindre indeholder disse retningslinjer Kommissionens fortolkning af CRA med henblik på at støtte overholdelsen af forordningen og bidrage til en effektiv gennemførelse heraf. Endvidere indeholder vejledningen en række eksempler, der illustrerer anvendelsen af udvalgte specifikke bestemmelser. Eksemplerne må dog ikke træde i stedet for en vurdering fra sag til sag, som altid vil være nødvendig for at tage højde for særlige forhold i de enkelte tilfælde.

9. I overensstemmelse med artikel 26 i CRA kan Kommissionen overveje at udstede yderligere vejledning, herunder vejledning målrettet mod fabrikanter, der er omfattet af CRA og anden EU-harmoniseringslovgivning eller af andre relaterede EU-retsakter. Denne vejledning kan f.eks. omhandle spørgsmål om samspillet mellem CRA og forordning (EU) 2024/1689 om harmoniserede regler for kunstig intelligens (forordningen om kunstig intelligens) og forordning (EU) 2022/2554 om digital operationel modstandsdygtighed i den finansielle sektor (DORA).

2. **ANVENDELSESOMRÅDE**

2.1. **Markedsføring**

10. CRA finder anvendelse på produkter med digitale elementer, der gøres tilgængelige på EU-markedet. Begrebet tilgængeliggørelse på markedet defineres i artikel 3, nr. 22), i CRA som »levering af et produkt med digitale elementer med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed mod eller uden vederlag«. I overensstemmelse med artikel 3, nr. 21), bringes et produkt med digitale elementer i omsætning på EU-markedet første gang, det gøres tilgængeligt.

11. Den seneste udgave af »Den blå vejledning om gennemførelse af EU's produktregler«, der blev offentliggjort i 2022 (i det følgende benævnt »den blå vejledning«) ([6]) indeholder en vejledning, der gør det lettere at forstå EU's produktregler og anvende dem ensartet på tværs af de forskellige sektorspecifikke retlige rammer, der er tilpasset den nye lovgivningsmæssige ramme (NLF), såsom CRA. Den blå vejledning angiver, at begreberne »bringe i omsætning« og »tilgængeliggørelse« skal forstås som en henvisning »til hvert enkelt produkt og ikke til en produkttype, eller hvorvidt det blev fremstillet for sig selv eller som led i en serie« (afsnit 2.3).

12. For så vidt angår mere »traditionelle« produkter med digitale elementer, der er omfattet af NLF, såsom hardware i form af maskiner eller radioudstyrsprodukter med digitale elementer, er begrebet »bringe i omsætning« veletableret, og den blå vejledning indeholder en yderligere præcisering af, hvornår sådanne produkter anses for at være bragt i omsætning. Under »Kortfattede eksempler« i afsnit 2.12 i den blå vejledning gives yderligere eksempler på begrebet »bringe i omsætning«.

13. I betragtning af karakteren af immaterielle produkter med digitale elementer såsom enkeltstående software er der imidlertid behov for yderligere vejledning om, hvornår sådanne produkter med digitale elementer anses for at være bragt i omsætning. Når fremstillingsfasen for en software er afsluttet, og et produkt med digitale elementer tilbydes til mulige brugere på EU-markedet, kan fabrikanten anses for at have fremstillet flere eksemplarer af det samme softwareprodukt med digitale elementer og for at have leveret dem med henblik på distribution eller anvendelse. Enkeltstående software er nemlig, i modsætning til materielle produkter med digitale elementer, ikke underlagt

([4]) Ekspertgruppen om cybersikkerhed for produkter med digitale elementer i Kommissionens register over ekspertgrupper og lignende enheder.
([5]) Offentlig høring om udkast til Kommissionens vejledning om forordningen om cyberrobusthed.
([6]) Meddelelse fra Kommissionen Den blå vejledning om gennemførelse af EU's produktregler 2022 2022/C 247/01 (EUT C 247 af 29.6.2022, s. 1–152).

begrænsninger vedrørende fysisk produktion eller lager: hver handling, hvorved softwaren gøres tilgængelig med henblik på download eller distribution, resulterer i, at der oprettes en ny identisk kopi til brugeren. Så længe denne version af softwaren ikke ændres på en måde, der påvirker overholdelse af CRA, skal markedsføringen på EU-markedet anses for at have fundet sted på tidspunktet for det første tilbud med henblik på distribution eller anvendelse. Muligheden for efterfølgende download eller distribution af denne version af et softwareprodukt med digitale elementer skal derfor betragtes som et tilfælde, hvor softwareproduktet med digitale elementer gøres tilgængeligt ([7]).

14. Et enkeltstående softwareprodukt med digitale elementer bør derfor anses for at være bragt i omsætning, når dets fremstillingsfase er afsluttet, og den pågældende software første gang leveres med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed. Fabrikanten bør anses for at have bragt flere kopier af det samme softwareprodukt med digitale elementer i omsætning samtidigt. Selv om flere kopier af den samme software således fortsat er individuelle produkter med digitale elementer, anses de for at være bragt i omsætning samtidigt, uanset hvornår besiddelsen eller brugsretten til den enkelte kopi overdrages til en anden fysisk eller juridisk person. Samtidig gælder det, at når fabrikanten gør software tilgængelig i forskellige varianter, der adskiller sig med hensyn til inkluderede komponenter, konfigurationer eller aktiverede funktionaliteter (f.eks. builds til forskellige operativsystemer eller pakker med forskellige features), kan disse varianter ikke betragtes som kopier af det samme softwareprodukt med digitale elementer. De bør derfor behandles som særskilte produkter med digitale elementer med henblik på markedsføring.

Eksempel1: Den 1. januar 2028 leverer virksomhed A første gang version 1.0.0 af software X med henblik på distribution via virksomhedens websted. Samme dag køber kunde 1 en kopi af version 1.0.0 af software X. Den 15. januar 2028 køber kunde 2 en kopi af version 1.0.0 af software X. Begge kopier af version 1.0.0 af software X bringes i omsætning den 1. januar 2028.

15. På grund af softwareudviklingens iterative karakter bør det endvidere præciseres, at efterfølgende iterationer af et softwareprodukt med digitale elementer anses for at være bragt i omsætning på ny, når disse iterationer udgør en »væsentlig ændring« af et softwareprodukt med digitale elementer, der allerede er bragt i omsætning, som angivet i betragtning 41 i CRA. Iterationer, der ikke udgør væsentlige ændringer, kræver ikke, at fabrikanten gennemfører en ny overensstemmelsesvurderingsprocedure, og ændrer derfor ikke datoen for den pågældende softwares markedsføring. Yderligere vejledning om begrebet væsentlige ændringer findes i afsnit 4 *Væsentlige ændringer*.

Eksempel2: Den 1. januar 2028 leverer virksomhed A første gang version 1.0.0 af software X med henblik på distribution via sit websted. Samme dag køber kunde 1 en kopi af version 1.0.0 af software X. Den 15. januar 2028 frigiver virksomhed A en ajourført version 1.0.1 af software X, der ikke udgør en væsentlig ændring. Den 30. januar 2028 køber kunde 2 en kopi af version 1.0.1 af software X. Begge kopier af version 1.0.0 og 1.0.1 af software X anses for at være bragt i omsætning den 1. januar 2028.

16. Vejledningen i punkt 13, 14 og 15 finder udelukkende anvendelse under forudsætning af, at produktet med digitale elementer er enkeltstående software. Dette er f.eks. ikke tilfældet, når softwaren kombineres med hardware, som drøftet i afsnit *2.4 Kombination af hardware og software, der udgør* et produkt.

2.2. **Software som et produkt med digitale elementer**

17. I artikel 3, nr. 1), i CRA defineres et produkt med digitale elementer som »et software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der bringes i omsætning separat«. Sådanne produkter med digitale elementer er omfattet af CRA, hvis deres tilsigtede formål eller rimeligt forudsigelige anvendelse omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk.

([7]) I overensstemmelse med artikel 13, stk. 11, kan fabrikanter opretholde offentlige softwarearkiver, der forbedrer brugernes adgang til historiske versioner. I disse tilfælde skal brugerne på en lettilgængelig måde informeres klart om de risici, der er forbundet med brug af ikkeunderstøttet software.

18. CRA kan derfor omfatte en række produkter med digitale elementer, herunder: i) enkeltstående software såsom apps og computerprogrammer, uanset om de distribueres digitalt eller fysisk, ii) hardware med indlejret software (f.eks. enheder, der er forbundet til tingenes internet, bærbare computere og tablets), iii) enkeltstående hardware (f.eks. indbyggede kredsløb og bundkort) og iv) alle kombinationer af hardware og software, der leveres separat, men er beregnet til at fungere sammen.

19. Enkeltstående software er derfor omfattet af CRA, hvis den bringes i omsætning som et produkt med digitale elementer. Det er nyttigt at sondre mellem softwareprodukter med digitale elementer, der er omfattet af CRA, og fjernlevering af tjenester, der ikke er omfattet af CRA.

20. For at software kan være omfattet af CRA, skal et softwareprodukt med digitale elementer leveres til og erhverves af en bruger samt afvikles på eller som en del af et elektronisk informationssystem hos brugeren. Software, der downloades, installeres eller på anden måde leveres til brugeren, og som afvikles på brugerens elektroniske informationssystem, opfylder disse kriterier. Det gælder eksempelvis software i form af en browserudvidelse eller en applikation, der er udviklet ved hjælp af webteknologier, men leveres med henblik på lokal afvikling.

21. Derimod er software, der eksekveres på afstand og blot tilgås af brugeren, alene af den grund ikke et produkt med digitale elementer. I betragtning 11 og 12 i CRA foretages der da også denne sondring, idet det forklares, at ekstern behandling og lagring kun er omfattet af CRA, i det omfang det er nødvendigt for, at et produkt med digitale elementer kan udføre sine funktioner (dvs. gennem begrebet fjerndatabehandling som defineret i artikel 3, nr. 2), og ikke i sig selv udgør et produkt med digitale elementer. Dette er typisk tilfældet for webapplikationer, inklusive progressive webapps, som udelukkende tilgås via en webbrowser. Det samme gælder for websteder: selv om websteder i begrænset omfang teknisk set kan køre og afvikles på brugerens enhed, følger det af betragtning 12 i CRA, at websteder ikke i sig selv skal betragtes som produkter med digitale elementer og kun er omfattet af CRA, hvis de understøtter funktionaliteten i et produkt med digitale elementer, dvs. i det omfang de udgør fjerndatabehandling (som nærmere forklaret i afsnit *8* og navnlig *8.1.2 Ville fraværet af en sådan databehandling forhindre produktet med digitale elementer i at udføre en af funktionerne?*).

Eksempel 3: En mobilapplikation, som en bruger downloader fra en appbutik og installerer på sin smartphone, leveres til brugeren og eksekveres på brugerens enhed. Den er derfor et produkt med digitale elementer. Hvis den bringes i omsætning som led i en kommerciel aktivitet, kan den være omfattet af CRA.

Eksempel 4: En desktopapplikation, der er udviklet ved hjælp af webteknologier, men pakket med henblik på lokal installation, leveres til brugeren og afvikles på brugerens enhed. Den er derfor et produkt med digitale elementer. Hvis den bringes i omsætning som led i en kommerciel aktivitet, kan den være omfattet af CRA.

Eksempel 5: En webapplikation, som brugeren udelukkende tilgår via en webbrowser, er ikke et produkt med digitale elementer. Medmindre den understøtter funktionaliteten i et produkt med digitale elementer, er den ikke omfattet af CRA. I modsætning hertil er en applikation, der leveres til brugeren som en lokalt installeret klient, og som afvikles på brugerens enhed, et produkt med digitale elementer. Hvis den bringes i omsætning som led i en kommerciel aktivitet, kan den være omfattet af CRA.

Hvis denne klient for at udføre en eller flere funktioner er afhængig af fjerndatabehandling, der opfylder definitionen af fjerndatabehandling, er denne fjerndatabehandling også en del af produktet med digitale elementer.

Eksempel 6: Et websted, der blot præsenterer oplysninger for de besøgende og ikke understøtter funktionaliteten af et produkt med digitale elementer, er ikke i sig selv et produkt med digitale elementer. Det er derfor ikke omfattet af CRA.

2.3. **Computerkode**

22. Det er også nyttigt at præcisere, om kildekode kan udgøre et softwareprodukt med digitale elementer. I CRA defineres software som »den del af et elektronisk informationssystem, der består af computerkode« (artikel 3, nr. 4)). Computerkode kan tage form af i) maskinkode, som er det sæt instruktioner, der afvikles direkte af en computers processor, og som er skrevet i binært format, eller ii) kildekode, dvs. det sæt instruktioner og programsætninger, der er skrevet i et programmeringssprog, og som skal kompileres eller fortolkes for at kunne udføres af en computer. Definitionen af software i CRA omfatter begge former.

23. Et særskilt spørgsmål er, om en given mængde computerkode indebærer, at et produkt med digitale elementer bringes i omsætning på EU-markedet, hvilket forudsætter en levering som led i en kommerciel aktivitet. Dette er ofte ikke tilfældet for kildekode. For eksempel anses en fysisk eller juridisk person, der deler fri og open source-computerkode i offentligt tilgængelige repositories, for så vidt angår CRA generelt ikke for at bringe denne kode i omsætning på EU-markedet (som drøftet nærmere i afsnit *3 Fri og open source-software*). Ufærdig kode, der deles i design- og udviklingsfasen for et produkt med digitale elementer (f.eks. med henblik på test eller review), anses for så vidt angår CRA heller ikke for at være bragt i omsætning, da fremstillingsfasen ikke er afsluttet. På samme måde anses sample eller demokode, der leveres som en del af vejledninger eller undervisningsmateriale, for så vidt angår CRA heller ikke for at være bragt i omsætning ([8]).

24. Derimod anses denne kode for at være bragt i omsætning, når en fabrikant forsyner kunderne med computerkode som et produkt med digitale elementer, uanset om der er tale om maskinkode eller kildekode ([9]).

Eksempel 7: Virksomhed A licenserer kildekode til virksomhed B til en intern platform, der kan tilpasses, og leverer denne kildekode i en tekstfil. Selv hvis denne kildekode kræver yderligere tilpasning og kompilering hos virksomhed B, inden den anvendes, bringer virksomhed A denne kildekode i omsætning og er derfor omfattet af CRA. Virksomhed A er ikke ansvarlig for, at virksomhed B's efterfølgende tilpasninger og kompilering af denne kode overholder CRA.

2.4. **Kombination af hardware og software, der udgør et produkt med digitale elementer**

25. Hvorvidt software indgår i et produkt med digitale elementer, bør ikke afgøres ud fra, hvordan eller hvornår denne software leveres til brugeren, men ud fra, om softwaren på baggrund af produktets tilsigtede formål og anvendelse, der med rimelighed kan forudses, er nødvendig for, at produktet med digitale elementer kan udføre de tilsigtede funktioner. Hvis et hardwareprodukt med digitale elementer er designet til at fungere sammen med en bestemt software, der leveres af samme fabrikant for at kunne udføre de tilsigtede funktioner, udgør denne hardware og denne software tilsammen produktet med digitale elementer. Software, der er nødvendig for at betjene, konfigurere, styre eller anvende et produkt med digitale elementer i overensstemmelse med det tilsigtede formål, er derfor en del af produktet med digitale elementer, selv om den fås gennem en særskilt kanal (f.eks. en appbutik, et downloadlink eller en anden digital kanal, efter at hardwareproduktet med digitale elementer er blevet bragt i omsætning). Softwaren bringes således i omsætning på samme tidspunkt, som hardwareenhederne med digitale elementer bringes i omsætning.

Eksempel 8: En netværksprinter bringes i omsætning som et hardwareprodukt med digitale elementer, mens de softwaredrivere, der er nødvendige for at sende udskriftsjob, konfigurere enheden og administrere dens drift, gøres tilgængelige til download fra fabrikantens websted. Selv om printeren og driverne leveres via forskellige kanaler, udgør de tilsammen ét enkelt produkt med digitale elementer, fordi printeren ikke kan opfylde det tilsigtede formål uden driverne.

Eksempel 9: Et sportsur bringes i omsætning med henblik på at måle en brugers hjertefrekvens og aktivitet, mens en smartphoneapplikation, der leveres af fabrikanten, er nødvendig for at vise målingerne og historikken og gøre det muligt at konfigurere enheden. Selv om applikationen downloades separat gennem en appbutik, udgør enheden og applikationen tilsammen ét enkelt produkt med digitale elementer, fordi de er udformet og beregnet til at fungere sammen for at levere funktionaliteten i produktet med digitale elementer.

([8]) Det bør også erindres, at artikel 4, stk. 3, giver fabrikanter mulighed for at gøre ufærdig software, der ikke overholder forordningen, såsom alfaversioner, betaversioner eller release candidates, tilgængelig på markedet, forudsat at den ufærdige software kun gøres tilgængelig i det tidsrum, der er nødvendigt for at teste den og indsamle feedback.

([9]) På den anden side bør det bemærkes, at computerkode i sig selv ikke udgør et produkt inden for produktansvarsretten, og at fabrikanter, der bringer sådan kode i omsætning, derfor ikke kan holdes ansvarlige i henhold til direktiv (EU) 2024/2853 (produktansvarsdirektivet). I betragtning 13 til nævnte direktiv anføres det, at »oplysninger bør imidlertid ikke betragtes som et produkt, og produktansvarsreglerne bør derfor ikke finde anvendelse på indholdet af digitale filer såsom mediefiler eller e-bøger eller blot kildekoden for software«. Dette udelukker ikke, at fabrikanter kan ifalde ansvar efter national erstatningsret.

2.5. **Dataforbindelse**

26. I artikel 2, stk. 1, anføres det, at CRA »finder anvendelse på produkter med digitale elementer, der gøres tilgængelige på markedet, hvis tilsigtede formål eller rimeligt forudsigelige anvendelse omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk.« Anvendelsesområdet for CRA defineres således ikke ved den blotte tilstedeværelse af elektronik, men ved det pågældende produkt med digitale elementers evne til at udveksle digitale oplysninger.

27. Begreberne »logisk forbindelse« og »fysisk forbindelse« er defineret i artikel 3, men CRA indeholder ingen definition af »dataforbindelse« eller »digitale data«. Det er derfor nyttigt at fastlægge en fortolkning af, hvad en dataforbindelse er, med henblik på at præcisere afgrænsningen af anvendelsesområdet for CRA. Denne afgrænsning er særligt vigtig for at skelne mellem produkter med digitale elementer, der blot anvender elektriske signaler, og produkter med digitale elementer, der indgår i en digital kommunikation og derfor er eksponeret for cybersikkerhedsrisici.

28. På det mest grundlæggende niveau indebærer en dataforbindelse overførsel af information i binær form, dvs. som en sekvens af 0'er og 1-taller. Det forhold, at en udgang blot slås til og fra (dvs. 0/1), udgør ikke i sig selv en dataforbindelse, hvis disse tilstande ikke er beregnet til at repræsentere data eller ikke aflæses af en digital indgang. For at der kan foreligge en dataforbindelse, skal de binære tilstande bevidst være kodet som information af en kilde og kunne afkodes som information hos modtageren. Der skal med andre ord være en afsender, som bevidst genererer digitale symboler efter et fastlagt system, og en modtager, som kan fortolke disse symboler som data. Hvis elektriske eller elektroniske signaler udelukkende anvendes til at aktivere eller drive en funktion uden at overføre digitalt kodet information, foreligger der ikke en dataforbindelse i CRA's forstand, og produktet med digitale elementer falder derfor ikke ind under anvendelsesområdet for artikel 2, stk. 1.

2.6. **Komplekse systemer**

29. Produkter med digitale elementer, der er omfattet af anvendelsesområdet for CRA, kan både bestå af enkeltstående enheder eller softwarekomponenter og af komplekse systemer, herunder systemer, der består af flere hardware- og softwareelementer, som fungerer sammen for at udføre en bestemt funktion. Hvis et sådant system bringes i omsætning som ét enkelt produkt med digitale elementer, udgør det et produkt med digitale elementer som beskrevet i CRA.

30. Sådanne komplekse systemer er ofte kendetegnet ved lange konstruktions- og udviklingscyklusser, kontrakter, der kan være underskrevet, inden CRA finder anvendelse, lange driftslevetider og en høj grad af teknisk og organisatorisk kompleksitet. Sådanne systemer, der skal bringes i omsætning, efter at CRA finder anvendelse, kan basere sig på komponenter, der er bragt i omsætning, inden CRA fandt anvendelse, på etablerede arkitekturer eller på udbredte interoperabilitetsstandarder, herunder standarder, der er omhandlet i anden EU-lovgivning eller er omfattet af sektorspecifikke rammer. Som følge heraf kan visse tekniske egenskaber ved disse systemer være vanskelige eller uforholdsmæssigt byrdefulde at ændre uden at påvirke det tilsigtede formål, sikkerhed, pålidelighed eller interoperabilitet med eksisterende infrastruktur.

31. Disse egenskaber alene udelukker ikke komplekse systemer fra anvendelsesområdet for CRA. De illustrerer snarere den risikobaserede tilgang i CRA, som gør det muligt at påvise overholdelse på forskellige måder afhængigt af produktet med digitale elementers egenskaber og begrænsninger, i overensstemmelse med artikel 13, stk. 3, i CRA. Disse egenskaber indgår i systemets tilsigtede formål og driftskontekst og er derfor relevante ved vurderingen af overensstemmelsen med de væsentlige cybersikkerhedskrav (de »væsentlige krav«). Navnlig anerkendes det udtrykkeligt i betragtning 55, at visse væsentlige krav muligvis ikke er fuldt forenelige med arten af et produkt med digitale elementer. Dette kan f.eks. være tilfældet, hvis overholdelse ville underminere obligatoriske interoperabilitetskrav eller systemets korrekte funktion.

32. Fabrikanterne skal derfor håndtere cybersikkerhedsrisici på grundlag af den cybersikkerhedsrisikovurdering, der er omhandlet i artikel 13, stk. 2. Som det også forklares i betragtning 55, finder specifikke væsentlige krav i nogle tilfælde ikke anvendelse eller kan ikke opfyldes ved gennemførelse af sikkerhedsforanstaltninger på det aktuelle

tekniske niveau, f.eks. på grund af systemets tilsigtede formål, som kræver, at produktet med digitale elementer interagerer med eksisterende afhængigheder eller overholder visse interoperabilitetskrav. I sådanne tilfælde bør fabrikanterne identificere og dokumentere disse specifikke begrænsninger, vurdere de tilknyttede risici og gennemføre passende alternative eller kompenserende risikobegrænsende foranstaltninger for ikke at underminere sikkerheden i produktet med digitale elementer. Til disse formål spiller både den tekniske dokumentation, der er omhandlet i artikel 31, og de oplysninger og instruktioner til brugeren, der er omhandlet i bilag II, en central rolle med hensyn til på gennemsigtig vis at beskrive de identificerede begrænsninger, de tilknyttede cybersikkerhedsrisici og de gennemførte risikobegrænsende foranstaltninger. I overensstemmelse med forpligtelsen til at holde risikovurderingen ajour i vedligeholdelsesperioden bør fabrikanterne også regelmæssigt revurdere, om sådanne begrænsninger fortsat består. Hvis sådanne begrænsninger kan ophæves eller reduceres over tid, bør fabrikanterne ajourføre produktet med digitale elementer i overensstemmelse hermed, så det kan opnå et passende cybersikkerhedsniveau ([10]).

Eksempel 10: En fabrikant bringer et produkt med digitale elementer i omsætning, der kommunikerer med eksterne systemer ved hjælp af en netværksprotokol. Som led i anvendelsen af de væsentlige krav fastslår fabrikanten på grundlag af cybersikkerhedsrisikovurderingen, at det er nødvendigt at anvende en sikker kommunikationsprotokol for at sikre fortroligheden og integriteten af de data, som produktet med digitale elementer udveksler.

Det tilsigtede formål omfatter imidlertid interoperabilitet med eksisterende systemer, der kun understøtter en ældre eller mindre sikker protokol. I sådanne tilfælde kan fabrikanten implementere denne protokol, hvis det er nødvendigt for at opnå interoperabilitet, forudsat at de tilknyttede cybersikkerhedsrisici identificeres og afbødes på anden måde.

Hvis det er teknisk muligt for produktet med digitale elementer at understøtte både den sikre protokol og den mindre sikre protokol, forventes fabrikanten at implementere den sikre protokol og aktivere brugen af den som standard. Den mindre sikre protokol bør kun være tilladt, hvor det er nødvendigt af hensyn til interoperabilitet.

Eksempel 11: En fabrikant af et industrielt automatiseringssystem køber nogle mikrocontrollere, inden CRA finder anvendelse. Fabrikanten foretager cybersikkerhedsrisikovurderingen for sit industrielle automatiseringssystem, der skal bringes i omsætning, efter at CRA finder anvendelse. På grundlag af denne cybersikkerhedsrisikovurdering identificerer fabrikanten ikke specifikke cybersikkerhedsrisici forbundet med anvendelsen af en af disse mikrocontrollere. Fabrikanten integrerer mikrocontrolleren i sit industrielle automatiseringssystem og sikrer, at produktet med digitale elementer som helhed (det industrielle automatiseringssystem) opfylder de væsentlige krav.

2.7. **Produkter med digitale elementer, der er udformet før CRA begyndte at finde anvendelse**

33. I visse tilfælde bringer en fabrikant, efter at CRA begynder at finde anvendelse den 11. december 2027, enheder af et produkt med digitale elementer i omsætning, som er fremstillet i overensstemmelse med en type eller model, der er udformet og udviklet før anvendelsesdatoen for CRA. I sådanne tilfælde kræver overensstemmelse med denne forordning ikke nødvendigvis, at disse enheder af produktet med digitale elementer udformes på ny. Fabrikanten skal foretage en cybersikkerhedsrisikovurdering i overensstemmelse med artikel 13, stk. 2, i CRA for på grundlag af det tilsigtede formål med og den rimeligt forudsigelige brug af produktet med digitale elementers at fastslå, hvilke af de væsentlige krav i bilag I, del I, der finder anvendelse på det pågældende produkt med digitale elementer, og hvordan disse krav gennemføres.

34. Hvis resultatet af denne risikovurdering viser, at produktet med digitale elementer allerede indeholder hensigtsmæssige og effektive sikkerhedsforanstaltninger, der imødegår de relevante risici, kan fabrikanten basere sig på disse eksisterende foranstaltninger for at påvise overensstemmelse med CRA. CRA alene pålægger ikke en forpligtelse til at indføre nye sikkerhedsfeatures eller til at udforme produktet med digitale elementer på ny, hvis dette ikke er nødvendigt for at imødegå de identificerede risici.

([10]) Det bør bemærkes, at betragtningerne i dette afsnit efter omstændighederne kan finde anvendelse på alle produkter med digitale elementer, der er omfattet af CRA, og ikke kun på »komplekse systemer«.

35. Fabrikanten er ikke desto mindre fortsat underlagt de forpligtelser, der er fastsat i CRA. Disse omfatter at sikre, at den relevante overensstemmelsesvurderingsprocedure er blevet gennemført, EU-overensstemmelseserklæringen er blevet udarbejdet og CE-mærkningen anbragt, inden produktet med digitale elementer bringes i omsætning. Overholdelsen af disse krav afhænger ikke af, om udformningen af produktet med digitale elementer skulle ændres som følge af risikovurderingen. For produkter med digitale elementer, der er udformet før anvendelsesdatoen for CRA, men som bringes i omsætning efter denne dato, bør forpligtelsen i artikel 13, stk. 2, i tilfælde, hvor det ikke er muligt for fabrikanten at påvise, hvordan der er taget hensyn til risikovurderingen under udformningen og udviklingen af produktet med digitale elementer, forstås således, at den indebærer krav om, at fabrikanter foretager en cybersikkerhedsrisikovurdering og på dette grundlag påviser, at produktet med digitale elementer indeholder passende sikkerhedsforanstaltninger med henblik på at minimere cybersikkerhedsrisici, forebygge hændelser og minimere deres indvirkning, herunder i forbindelse med brugernes sundhed og sikkerhed.

36. Produkter med digitale elementer, der er udformet før CRA begyndte at finde anvendelse, kan derfor bringes i omsætning i henhold til CRA uden at blive udformet på ny, forudsat at fabrikanten gennem cybersikkerhedsrisikovurderingen og den tekniske dokumentation kan påvise, at produktet med digitale elementer opnår et passende cybersikkerhedsniveau i lyset af det tilsigtede formål og den rimeligt forudsigelige anvendelse og opfylder de væsentlige cybersikkerhedskrav.

37. Endvidere er det nyttigt at præcisere anvendelsen af overensstemmelsesvurderingsforpligtelserne for fabrikanter af produkter med digitale elementer, der bringes i omsætning, efter at CRA begynder at finde anvendelse, men er fremstillet i overensstemmelse med en type eller model, der er udformet og udviklet før denne dato. I overensstemmelse med artikel 13, stk. 12, skal fabrikanten ved hjælp af den relevante overensstemmelsesvurderingsprocedure påvise, at fabrikantens produkt med digitale elementer er i overensstemmelse med de gældende væsentlige krav, og medtage dokumentation herfor i produktets tekniske dokumentation (bilag VII, punkt 6).

38. Anvendelsen af sådanne krav skal imidlertid fortolkes i lyset af cybersikkerhedsrisikovurderingen og cybersikkerhedsrisikoprofilen for produktet med digitale elementer. Navnlig for produkter med digitale elementer, der er udformet før anvendelsesdatoen for CRA, (men som bringes i omsætning efter denne dato), og som er omfattet af procedurerne for overensstemmelsesvurdering i artikel 32, stk. 1, bør forpligtelsen til at fremlægge dokumentation som led i overensstemmelsesvurderingsproceduren, hvis risikovurderingen viser, at produktet med digitale elementer allerede indeholder hensigtsmæssige og effektive sikkerhedsforanstaltninger, der imødegår det pågældende produkts risici, ikke forstås således, at den kræver, at fabrikanten fremlægger testresultater, der omfatter de oprindelige faser for udformning og udvikling af sådanne produkter med digitale elementer. Dette ville ikke være nødvendigt, da det ikke ville bidrage til at øge sikkerheden for selve produktet med digitale elementer. Hvis test ikke desto mindre kan være nødvendige, forventes fabrikanter ikke at fremlægge dokumentation for test udført på alle produktvarianter, men kan samle sådanne test på tværs af produktfamilier, som nærmere behandlet i afsnit *7.4 Genbrug af risikovurderinger og overensstemmelsesdokumentation for familier af produkter med digitale elementer*.

39. Ikke desto mindre bør fabrikanten fremlægge dokumentation for, hvordan fabrikanten overholder de processer for håndtering af sårbarheder, der er fastsat i bilag I, del II. Fabrikanten bør også holde sin risikovurdering ajour i overensstemmelse med artikel 13, stk. 3, og opfylde alle andre forpligtelser, der er fastsat i CRA, herunder ved at give brugerne oplysninger og instruktioner i overensstemmelse med artikel 13, stk. 18.

Eksempel 12: En fabrikant bringer en mikrocontroller, der er udformet og udviklet før anvendelsesdatoen for CRA, i omsætning. Mikrocontrolleren er beregnet til at blive integreret i en række elektroniske produkter med digitale elementer, herunder produkter med digitale elementer, der har konnektivitetsfunktioner.

Inden fabrikanten bringer nye enheder af mikrocontrolleren i omsætning, efter at CRA finder anvendelse, foretager fabrikanten en cybersikkerhedsrisikovurdering i overensstemmelse med artikel 13, stk. 2. På grundlag af mikrocontrollerens tilsigtede formål og dens rimeligt forudsigelige anvendelse identificerer fabrikanten relevante cybersikkerhedsrisici såsom uautoriseret adgang, manipulation af software eller data og misbrug af tilgængelige grænseflader.

Resultatet af risikovurderingen viser, at mikrocontrolleren i den oprindelige udformning allerede indeholder hensigtsmæssige og effektive sikkerhedsforanstaltninger, der imødegår de identificerede risici. Fabrikanten konkluderer derfor, at produktet med digitale elementer opfylder de relevante væsentlige krav i bilag I, del I, og at det ikke er nødvendigt at udforme det på ny eller indføre yderligere sikkerhedsfunktioner.

Hvis det ikke er muligt at påvise, hvordan der blev taget højde for en cybersikkerhedsrisikovurdering i den oprindelige udformnings- og udviklingsfase, dokumenterer fabrikanten en aktuel cybersikkerhedsrisikovurdering og forklarer, hvordan den eksisterende udformning og de eksisterende foranstaltninger afbøder de identificerede risici. Fabrikanten er ikke forpligtet til at genskabe historisk udformnings- eller testdokumentation, da dette ikke ville bidrage til at styrke cybersikkerheden i produktet med digitale elementer. Hvis flere varianter af mikrocontrolleren er baseret på samme udformning og har samme cybersikkerhedsrisikoprofil, kan fabrikanten også basere sig på repræsentativ dokumentation, der dækker den relevante produktfamilie.

Fabrikanten sikrer også overholdelse af de krav til håndtering af sårbarheder, der er fastsat i bilag I, del II, herunder ved at opretholde processer til at håndtere og afhjælpe sårbarheder og ved at holde cybersikkerhedsrisikovurderingen under løbende revision i overensstemmelse med artikel 13, stk. 3.

Under disse omstændigheder kan den mikrocontroller, der er udformet før anvendelsesdatoen for CRA, bringes i omsætning uden at blive udformet på ny, forudsat at fabrikanten gennem cybersikkerhedsrisikovurderingen og den tekniske dokumentation kan påvise, at den opnår et passende cybersikkerhedsniveau på baggrund af det tilsigtede formål og den rimeligt forudsigelige anvendelse og opfylder de gældende væsentlige krav.

3. **FRI OG OPEN SOURCE-SOFTWARE**

40. Som anført i afsnit *2.1 Markedsføring* finder CRA anvendelse på produkter med digitale elementer, når de gøres tilgængelige på EU-markedet som led i erhvervsvirksomhed første gang (dvs. »bringes i omsætning«), samt på efterfølgende tilfælde af tilgængeliggørelse på markedet af det samme produkt med digitale elementer. Den blå vejledning (afsnit 2.2) præciserer, at »erhvervsvirksomhed« skal forstås som levering af varer mod betaling eller gratis i en forretningsmæssig sammenhæng og kun kan vurderes i hvert enkelt tilfælde under hensyntagen til leveringernes regelmæssighed, produktets egenskaber, leverandørens hensigter osv.

41. Levering som led i erhvervsvirksomhed er kendetegnet ved en række omstændigheder, som er udførligt dokumenteret i den blå vejledning og omtalt i betragtning 15 i CRA. Dette kan omfatte direkte opkrævning af en pris samt »opkrævning af en pris for tekniske supporttjenester, hvor dette ikke blot tjener til dækning af de reelle omkostninger, ved et formål om at tjene penge, f.eks. ved tilrådighedsstillelse af en softwareplatform, hvorigennem fabrikanten tjener penge på andre tjenester, ved at kræve behandling af personoplysninger til andre formål end blot at forbedre softwarens sikkerhed, kompatibilitet eller interoperabilitet som forudsætning for anvendelsen, eller ved at modtage donationer, der overstiger de omkostninger, der er forbundet med design, udvikling og levering af et produkt med digitale elementer« (betragtning 15) ([11]).

42. CRA indeholder dog en anerkendelse af de særlige forhold ved de forskellige måder at udvikle og offentliggøre »fri og open source-software« (FOSS) på og indeholder en vejledning, der kan bidrage til at fastslå, om FOSS er et produkt med digitale elementer, der bringes i omsætning (dvs. som led i erhvervsvirksomhed), som omhandlet i CRA. Følgende fremgår af betragtning 18: »De omstændigheder, hvorunder produktet er blevet udviklet, eller hvordan udviklingen er blevet finansieret, bør derfor ikke i sig selv tages i betragtning ved fastlæggelsen af den pågældende aktivitets kommercielle eller ikkekommercielle karakter. Mere specifikt bør levering af produkter med digitale elementer, der kan betegnes som fri og open source-software, som fabrikanterne ikke tjener penge på, ikke anses som værende erhvervsvirksomhed [...] for at sikre, at der skelnes klart mellem udviklings- og leveringsfaserne.«

([11]) Det bør også erindres, at selv om der ofte (også) tjenes penge på produkter med digitale elementer via behandling af personoplysninger, er beskyttelse af personoplysninger en grundlæggende rettighed, og personoplysninger kan derfor ikke betragtes som en handelsvare, som anført i betragtning 24 til Europa-Parlamentets og Rådets direktiv (EU) 2019/770 af 20. maj 2019 om visse aspekter af aftaler om levering af digitalt indhold og digitale tjenester, EUT L 136 af 22.5.2019, s. 1-27, ELI: http://data.europa.eu/eli/dir/2019/770/oj.

43. Det er derfor nyttigt i) at præcisere, hvad FOSS er, ii) hvornår det anses for at henhøre under en fysisk eller juridisk persons ansvar og iii) at give eksempler, der kan hjælpe interessenter med at forstå, hvornår distribution af FOSS udgør en markedsføring. Hvis FOSS ikke bringes i omsætning, falder den uden for anvendelsesområdet for CRA, medmindre den enhed, der offentliggør den, er en juridisk person, der opfylder definitionen af »open source-softwareforvalter« (i det følgende benævnt »forvalter«) i artikel 3, nr. 14). I så fald er den kun underlagt de forpligtelser, der er fastsat i artikel 24.

44. I artikel 3, nr. 48), defineres FOSS som »software, hvis kildekode deles åbent, og som stilles til rådighed under en fri og open source-licens, der giver samtlige rettigheder til, at den kan deles åbent og er frit tilgængelig, anvendelig, modificerbar og redistribuerbar«. Selv om specifikke fri og open source-licenser, der er forenelige med definitionen i artikel 3, nr. 48), ikke defineres i denne vejledning, følger det af ordlyden af denne bestemmelse, at kun software, der kumulativt opfylder to betingelser, kan betegnes som FOSS for så vidt angår CRA: i) softwaren skal stilles til rådighed under en fri og open source-licens, der giver alle de rettigheder, der er omhandlet i artikel 3, nr. 48), og ii) softwarens kildekode skal deles åbent.

45. Kravet om, at licensen skal foreskrive, at softwaren er »frit tilgængelig, anvendelig, modificerbar og redistribuerbar«, afspejler den traditionelle forståelse af FOSS, nemlig at brugerne skal kunne tilgå kildekoden, bruge den uden unødige begrænsninger, ændre den og redistribuere originale eller ændrede versioner. Adgang til kildekoden er derfor en nødvendig forudsætning for at kunne udøve de øvrige rettigheder: Uden adgang til kildekoden er det i praksis ikke muligt at ændre eller genbruge softwaren på en meningsfuld måde.

46. Artikel 3, nr. 48), går imidlertid videre end blot til at henvise til licensvilkårene, idet det udtrykkeligt kræves, at kildekoden »deles åbent«. Begrebet »deles åbent« angiver, at kildekoden skal gøres offentligt tilgængelig (enten »upstream« eller »downstream«) og ikke blot stilles til rådighed på et begrænset eller betinget grundlag. Software, der distribueres under en fri og open source-licens, men hvis kildekode kun deles (eller må deles) med betalende kunder eller en begrænset gruppe brugere, skal derfor ikke anses for at være FOSS som defineret i artikel 3, nr. 48). For så vidt angår CRA bør kun software, hvis kildekode er offentligt tilgængelig og licenseret under en fri og open source-licens, der giver alle de rettigheder, der er omhandlet i artikel 3, nr. 48), derfor kunne betegnes som FOSS.

3.1. **Fastlæggelse af, om fri og open source-software hører under en persons ansvar**

47. CRA pålægger økonomiske aktører, der leverer produkter med digitale elementer på EU-markedet, centrale ansvarsområder. I forordningen defineres fabrikanten som den fysiske eller juridiske person, der leverer et produkt med digitale elementer under sit navn eller varemærke, og som gør dette som led i erhvervsvirksomhed (og derved bringer det i omsætning). Tilsvarende er en importør den fysiske eller juridiske person, der er etableret i EU, og som leverer et produkt med digitale elementer fra en person, der er etableret uden for EU, og som gør dette som led i erhvervsvirksomhed (og derved bringer det i omsætning). Forpligtelserne for open source-softwareforvaltere gælder for den juridiske person, der leverer FOSS beregnet til kommercielle aktiviteter ([12]), men ikke bringer den i omsætning som omhandlet i CRA.

48. For at afgøre, om en fysisk eller juridisk person bringer FOSS i omsætning på EU-markedet, skal det derfor først afklares, om den pågældende fysiske eller juridiske person faktisk leverer FOSS. For korrekt at fastlægge de gældende forpligtelser i henhold til CRA er det afgørende at fastslå, om den fysiske eller juridiske person faktisk foretager leveringen af FOSS. Som anført i betragtning 18 finder CRA således ikke anvendelse på fysiske eller juridiske personer, der bidrager med kildekode til produkter med digitale elementer, der kan betegnes som FOSS, som ikke er under deres ansvar.

([12]) Dette er en nødvendig, men ikke tilstrækkelig, betingelse for, at en juridisk person kan betegnes som open source-softwareforvalter, da definitionen i artikel 3, nr. 14), fastsætter yderligere betingelser for, at en juridisk person kan betegnes som forvalter.

49. På baggrund af de særlige forhold ved udviklingen af FOSS, som ofte involverer mange bidragydere, decentraliserede samarbejdsmodeller og en adskillelse mellem bidrag og beslutningstagning, er det nyttigt at præcisere, at ansvaret for FOSS anses for at påhvile de fysiske eller juridiske personer, der offentliggør FOSS og udøver primær kontrol over dens udvikling, udgivelser og beslutninger om distribution (ofte benævnt »reparatører«). Personer, der bidrager med kildekode, men ikke kontrollerer udgivelser, køreplaner eller styringsbeslutninger, anses for »bidragydere«, i sådanne tilfælde er FOSS ikke under deres ansvar, selv om de har bidraget med kode til den. Den blotte tilstedeværelse af tekniske tilladelser, såsom commit-adgang, er ikke tilstrækkelig til at fastslå, at FOSS er under den pågældende persons ansvar; ansvaret ligger hos dem, der offentliggør og kontrollerer FOSS.

Eksempel13: En individuel udvikler eller en medarbejder i en virksomhed indsender en »pull request« eller »merge request« til et FOSS-projekt med en sikkerhedsrettelse eller en ny funktion. Projektets reparatører gennemgår og accepterer bidraget og indarbejder koden i det primære repository, hvorefter den medtages i en ny version. I dette tilfælde er den person, der indsendte anmodningen, en »bidragyder« og ikke omfattet af CRA. Selv om personen har bidraget med kildekode, udøver vedkommende ikke den primære kontrol over udviklingen eller over beslutninger om versionsudgivelser eller distribution.

3.2. **Fastlæggelse af, om fri og open source-software bringes i omsætning på EU-markedet**

50. Når det er fastslået, at en FOSS er under en fysisk eller juridisk persons ansvar, skal det fastslås, om denne person leverer den som led i erhvervsvirksomhed og dermed bringer den i omsætning.

3.2.1. *Opkrævning af en pris*

51. Hvis den fysiske eller juridiske person, der leverer en FOSS, opkræver en pris for selve softwaren (f.eks. ved at opkræve et beløb for færdigkompilerede binære filer/programmer), bringer denne person et produkt med digitale elementer i omsætning. Den person, der bringer en FOSS i omsætning, er derfor fabrikant i henhold til CRA.

52. Fabrikanter af FOSS leverer ofte gratis versioner af denne software (ofte kaldet »community versions«), hvis kodebase er (næsten) identisk med den betalte version. Disse produkter med digitale elementer er imidlertid forskellige produkter: Der tjenes penge på den betalte version (f.eks. enten ved opkrævning af en pris eller på anden vis som omhandlet i dette afsnit), og den anses derfor for at være bragt i omsætning, hvilket udløser fabrikantens forpligtelser. Der tjenes ikke penge på den version, der leveres gratis (eller communityversionen), og den anses derfor ikke for at være bragt i omsætning for så vidt angår CRA. Dette er også tilfældet, hvor den betalte version er en »udvidet« version henvendt til erhverv med udvidet kodebase i forhold til den version, der leveres gratis, eller denne version integreres i et bredere produkt med digitale elementer (f.eks. som i tilfældet med »open-core«-modellen).

53. Hvis den person, der leverer communityversionen, er en juridisk person, er denne juridiske person også omfattet af forpligtelserne for forvaltere for den version, som den leverer gratis (communityversionen). Hvis enheden er en fysisk person, er den version, der leveres gratis (communityversionen), ikke omfattet af anvendelsesområdet for CRA.

3.2.2. *Indtjening på andre tjenester eller krav om behandling af personoplysninger*

54. En fysisk eller juridisk person, der offentliggør en FOSS, kan også bringe den i omsætning (dvs. levere den som led i erhvervsvirksomhed), hvis personen leverer softwaren, hvorigennem vedkommende tjener penge på andre produkter med digitale elementer eller tjenester, eller hvis personen som betingelse for anvendelse kræver behandling af personoplysninger af andre grunde end udelukkende at forbedre softwarens sikkerhed, kompatibilitet eller interoperabilitet.

Eksempel 14: En fysisk eller juridisk person offentliggør en fri og open source-markedspladsapplikation. Applikationen er gratis tilgængelig og gør det muligt for brugere at købe varer eller tjenesteydelser gennem den. Appen gør det muligt for den person, der offentliggjorde den, at tjene penge på andre produkter med digitale elementer og tjenester, der udbydes gennem den (f.eks. gennem reklamer, provisionsgebyrer eller abonnementsgebyrer). Applikationen anses derfor for at være bragt i omsætning som led i erhvervsvirksomhed.

Eksempel 15: En fysisk eller juridisk person offentliggør en fri og open source-VPN. Applikationen er gratis tilgængelig, men den gør det muligt for brugerne at betale for adgang til yderligere servere eller dedikerede IP-adresser. Applikationen gør det muligt for personen at tjene penge på andre tjenester, der udbydes gennem applikationen, og den anses derfor for at være bragt i omsætning som led i erhvervsvirksomhed.

Eksempel 16: En fysisk eller juridisk person offentliggør en fri og open source-applikation til fitness- eller aktivitetsmåling. Applikationen er gratis tilgængelig, men anvendelsen af den er betinget af behandling af brugernes personoplysninger til formål såsom målrettet reklame eller analyse, der ikke vedrører softwarens sikkerhed, kompatibilitet eller interoperabilitet. Ved at kræve sådan databehandling som betingelse for anvendelse anses applikationen derfor for at være bragt i omsætning som led i erhvervsvirksomhed.

3.2.3. *Støttetjenester*

55. Det forhold, at en fysisk eller juridisk person, der offentliggør en FOSS, også tilbyder betalte støttetjenester vedrørende den pågældende FOSS, betyder ikke i sig selv, at produktet med digitale elementer leveres som led i erhvervsvirksomhed. Støttetjenester kan omfatte aktiviteter såsom rådgivning, uddannelse eller professionelle tjenesteydelser vedrørende kundens brug af, dokumentation for, konfiguration og udrulning af softwaren.

56. Det afgørende er, om adgangen til en FOSS (dvs. leveringen af produktet med digitale elementer), herunder vedligeholdelse heraf, er betinget af vederlag, snarere end blot tilbuddet om professionelle tjenesteydelser omkring et frit tilgængeligt produkt med digitale elementer, jf. betragtning 18 til CRA (»bør levering af produkter med digitale elementer, der kan betegnes som fri og open source-software, som fabrikanterne ikke tjener penge på, ikke anses som værende erhvervsvirksomhed«). Hvis en FOSS frit kan downloades og installeres, og brugerne kan vælge at købe professionelle tjenesteydelser særskilt, anses den pågældende FOSS ikke for at være bragt i omsætning.

57. Derimod er adgangen til en specifik version af produktet med digitale elementer, herunder visse ydelser såsom teknisk bistand eller optimering af ydeevne, i nogle tilfælde betinget af vederlag. I sådanne tilfælde udgør dette en levering af et produkt med digitale elementer, der tjenes penge på, og som leveres som led i erhvervsvirksomhed, og produktet anses derfor for at være bragt i omsætning. Dette omfatter tilfælde, hvor en betalt udgave eller virksomhedsversion gøres tilgængelig i henhold til en kommerciel aftale, uanset om funktionelt tilsvarende software også er gratis tilgængelig under en fri og open source-licens.

Eksempel 17: En fysisk eller juridisk person offentliggør et fri og open source-operativsystem og tilbyder en betalt version af dette operativsystem, som omfatter støttetjenester såsom teknisk bistand eller optimering af ydeevne. Den betalte version af operativsystemet anses for at være bragt i omsætning som led i erhvervsvirksomhed.

Eksempel 18: En fysisk eller juridisk person offentliggør et fri og open source-kommandolinjeværktøj. Værktøjet er frit tilgængeligt, og enhver kan downloade og installere det. Den fysiske eller juridiske person tilbyder særskilt professionelle tjenesteydelser, såsom valgfrie konsulentydelser, til at oplære brugerne og støtte dem i at installere og bruge værktøjet. Den pågældende FOSS anses ikke for at være bragt i omsætning som omhandlet i CRA.

58. Navnlig for fysiske personer, der offentliggør FOSS, vil tilbud om teknisk bistand, der indgår i en pakke kombineret med adgang til produktet med digitale elementer, fortsat ikke blive betragtet som erhvervsvirksomhed, hvis den opkrævede pris, som anført i betragtning 15 til CRA, kun tjener til dækning af de faktiske omkostninger. De faktiske omkostninger omfatter en række omkostninger vedrørende den pågældende softwares udformning, udvikling og vedligeholdelse, herunder personens rimelige leveomkostninger. En fysisk person, der offentliggør en FOSS og tilbyder teknisk bistand for at dække sine omkostninger og opnå et rimeligt vederlag, anses derfor ikke alene på dette grundlag for at bringe denne software i omsætning på EU-markedet.

59. En fysisk eller juridisk person, der tilbyder teknisk bistand vedrørende en FOSS, som ikke er under den pågældendes ansvar, anses ikke for at bringe denne software i omsætning, medmindre denne person foretager en væsentlig ændring af den pågældende FOSS i overensstemmelse med artikel 22 som led i leveringen af en sådan bistand.

Eksempel 19: En tjenesteyder offentliggør ikke en FOSS, men hjælper en kunde med at installere den på kundens lokale server. Dette sker uden at foretage en væsentlig ændring af den pågældende FOSS. Tjenesteyderen anses derfor ikke for at bringe den pågældende FOSS i omsætning.

3.2.4. *Donationer*

60. Fysiske eller juridiske personer, der offentliggør FOSS-projekter, kan rutinemæssigt inkludere forslag til, hvordan brugerne af softwaren frivilligt kan donere penge til projektets udgiver(e), bl.a. for at sikre, at projektet fortsat vedligeholdes aktivt.

61. Som anført i betragtning 15 til CRA bør »modtagelse af donationer uden gevinst for øje bør ikke anses som værende erhvervsvirksomhed«. Alene det forhold, at der medtages et link til en donationsplatform eller lignende værktøjer til at indsamle donationer, bør ikke betragtes som en hensigt om at opnå en fortjeneste, heller ikke hvis det beløb, der indsamles via donationer, overstiger de blotte omkostninger forbundet med udformning, udvikling og levering af et produkt med digitale elementer. Dette omfatter rimelig kompensation til bidragydere, der er ansat af en juridisk person, og/eller en fysisk persons rimelige leveomkostninger. Donationer svinger i sagens natur over tid, og der skal derfor udvises en vis fleksibilitet ved vurderingen af, om en FOSS, der udelukkende giver indtægter gennem donationer, anses for at være bragt i omsætning. En FOSS, der udelukkende støttes gennem donationer, vil derfor sandsynligvis ikke blive anset for at være bragt i omsætning som omhandlet i CRA.

Eksempel 20: En fysisk eller juridisk person offentliggør et FOSS-værktøj i et offentligt onlinelager, hvorved enhver kan downloade, bruge, ændre og redistribuere det under en fri og open source-licens. Udgiveren opfordrer brugerne til at give frivillige donationer via en donationsplatform for at støtte projektets fortsatte udvikling og vedligeholdelse. Adgang til softwaren, kildekoden og opdateringer er ikke betinget af, at der gives en donation. Den pågældende FOSS anses ikke for at være leveret som led i erhvervsvirksomhed og anses ikke for at være bragt i omsætning som omhandlet i CRA.

62. Ikke desto mindre er der tilfælde, hvor en FOSS, der støttes gennem donationer, kan anses for at være bragt i omsætning. Det er tilfældet, når donationerne på grundlag af en samlet vurdering af omstændighederne reelt svarer til opkrævning af en pris for adgang til produktet med digitale elementer eller visse af produktets funktionaliteter. Dette kan navnlig være tilfældet, når adgang til den pågældende FOSS, til væsentlige funktionaliteter eller til opdateringer heraf i praksis er betinget af, at der gives en donation, eller hvor donationer er forbundet med kontraktlige fordele eller eksklusive fordele, der rækker ud over fællesskabsfordelene.

Eksempel 21: En fysisk eller juridisk person offentliggør et softwareprodukt med digitale elementer under en fri og open source-licens, men stiller kun udgivelser, der kan downloades, og sikkerhedsopdateringer til rådighed for brugere, der giver en donation. Brugere, der ikke giver en donation, har ikke adgang til den seneste version af softwaren.

I dette tilfælde er donationerne reelt en betingelse for adgang til produktet med digitale elementer og svarer derfor til opkrævning af en pris. Den pågældende FOSS anses derfor for at være bragt i omsætning som omhandlet i CRA.

Eksempel 22: En fysisk eller juridisk person gør kildekoden til en FOSS offentligt tilgængelig, men stiller kun prækompilerede binære filer, regelmæssige opdateringer og garanterede rettelser af sikkerhedsfejl til rådighed for donorer. I dette tilfælde er donationerne knyttet til adgang til væsentlige aspekter af produktet med digitale elementer og udgør vederlag for leveringen af dette produkt. Den pågældende FOSS anses derfor for at være bragt i omsætning som led i erhvervsvirksomhed.

3.2.5. *Finansiering af fri og open source-software*

63. Det forhold, at en tredjepart har betalt for, sponsoreret eller på anden måde finansieret udviklingen af en FOSS, er ikke i sig selv afgørende for, om denne FOSS er bragt i omsætning. Det er almindelig praksis i FOSS-økosystemet, at individuelle udviklere, fonde eller fællesskaber modtager finansiering fra virksomheder, offentlige organer eller andre sponsorer med henblik på at arbejde på specifikke features, rette fejl eller vedligeholde kritiske komponenter. Denne finansiering kan antage mange former, herunder tilskud, bug bounty-ordninger, sponsorater, tjenesteydelseskontrakter eller betalt udviklingsarbejde.

64. Som allerede nævnt præciseres det i betragtning 18 i CRA, at de omstændigheder, hvorunder produktet med digitale elementer er blevet udviklet, eller hvordan udviklingen er blevet finansieret, i sig selv ikke bør tages i betragtning ved fastlæggelsen af den pågældende aktivitets kommercielle karakter.

65. Hvis FOSS derfor deles åbent og gøres frit tilgængelig for alle med henblik på adgang, brug, ændring og videredistribution, bør det forhold, at en kommerciel enhed kan have betalt for projektet, ikke bidrage til at afgøre, om softwaren er bragt i omsætning. Hvis den pågældende FOSS reelt ikke på anden vis bringer indtjening, skal den ikke anses for at være bragt i omsætning. Hvis den virksomhed, der finansierede udviklingen af FOSS (såvel som enhver anden virksomhed), integrerer den i virksomhedens produkt med digitale elementer, skal virksomheden udvise due diligence i overensstemmelse med artikel 13, stk. 5, i CRA.

Eksempel23: En individuel udvikler offentliggør et FOSS-projekt og vedligeholder det aktivt. Fabrikant A anmoder den individuelle udvikler om at tilføje en specifik funktion til den pågældende FOSS og finansierer denne udvikling. Udvikleren tilføjer funktionen til kodebasen bag den pågældende FOSS, deler den åbent og gør den frit tilgængelig for alle med henblik på adgang, brug, ændring og videredistribution. Den individuelle udvikler anses ikke for at have bragt den pågældende FOSS i omsætning. Hvis fabrikanten integrerer en FOSS i fabrikantens produkt med digitale elementer, skal fabrikanten udvise due diligence i overensstemmelse med artikel 13, stk. 5.

3.2.6. *Almennyttige enheder oprettet med henblik på almennyttige mål*

66. Hvis en juridisk person, der offentliggør FOSS, er en almennyttig organisation, der er »oprettet på en sådan måde, at det sikres, at al indtjening efter fradrag af omkostninger anvendes til at nå almennyttige mål« (betragtning 18 i CRA), anses den FOSS, som den offentliggør, ikke for at være bragt i omsætning. Hvis den juridiske person opfylder definitionen af »forvalter«, er den omfattet af de tilsvarende forpligtelser (artikel 24 i CRA).

Eksempel24: En juridisk person offentliggør en fri og open source-browser, der skaber direkte indtjening via partnerskaber med søgemaskiner, men alle indtægter efter fradrag af omkostninger anvendes til almennyttige formål. Browseren anses ikke for at være bragt i omsætning som omhandlet i CRA. Den juridiske person, der offentliggør den, er omfattet af de forpligtelser, der gælder for forvaltere.

3.2.7. *Integration foretaget af andre fabrikanter*

67. I visse tilfælde offentliggøres FOSS af en klart identificerbar fysisk eller juridisk person, men denne FOSS er »beregnet til, at andre fabrikanter kan integrere dem i deres egne produkter med digitale elementer«. I sådanne tilfælde anses den pågældende FOSS ikke for at være bragt i omsætning på EU-markedet, medmindre den også skaber indtjening til den person, der offentliggør den (dvs. den oprindelige fabrikant), i overensstemmelse med de foregående afsnit i denne vejledning.

68. Hvis den pågældende FOSS ikke bringes i omsætning, vil den juridiske person, der offentliggør den, være omfattet af forvalterforpligtelserne, hvis den yder støtte på et vedvarende grundlag i overensstemmelse med definitionen af »forvalter«.

Eksempel25: En juridisk person offentliggør et FOSS-bibliotek til opbygning af brugergrænseflader. Personen tjener ikke penge på leveringen af dette bibliotek, men integrerer det i et af sine produkter med digitale elementer (som igen bringes i omsætning). Biblioteket anses ikke for at være bragt i omsætning som omhandlet i CRA, men det er beregnet til integration i produkter med digitale elementer. Den juridiske person, der offentliggør det, er dets forvalter.

Eksempel26: En juridisk person bringer et operativsystem i omsætning og offentliggør også FOSS-biblioteker, der skal fungere som referenceimplementeringer for brugere af dette operativsystem. Den juridiske person tjener ikke penge på FOSS-bibliotekerne, der er beregnet til integration i andre produkter med digitale elementer. Den juridiske person, der offentliggør dem, er forvalter for disse FOSS-biblioteker.

3.3. **Open source-software-forvaltere**

69. CRA indfører den nye retlige kategori »open source-software-forvalter« i lyset af »hvilken betydning mange produkter med digitale elementer, der kan betegnes som fri og open source-software, og som offentliggøres, men ikke gøres tilgængelige på markedet i den i [CRA] anvendte betydning, spiller for cybersikkerheden« (betragtning 19 i CRA).

70. I visse tilfælde offentliggøres FOSS, men gøres ikke tilgængelig på markedet som omhandlet i CRA, af en juridisk person, der »har til formål eller mål systematisk at yde vedvarende støtte til udvikling af [FOSS] […] beregnet til kommercielle aktiviteter, og som sikrer disse produkters levedygtighed« (artikel 3, nr. 14, i CRA). I sådanne tilfælde er den juridiske person omfattet af forvalterforpligtelserne.

71. En forvalter defineres som »en juridisk person, der ikke er fabrikant«, fordi en fabrikant pr. definition er den fysiske eller juridiske person, som bringer produkter med digitale elementer i omsætning (»markedsfører dem«) under eget navn eller varemærke. En juridisk person kan kun være forvalter for produkter med digitale elementer, der betegnes som FOSS, og som offentliggøres, men ikke gøres tilgængelige på markedet som omhandlet i CRA. Begrebet forvalter finder derfor anvendelse på specifikke forekomster af FOSS, der »i sidste ende er beregnet til erhvervsvirksomhed såsom integration i kommercielle tjenester eller i produkter med digitale elementer, som der tjenes penge på« (betragtning 19 i CRA ([13])), men som ikke gøres tilgængelige på markedet som omhandlet i CRA, og for hvilke den juridiske person, der offentliggør den pågældende FOSS, sikrer systematisk støtte.

72. At være forvalter for én specifik FOSS betyder ikke nødvendigvis, at den juridiske person også er forvalter for andre FOSS, som den offentliggør. Tilsvarende betyder det at være fabrikant for én specifik FOSS ikke, at den juridiske person ikke kan være forvalter for andre FOSS. Dette omfatter levering af »community«-versioner af samme FOSS, som beskrevet i afsnit *3.2.1 Opkrævning af en* pris.

73. En juridisk person kan derfor samtidig være forvalter for én specifik FOSS (hvis forvalteren systematisk yder støtte på et vedvarende grundlag og sikrer softwarens levedygtighed) og fabrikant for en anden specifik FOSS (hvis den bringer den i omsætning). Med andre ord kan den samme juridiske enhed være forpligtet til at udfylde forskellige roller for forskellige FOSS-projekter.

74. For hver specifik FOSS, som den offentliggør, skal den juridiske person fastslå, om den pågældende FOSS anses for at være bragt i omsætning som omhandlet i CRA. Hvis det er tilfældet, bliver den juridiske enhed fabrikant af softwaren. Hvis FOSS ikke anses for at være bragt i omsætning, kan den juridiske person være forvalter for den, hvis softwaren er bestemt til kommercielle aktiviteter, og hvis den juridiske person opretholder den i overensstemmelse med definitionen af forvalter ([14]).

3.3.1. *Vedvarende støtte og sikring af levedygtigheden af en FOSS*

75. I betragtning 19 forklares det, at ydelse af vedvarende støtte til udviklingen af et produkt med digitale elementer kan omfatte (men ikke er begrænset til): i) hosting og forvaltning af samarbejdsplatforme for softwareudvikling, ii) hosting af kildekode eller software, iii) styring eller forvaltning af produkter med digitale elementer, der betegnes som FOSS og (iv) styring af udviklingen af sådanne produkter med digitale elementer.

76. Dette kan f.eks. være tilfældet for en juridisk enhed, der udvikler en FOSS med henblik på integration i enhedens egne produkter med digitale elementer og derefter offentliggør den uden at bringe den i omsætning. Dette behandles også i afsnit *3.2.7 Integration foretaget af andre* fabrikanter. I dette tilfælde er den juridiske enhed ikke fabrikant af softwaren, men kan være forvalter af den. Som også forklaret i de foregående afsnit anses en juridisk enhed, der offentliggør en gratis version (eller »communityversion«) og en indtægtsgivende version af samme FOSS, desuden for at være forvalter for den gratis version (eller »communityversionen«) og fabrikant for den indtægtsgivende version.

77. Tilsvarende er en juridisk enhed, der tjener penge på en FOSS, men er en almennyttig enhed, hvis indtægter efter fradrag af omkostninger anvendes til at nå almennyttige mål (og hvis FOSS derfor ikke er bragt i omsætning som omhandlet i CRA, som behandlet i afsnit *3.2.6 Almennyttige enheder*), forvalter for den FOSS, som den offentliggør.

78. Desuden tilbyder visse fonde samarbejdsplatforme med forskellige former for governance, som gør det muligt for fabrikanter regelmæssigt at bidrage til udviklingen af FOSS, og/eller som regelmæssigt finansieres af fabrikanter. Sådanne fonde skal anses for forvaltere i relation til specifikke FOSS, der er bestemt til kommercielle aktiviteter, til hvilke fonden tilbyder vedvarende støtte. Som forklaret i afsnit *3.3 Open source-software-forvaltere* kan en sådan fond dog være uden forpligtelser i henhold til CRA for andre specifikke FOSS, som den hoster, i tilfælde, hvor den ikke yder systematisk støtte til en specifik FOSS, ikke sikrer dens langsigtet levetid, og/eller hvor den specifikke software ikke er bestemt til kommercielle aktiviteter.

([13]) Dette begreb indgår også i formuleringen »beregnet til kommercielle aktiviteter« i definitionen af »open source-softwareforvalter« i artikel 3, nr. 14, i CRA.

([14]) Den juridiske person kan også være uden forpligtelser i henhold til CRA i tilfælde, hvor: i) en specifik FOSS ikke er bragt i omsætning som omhandlet i CRA og ii) den juridiske enhed ikke opfylder definitionen af forvalter i forhold til den pågældende specifikke FOSS.

79. Den type »vedvarende støtte«, som fonde og lignende organisationer yder til specifikke FOSS-projekter, kan variere betydeligt. Visse juridiske enheder yder f.eks. kun ikke-teknisk støtte, såsom forvaltning af projekters branding, fastsættelse af governanceregler, organisering af communityarrangementer eller indsamling af donationer. Andre enheder stiller også den underliggende IT-infrastruktur til rådighed, som er nødvendig for at drive projektet, såsom hosting af kildekodedepoter, tilrådighedsstillelse af versionsstyringssystemer eller generering af signeringsnøgler. Andre yder yderligere støtte ved aktivt at bidrage med tekniske ressourcer til projektet, f.eks. ved at ansætte udviklere, koordinere udviklingsarbejde, gennemgå eller indarbejde kode, administrere versionsudgivelser eller håndtere sårbarhedsrapporter og sikkerhedsrettelser. Alle juridiske enheder, der betegnes som forvaltere i henhold til CRA, skal overholde forpligtelserne i artikel 24, stk. 1 og 2, men det varierer, i hvilket omfang forpligtelserne i artikel 14, stk. 1, 3 og 8, finder anvendelse på disse juridiske enheder, afhængigt af den type støtte, de yder, jf. artikel 24, stk. 3.

80. En forvalter, der kun yder support af ikke-teknisk karakter, er f.eks. pr. definition ikke involveret i udviklingen af produktet med digitale elementer og er derfor ikke forpligtet til at indberette aktivt udnyttede sårbarheder. Denne forvalter stiller heller ikke netværks- og informationssystemer til rådighed for udviklingen af sådanne produkter med digitale elementer og er derfor ikke forpligtet til at indberette alvorlige hændelser til ENISA og CSIRT eller til berørte brugere. Hvis forvalteren ikke desto mindre bliver bekendt med en aktivt udnyttet sårbarhed (f.eks. via en rapport fra eksterne kilder såsom sikkerhedsforskere), bør den dele oplysningerne med reparatørerne af produktet med digitale elementer i overensstemmelse med forvalterens cybersikkerhedspolitik. Reparatørerne af produkterne med digitale elementer og/eller forvalterne bør også overveje frivilligt at indberette sårbarheden i overensstemmelse med artikel 15.

81. Hvis en forvalter derimod stiller den underliggende IT-infrastruktur til rådighed for visse produkter med digitale elementer, skal forvalteren i overensstemmelse med artikel 14, stk. 3, underrette ENISA og CSIRT om enhver alvorlig hændelse vedrørende denne infrastruktur, der har indvirkning på sikkerheden af produkterne med digitale elementer. Den skal også, hvor det er relevant, informere alle brugere (f.eks. via en generel meddelelse). Som anført i det foregående punkt er forvalteren ganske vist ikke forpligtet til at indberette aktivt udnyttede sårbarheder, som den bliver bekendt med, men den bør fremme korrekt håndtering af sårbarheder og overveje frivillig indberetning i overensstemmelse med artikel 15.

82. Endelig skal en forvalter, der også stiller tekniske ressourcer til rådighed for specifikke produkter med digitale elementer: i) i overensstemmelse med artikel 14, stk. 1, underrette om aktivt udnyttede sårbarheder, som forvalteren bliver bekendt med og ii) hvor det er relevant, informere alle brugere. I det omfang forvalteren også har en direkte forbindelse til berørte brugere, skal forvalteren også informere dem direkte i overensstemmelse med artikel 14, stk. 8.

83. Hvis en enhed ophører med systematisk at yde støtte på et vedvarende grundlag til en specifik FOSS, opfylder enheden muligvis ikke længere definitionen af forvalter og er derfor muligvis ikke længere omfattet af de tilsvarende forpligtelser. I sådanne tilfælde opfordres enheden til klart at kommunikere ændringen i status for den pågældende specifikke FOSS.

84. I visse situationer kan en enhed, der var forvalter for et specifikt projekt, beslutte at skabe direkte indtjening på projektet og dermed bringe produktet med digitale elementer i omsætning og udløse forpligtelserne for en fabrikant i henhold til CRA. Under sådanne omstændigheder kvalificerer enheden sig som fabrikant af produktet med digitale elementer fra den dato, hvor enheden bringer produktet i omsætning (men ikke for så vidt angår tidligere versioner, for hvilke enheden fungerede som forvalter).

3.4. **Bidragydere og anvendelser downstream**

85. Som allerede nævnt i afsnit *3.1 Fastlæggelse af, om fri og open* source-software hører under en persons ansvar præciseres det i CRA, at forordningen ikke finder anvendelse »på fysiske eller juridiske personer, som bidrager med kildekode til produkter med digitale elementer, der kan betegnes som fri og open source-software, som ikke er deres ansvar« (betragtning 18).

86. Fabrikanter af produkter med digitale elementer, der integrerer FOSS-komponenter i deres egne produkter med digitale elementer, bliver heller ikke ansvarlige for disse komponenters individuelle overholdelse af CRA, selv når fabrikanterne bidrager med kildekode til vedligeholdelsen heraf.

87. Tilsvarende har det forhold, at fabrikanter integrerer FOSS-komponenter i deres egne (indtægtsgivende) produkter med digitale elementer, i sig selv ingen indvirkning på den pågældende FOSS-komponents status i henhold til CRA. Reparatører af FOSS-komponenter, der ikke er bragt i omsætning, har ikke forpligtelser over for andre enheder, der måtte integrere sådanne komponenter i deres produkter med digitale elementer. Hvorvidt CRA finder anvendelse på en given FOSS-komponent, afhænger udelukkende af, om den fysiske eller juridiske person, der offentliggør den, bringer den i omsætning.

88. Ikke desto mindre skal fabrikanter af produkter med digitale elementer, der integrerer FOSS-komponenter, overholde CRA for deres egne produkter med digitale elementer. De har også en due diligence-forpligtelse i henhold til artikel 13, stk. 5, med hensyn til de FOSS-komponenter, som de integrerer. Desuden skal de indberette sårbarheder i integrerede komponenter og videregive rettelser af sikkerhedsfejl i overensstemmelse med artikel 13, stk. 6. Yderligere vejledning om dette emne findes i afsnit *9.2.1 Indberetning upstream og deling af rettelser* af sikkerhedsfejl.

3.5. **Illustrative scenarier**

89. Eksemplerne nedenfor er hypotetiske og har udelukkende til formål at illustrere forskellige tilfælde som forklaret i afsnittene ovenfor.

Eksempel 27: Den individuelle udvikler A har udviklet FOSS. Udvikler A offentliggør den pågældende FOSS under eget navn eller varemærke, men tager ikke betaling for brugen heraf. Softwaren deles åbent og er frit tilgængelig for alle med henblik på adgang, brug, ændring og videredistribution. Udvikler A medtager også et link til en platform til indsamling af frivillige donationer.

Virksomhederne B, C og D integrerer den pågældende FOSS i deres egne produkter med digitale elementer. For at støtte den løbende vedligeholdelse yder virksomhederne B, C og D frivillige donationer til udvikler A. Disse donationer sætter udvikler A i stand til at holde projektet aktivt vedligeholdt.

Den pågældende FOSS bringes ikke i omsætning som omhandlet i CRA. Udvikler A har ingen forpligtelser i henhold til CRA. Virksomhederne B, C og D skal udvise due diligence i overensstemmelse med artikel 13, stk. 5, når de integrerer den pågældende FOSS i deres egne produkter med digitale elementer.

Eksempel 28: Den almennyttige fond F offentliggør en FOSS-komponent med henblik på integration i andre kommercielle produkter med digitale elementer. Fond F forpligter sig til at yde vedvarende støtte til den pågældende FOSS for at sikre dens levedygtighed og udbredelse. Virksomhederne A, B og C integrerer den pågældende FOSS i deres egne produkter med digitale elementer. Virksomhederne A og B bidrager frivilligt med noget af deres udvikleres tid til udvikling og vedligeholdelse af FOSS-projekter inden for fond F, herunder for den pågældende FOSS.

Da fond F er en almennyttig enhed, der er oprettet på en sådan måde, at alle indtægter efter fradrag af omkostninger anvendes til at nå almennyttige mål, anses den pågældende FOSS ikke for at være bragt i omsætning som omhandlet i CRA. Fond F er forvalter for den pågældende FOSS og er omfattet af de tilsvarende forpligtelser, der er fastsat i artikel 24. Virksomhederne A, B og C skal udvise due diligence i overensstemmelse med artikel 13, stk. 5, når de integrerer den pågældende FOSS i deres egne produkter med digitale elementer.

Eksempel 29: Virksomhed A har udviklet en FOSS-komponent med henblik på integration i egne produkter med digitale elementer. Den offentliggør også den pågældende FOSS særskilt under eget navn eller varemærke og vedligeholder den aktivt. Den tager imidlertid ikke betaling for brugen heraf eller tjener på andre måder penge på den. Virksomhederne B, C og D integrerer den pågældende FOSS i deres egne produkter med digitale elementer og bidrager frivilligt med noget af deres udvikleres tid til vedligeholdelsen heraf.

Den pågældende FOSS anses ikke for at være bragt i omsætning som omhandlet i CRA. Virksomhed A er ikke dens fabrikant, men dens forvalter. Virksomhederne B, C og D skal udvise due diligence i overensstemmelse med artikel 13, stk. 5, når de integrerer den pågældende FOSS i deres egne produkter med digitale elementer.

Eksempel 30: Virksomhed A offentliggør en FOSS under eget navn eller varemærke og udbyder den som en betalt version, der omfatter visse fordele såsom teknisk bistand eller optimering af ydeevne. Udviklere fra virksomhederne B, C og D bidrager til vedligeholdelsen af den pågældende FOSS, men den forbliver under virksomhed A's kontrol.

Virksomhed A anses for at være fabrikant af den pågældende FOSS ([15]). Virksomhederne B, C og D er ikke omfattet af forpligtelser i henhold til CRA for den pågældende specifikke FOSS. Hvis de integrerer den pågældende FOSS i deres egne produkter med digitale elementer, skal de udvise due diligence i overensstemmelse med artikel 13, stk. 5.

Eksempel 31: Virksomhed A offentliggør en FOSS under eget navn eller varemærke og leverer løbende vedligeholdelse for at sikre dens langsigtede levedygtighed og gøre det muligt at integrere denne software i andre virksomheders produkter med digitale elementer. Virksomhed A tager ikke betaling for brugen heraf, behandler ikke personoplysninger, som den indsamler gennem produktet med digitale elementer, og sælger ikke støttetjenester i forbindelse med offentliggørelsen af den pågældende FOSS.

Virksomhed B bidrager med kode og udvikleres tid til vedligeholdelsen af den pågældende FOSS, men distribuerer den ikke kommercielt. Virksomhed B tilbyder tekniske supporttjenester uafhængigt af distributionen af den pågældende FOSS. Virksomhed A anses for at være forvalter for den pågældende FOSS, mens virksomhed B ikke har forpligtelser i henhold til CRA for den pågældende FOSS.

Eksempel 32: En FOSS-komponent offentliggøres af en almennyttig enhed, der er oprettet på en sådan måde, at alle indtægter efter fradrag af omkostninger anvendes til at nå almennyttige mål. Enheden yder vedvarende støtte for at sikre projektets langsigtede levedygtighed. Vedligeholdelsen finansieres gennem offentlig finansiering såsom forskningstilskud. Yderligere udvikling, herunder nye funktioner, finansieres gennem donationer og specifikke projekter, der gennemføres i partnerskab med fabrikanter, som integrerer den pågældende FOSS i deres produkter med digitale elementer. Sådanne funktioner indarbejdes i kodebasen til den pågældende FOSS.

Den almennyttige enhed, der offentliggør den pågældende FOSS, anses for at være forvalter for den pågældende FOSS-komponent. En fabrikant, der har bidraget til udviklingen af visse funktioner, bliver ikke fabrikant af den pågældende FOSS-komponent. Hvis fabrikanten integrerer den pågældende FOSS-komponent i fabrikantens eget produkt med digitale elementer, skal denne udvise due diligence i overensstemmelse med artikel 13, stk. 5.

Eksempel 33: En almennyttig enhed, der er oprettet på en sådan måde, at alle indtægter efter fradrag af omkostninger anvendes til at nå almennyttige mål, offentliggør et FOSS-softwareudviklingssæt (SDK) og sikrer den løbende vedligeholdelse heraf. Det pågældende SDK deles åbent og er frit tilgængeligt for alle med henblik på adgang, brug, ændring og videredistribution. Finansieringen tilvejebringes gennem medlemskontingenter, der betales til den almennyttige enhed, og udviklere, der er ansat af medlemsorganisationer, bidrager med kode og andre ressourcer til udviklingen af det pågældende SDK. Fabrikanter anvender det pågældende SDK som en komponent til at opbygge andre produkter med digitale elementer.

Den almennyttige enhed, der offentliggør det pågældende SDK, er forvalter af det. Fondens medlemmer er ikke ansvarlige for, at det pågældende SDK overholder CRA. Hvis fabrikanter anvender det pågældende SDK til at bygge deres eget produkt med digitale elementer, skal de udvise due diligence i overensstemmelse med artikel 13, stk. 5.

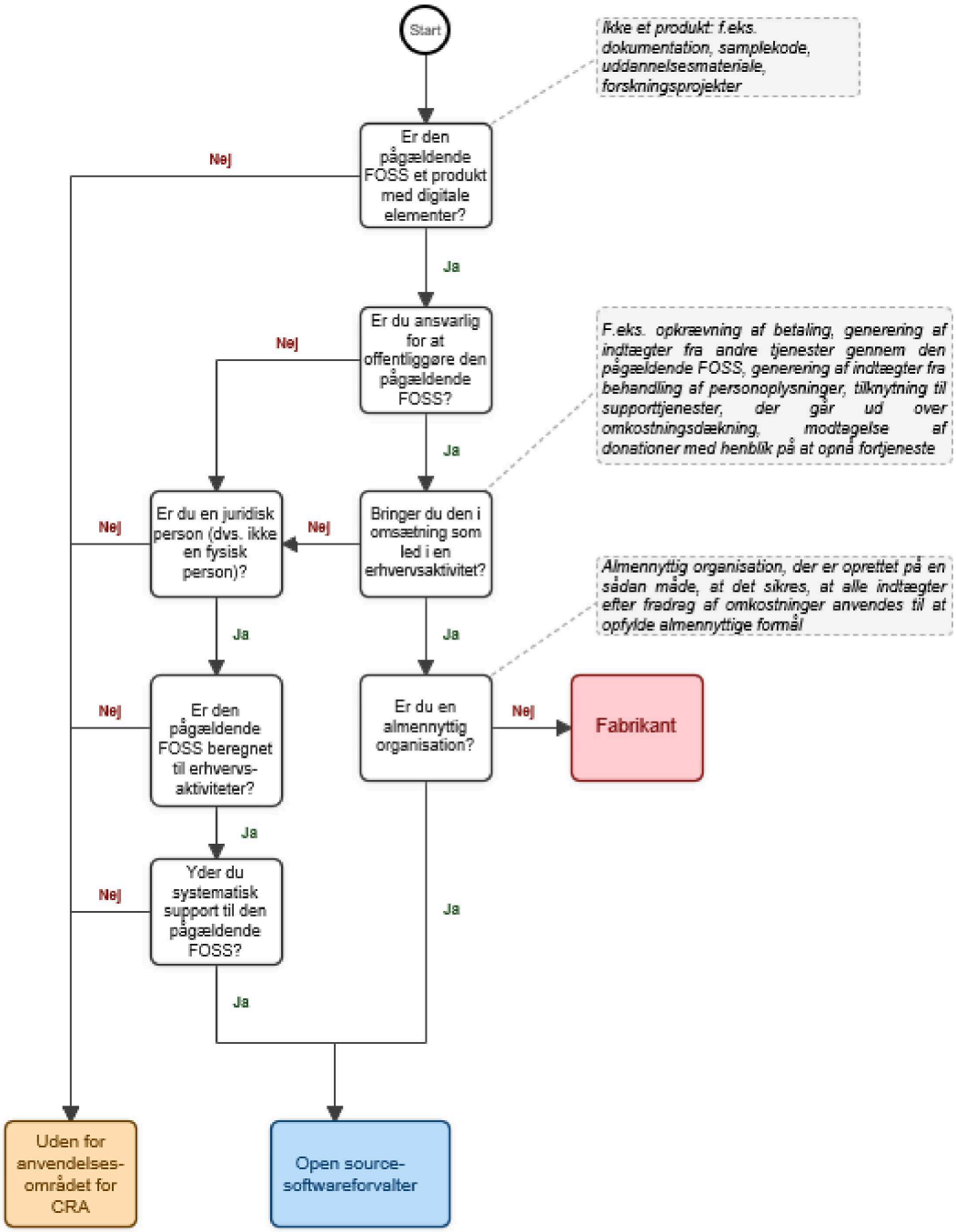
Eksempel 34: En individuel udvikler offentliggør et FOSS-bibliotek i et offentligt pakkearkiv for et givet programmeringssprog og vedligeholder det aktivt. I pakkedokumentationen indsætter udvikleren et link til indsamling af donationer. En fabrikant downloader biblioteket gratis fra arkivet og integrerer det i sit eget produkt med digitale elementer.

Den individuelle udvikler og pakkearkivet har ingen forpligtelser i henhold til CRA. Den fabrikant, der integrerer biblioteket, skal udvise due diligence i overensstemmelse med artikel 13, stk. 5.

([15]) Medmindre virksomhed A er en almennyttig enhed, der er oprettet på en sådan måde, at alle indtægter efter fradrag af omkostninger anvendes til at nå almennyttige mål, i hvilket tilfælde den ville være forvalter for den pågældende FOSS.

Figur 1:

Stiliseret flowdiagram over CRA's dækning af fri og open source-software



4. VÆSENTLIGE ÆNDRINGER OG RESERVEDELE

90. I artikel 3, nr. 30), i CRA defineres en »væsentlig ændring« som en ændring af produktet med digitale elementer, efter at det er bragt i omsætning, som i) har indvirkning på overensstemmelsen af produktet med digitale elementer med de væsentlige cybersikkerhedskrav i bilag I, del I, eller ii) som medfører en ændring af det tilsigtede formål, for hvilket produktet med digitale elementer er blevet vurderet.

91. Begrebet væsentlig ændring er relevant for fastlæggelsen af forpligtelserne i henhold til CRA i en række tilfælde, herunder følgende:

a) i overensstemmelse med artikel 21 anses en importør eller distributør, der foretager en væsentlig ændring af et produkt med digitale elementer, som allerede er bragt i omsætning, for at være dets fabrikant

b) i overensstemmelse med artikel 22 anses enhver fysisk eller juridisk person, der foretager en væsentlig ændring af et produkt med digitale elementer og gør det tilgængeligt på markedet, for at være dets fabrikant

c) i overensstemmelse med artikel 69, stk. 2, anses enhver fysisk eller juridisk person, som efter den 11. december 2027 foretager en væsentlig ændring af et produkt med digitale elementer, der er bragt i omsætning før den 11. december 2027, og bringer det i omsætning, for at være dets fabrikant

d) for fabrikanter af produkter med digitale elementer, der er bragt i omsætning efter den 11. december 2027, med henblik på at fastslå, om et produkt med digitale elementer skal gennemgå en ny overensstemmelsesvurderingsprocedure som følge af ændringer foretaget efter denne dato, navnlig i lyset af softwareudviklingens iterative karakter.

92. Det er derfor vigtigt at tilvejebringe en vejledning, der hjælper økonomiske aktører med at forstå, hvornår ændringer af hardware eller software betragtes som væsentlige ændringer.

4.1. **Fysiske reparationer**

93. Følgende er anført i betragtning 42 i CRA: »Hvor et produkt med digitale elementer er genstand for »istandsættelse«, »vedligeholdelse« og »reparation« som defineret i artikel 2, nr. 18), 19) og 20), i Europa-Parlamentets og Rådets forordning (EU) 2024/1781, fører dette ikke nødvendigvis til en væsentlig ændring af produktet, f.eks. hvis det tilsigtede formål og den tilsigtede funktionalitet ikke ændres, og risikoniveauet ikke påvirkes. En fabrikants opgradering af et produkt med digitale elementer kan imidlertid føre til ændringer i det pågældende produkts design og udvikling og kan derfor påvirke dets tilsigtede formål og opfyldelse af kravene i nærværende forordning.« Dette er i overensstemmelse med afsnit 2.1 i den blå vejledning, hvori det anføres, at »et produkt, der har været genstand for betydelige ændringer eller ombygninger, efter at det er blevet taget i brug, skal betragtes som et nyt produkt, hvis: i) dets oprindelige ydeevne, formål eller type er ændret, uden at dette er forudset i den indledende risikovurdering, ii) farens art har ændret sig, eller risikoniveauet er forøget i forhold til den relevante EU-harmoniseringsretsakt, og iii) produktet er gjort tilgængeligt (eller taget i brug, hvis den gældende retsakts anvendelsesområde også omfatter ibrugtagning). Dette vurderes i hvert enkelt tilfælde og især på baggrund af lovgivningens formål og den type produkter, der er omfattet af den pågældende lovgivning«

94. Istandsættelses-, vedligeholdelses- eller reparationsarbejder, der medfører fysiske ændringer af produkter med digitale elementer, der allerede er bragt i omsætning, udgør ikke nødvendigvis væsentlige ændringer. Der bør derfor foretages en vurdering i hvert enkelt tilfælde for at fastslå, om en sådan fysisk ændring har indvirkning på et produkt med digitale elementers overensstemmelse med de væsentlige krav i bilag I, del I, eller medfører en ændring af produktets tilsigtede formål, som er omfattet af cybersikkerhedsrisikovurderingen.

95. Udskiftning af defekte dele eller slidte elementer med dele, der har en bedre ydeevne (f.eks. på grund af tekniske fremskridt, eller fordi den gamle del ikke længere produceres), udløser ikke i sig selv en væsentlig ændring af det reparerede produkt med digitale elementer. Det gør det kun, hvis ændringen i ydeevnen eller den måde, det reparerede produkt med digitale elementer fungerer på, i) har indvirkning på dets overensstemmelse med de væsentlige krav eller ii) medfører en ændring af det tilsigtede formål, som ikke var omfattet af risikovurderingen.

Eksempel 35: Fabrikanten af en computerserver udfører en reparation, hvor et defekt RAM-modul udskiftes med et nyt modul med bedre ydeevne. Serverens overensstemmelse med de væsentlige krav påvirkes ikke. Serverens ydeevne forbedres, men dens nye ydeevne ligger fortsat inden for serverens tilsigtede anvendelse som lagt til grund i cybersikkerhedsrisikovurderingen. Computerserveren anses ikke for at være blevet væsentligt ændret.

4.2. **Reservedele**

96. I artikel 2, stk. 6, i CRA fastsættes det, at reservedele, der er beregnet til at udskifte identiske komponenter og er fremstillet efter de samme specifikationer som disse komponenter, ikke er omfattet af CRA. I betragtning 29 anføres det endvidere, at undtagelsen omfatter både reservedele til produkter med digitale elementer, der er gjort tilgængelige, før CRA begyndte at finde anvendelse, og reservedele, der allerede har gennemgået en overensstemmelsesvurderingsprocedure som fastsat i forordningen.

97. Undtagelsen i artikel 2, stk. 6, i CRA bør forstås således, at den kun finder anvendelse, hvor reservedelen specifikt leveres med henblik på at reparere eller forlænge holdbarheden af et produkt med digitale elementer, der allerede er bragt i omsætning (før eller efter den 11. december 2027). Hvis et produkt med digitale elementer leveres som et enkeltstående produkt uden nogen forbindelse til vedligeholdelse eller reparation af et allerede eksisterende produkt med digitale elementer, bringes det i omsætning som omhandlet i CRA og bør ikke anses for en reservedel, der er omfattet af anvendelsesområdet for artikel 2, stk. 6. Vedligeholdelses- eller reparationsformålet bør fremgå af leveringssammenhængen, f.eks. gennem identifikation af produktet med digitale elementer eller produktfamilien i ordren eller det kommercielle tilbud eller gennem levering via eftersalgs- eller servicekanaler. Understøttende dokumentation herfor bør også holdes til rådighed for markedsovervågningsmyndighederne. Det forhold, at et produkt med digitale elementer teknisk set kan anvendes til at erstatte en komponent, er ikke i sig selv tilstrækkeligt til at bringe det ind under undtagelsens anvendelsesområde, hvis sådanne elementer ikke foreligger.

98. Hvis en reservedel er identisk med en komponent, der allerede indgår i et produkt med digitale elementer, som enten er bragt i omsætning før anvendelsesdatoen for CRA eller er bragt i omsætning i overensstemmelse med CRA, er denne reservedel derfor ikke selv omfattet af CRA.

99. Vurderingen af, om en reservedel bør anses for identisk med en komponent, bør fokusere på dens funktionelle rolle i produktet med digitale elementer og de karakteristika, der kan være relevante for cybersikkerheden. Selv om en vurdering i det enkelte tilfælde altid er nødvendig, forhindrer forskelle, der ikke påvirker komponentens sikkerhedskarakteristika eller cybersikkerhedsrisikoprofil, ikke i sig selv, at reservedelen er omfattet af anvendelsesområdet for artikel 2, stk. 6, i CRA.

100. Derimod kan forskelle i karakteristika, der er relevante for komponentens cybersikkerhed, såsom algoritmer, protokoller, kryptografiske mekanismer, adgangskontrolfunktioner eller andre sikkerhedsrelevante karakteristika, betyde, at den nye del ikke kan anses for identisk med den komponent, den skal erstatte.

101. Hvis en reservedel ikke er identisk med den oprindelige komponent, udgør reservedelen et selvstændigt produkt med digitale elementer og er derfor omfattet af CRA. I sådanne tilfælde skal overensstemmelsen med de væsentlige krav vurderes i lyset af erstatningskomponentens tilsigtede formål. Af særlig relevans er erstatningskomponentens funktion med hensyn til at sikre kompatibilitet eller interoperabilitet med et eksisterende produkt med digitale elementer, herunder hvor dette produkt er et produkt med digitale elementer, der er bragt i omsætning, før CRA begyndte at finde anvendelse. Hvis visse væsentlige krav ikke med rimelighed kan opfyldes på grund af dette tilsigtede formål eller tekniske begrænsninger, skal fabrikanten afspejle dette i cybersikkerhedsrisikovurderingen og gennemføre passende alternative eller kompenserende risikobegrænsende foranstaltninger for ikke at undergrave sikkerheden af produktet med digitale elementer. Som også behandlet i afsnit *2.6 Komplekse systemer*, spiller både den tekniske dokumentation og oplysningerne og instruktionerne til brugeren en central rolle med hensyn til på en gennemsigtig måde at beskrive de identificerede begrænsninger, de tilknyttede cybersikkerhedsrisici og de gennemførte risikobegrænsende foranstaltninger. Som forklaret i afsnit *4.1 Fysiske reparationer*, udløser udskiftning af defekte dele eller slidte elementer med dele, der har en bedre ydeevne, ikke i sig selv en væsentlig ændring af det reparerede produkt med digitale elementer.

Eksempel 36: En fabrikant har bragt forbundne styreenheder i omsætning på EU-markedet. I ét tilfælde blev styreenheden bragt i omsætning i 2026, før anvendelsesdatoen for CRA. I et andet tilfælde blev styreenheden bragt i omsætning i 2028 i overensstemmelse med CRA. I 2028 svigter et digitalt kommunikationsmodul i begge typer styreenheder. Fabrikanten leverer som reservedel et erstatningsmodul, der er identisk med og fremstillet efter de samme specifikationer som det oprindelige.

I begge tilfælde er erstatningsmodulet omfattet af anvendelsesområdet for undtagelsen i artikel 2, stk. 6. Reservedelen er ikke selv omfattet af CRA, selv om den er et produkt med digitale elementer, fordi den erstatter en identisk komponent i et produkt med digitale elementer. Reparationen udgør ikke en væsentlig ændring af produktet med digitale elementer.

Eksempel 37: En fabrikant bragte en forbundet industriel styreenhed i omsætning på EU-markedet i 2026, før anvendelsesdatoen for CRA. I 2028 svigter en kommunikationschip i denne styreenhed. Da fabrikanten ikke længere fremstiller denne chip, leverer fabrikanten som reservedel en nyere chip med tilsvarende funktionalitet, men med en anden kryptografisk implementering og en ajourført mekanisme til sikker opstart med henblik på at opretholde kompatibilitet og fortsat drift.

I dette tilfælde kan erstatningschippen ikke anses for identisk, da forskellene i den kryptografiske implementering og mekanismen til sikker opstart påvirker chippens cybersikkerhedsegenskaber. Den er derfor ikke omfattet af undtagelsen i artikel 2, stk. 6, og udgør et produkt med digitale elementer, der er omfattet af CRA. Erstatningsdelens overensstemmelse skal vurderes i lyset af dens tilsigtede formål, herunder dens rolle med hensyn til at sikre interoperabilitet med det produkt med digitale elementer, der blev bragt i omsætning, før CRA begyndte at finde anvendelse.

Eksempel 38: En fabrikant bringer en styreenhed til intelligente bygninger i omsætning i 2028 i overensstemmelse med CRA. I 2029 svigter det trådløse modul i denne styreenhed. Da fabrikanten ikke længere fremstiller dette modul, leverer fabrikanten som reservedel et nyt modul, der udfører den samme funktion ved hjælp af de samme kommunikationsprotokoller og sikkerhedsmekanismer, men som er baseret på et andet chipsæt og har ajourført firmware, som ikke ændrer karakteristika, der kan være relevante for cybersikkerheden.

I dette tilfælde kan erstatningsmodulet anses for identisk. Modulet er derfor omfattet af undtagelsen i artikel 2, stk. 6, og ikke af CRA.

102. Undtagelsen for reservedele finder anvendelse, uanset om reservedelen erstatter en komponent i et produkt med digitale elementer, eller om den erstatter et komplet produkt med digitale elementer, som selv udgør en del af et større produkt, herunder hvor dette større produkt med digitale elementer består af flere integrerede komponenter, forudsat at erstatningsdelen specifikt leveres som reservedel som forklaret i de foregående afsnit.

Eksempel 39: I 2027 bringer en fabrikant et industrielt automatiseringssystem i omsætning, hvor en programmerbar logisk styreenhed (PLC) er integreret som en af komponenterne. I 2031 svigter PLC'ens centralenhed (CPU). Fabrikanten tilbyder to reparationsmuligheder: i) levering af en erstatningsenhed til CPU'en, som kan anses for identisk med den oprindeligt installerede CPU eller ii) levering af en komplet erstatnings-PLC, som kan anses for identisk med den oprindeligt installerede PLC. I begge tilfælde leveres erstatningen som reservedel gennem fabrikantens eftersalgsservicekanal, og det industrielle automatiseringssystem, som erstatningen er beregnet til, identificeres klart. I begge tilfælde er erstatningen omfattet af anvendelsesområdet for undtagelsen i artikel 2, stk. 6, uanset om erstatningen vedrører en komponent i PLC'en eller PLC'en som helhed.

4.3. **Softwareopdateringer som væsentlige ændringer**

103. Softwareudvikling er af iterativ karakter, idet softwareprodukter med digitale elementer, der allerede er bragt i omsætning, ofte og løbende opdateres. I denne forbindelse er det nyttigt at give yderligere vejledning med henblik på at fastslå, hvornår software skal anses for at være blevet væsentligt ændret. Denne vejledning har navnlig til formål at hjælpe fabrikanter af softwareprodukter med digitale elementer, der foretager ændringer i deres egne produkter, med at afgøre, om disse ændringer udgør en væsentlig ændring.

104. I betragtning 39 anføres det, at et produkt med digitale elementer er væsentligt ændret, hvis en ændring ændrer niveauet for cybersikkerhedsrisikoen, og hvis fabrikanten ikke har taget hensyn til en sådan ændret eller yderligere risiko i sin risikovurdering og følgelig i sin gennemførelse af de væsentlige krav. En fabrikant bør derfor i hvert enkelt tilfælde vurdere, om en softwareopdatering medfører nye eller øgede cybersikkerhedsrisici, og om der allerede er taget hånd om sådanne risici i fabrikantens risikovurdering.

105. Hvis en fabrikant indfører nye funktioner i et produkt med digitale elementer, som medfører en ændring af produktets tilsigtede formål som helhed, er det sandsynligt, at fabrikanten ikke har taget højde for disse ændringer i sin risikovurdering. Under sådanne omstændigheder betragtes ændringen generelt som en væsentlig ændring.

Eksempel 40: En fabrikant bringer et dashboard i omsætning, som indsamler data fra maskiner og viser tendenser og advarsler uden at kunne styre maskinerne. Fabrikanten udvikler efterfølgende en ny version af dashboardet og tilføjer funktioner, der gør det muligt at styre maskinerne, herunder at justere driftsparametre og genstarte maskiner efter fejltilstande. Som følge af disse ændringer har dashboardets tilsigtede formål ændret sig ud over det, der var forudset i risikovurderingen, idet det er gået fra at være et værktøj, der giver et situationsbillede, til at være et produkt med digitale elementer, der er beregnet til at udøve driftsmæssig styring af andre enheder. Dashboardet er derfor blevet væsentligt ændret.

Eksempel 41: En fabrikant bringer en softwareapplikation til forbrugere i omsætning, der er beregnet til at organisere og vise personoplysninger såsom e-mail, beskeder eller dokumenter og til at understøtte grundlæggende søge- og filtreringsfunktioner. Fabrikanten foretager efterfølgende en opdatering, så applikationen automatisk kan analysere brugerindhold med henblik på at generere adfærdsprofiler og træffe automatiserede beslutninger, der påvirker prioritering, undertrykkelse eller anbefaling af indhold uden brugerindgriben. Som følge af denne ændring skifter softwarens tilsigtede formål fra et brugerstyret informations-styringsværktøj til et automatiseret beslutningssystem, hvilket ikke var forudset i risikovurderingen. Applikationen er derfor blevet væsentligt ændret.

106. Det er dog muligt for en fabrikant gradvist at indføre nye funktioner, der allerede er omfattet af fabrikantens risikovurdering, eller som ikke i sig selv ændrer cybersikkerhedsrisikoprofilen for produktet med digitale elementer. Det kan f.eks. være tilfældet, hvis fabrikanten har planlagt udvikling af disse funktioner, allerede har beskrevet og vurderet de tilknyttede risici og har gennemført passende risikobegrænsende foranstaltninger for at sikre fortsat overholdelse af de væsentlige krav. Dette kan også være tilfældet, hvis de nye funktioner ikke indebærer ændringer, der medfører nye eller øgede risici. Opdateringer af denne art bør derfor ikke anses for væsentlige ændringer, da de ikke øger cybersikkerhedsrisikoen og følgelig ikke ændrer gennemførelsen af de væsentlige krav.

Eksempel 42: En beskedapplikation frigives indledningsvis med funktionalitet, der er begrænset til en-til-en-beskeder. Fabrikantens risikovurdering omfatter den senere indførelse af gruppebeskeder, herunder f.eks. den øgede kompleksitet ved beskedrouting. I en efterfølgende opdatering tilføjer fabrikanten gruppechatfunktionalitet sammen med administratorkontroller og moderationsværktøjer, der allerede var forudset og vurderet i det oprindelige design. Opdateringen medfører funktioner, der falder ind under det oprindelige tilsigtede formål og den oprindelige risikovurdering. Beskedapplikationen er derfor ikke blevet væsentligt ændret.

Eksempel 43: Et produktionsovervågningssystem bringes i omsætning med skrivebeskyttede kontrolpaneler aktiveret. Systemarkitekturen omfatter automatiserede styringsfunktioner, som er deaktiveret. Fabrikantens risikovurdering omfatter udtrykkeligt en fremtidig aktivering af de automatiserede styringsfunktioner, herunder cybersikkerhedsrisici forbundet med styring i lukket kredsløb, samt sikkerhedsforanstaltninger såsom mekanismer til operatørtilsidesættelse og fejlsikre tilstande. I en senere opdatering aktiverer fabrikanten de automatiserede styringsfunktioner og aktiverer sikkerhedsforanstaltningerne som oprindeligt vurderet. Produktionsovervågningssystemet er derfor ikke blevet væsentligt ændret.

107. Omvendt kan selv begrænsede eller tilsyneladende mindre nye funktioner medføre betydelige cybersikkerhedsrisici, som påvirker overholdelsen af de væsentlige krav. Vurderingen af, om der foreligger en væsentlig ændring, bør derfor ikke baseres på ændringens omfang eller kompleksitet, men på den mulige negative indvirkning på cybersikkerhedsrisikoprofilen for produktet med digitale elementer og følgelig på gennemførelsen af de væsentlige krav.

Eksempel 44: En fabrikant indfører en opdatering af en softwareapplikation, som tilføjer en »husk mig-funktion« eller en funktion til vedvarende login, der lagrer autentifikationstokens lokalt for at gøre løsningen mere brugervenlig. Selv om funktionaliteten er begrænset, medfører den nye risici for tyveri af autentifikationstokens, uautoriseret adgang og session hijacking, som ikke blev taget i betragtning i risikovurderingen. Opdateringen påvirker derfor overholdelsen af de væsentlige cybersikkerhedskrav. Softwareapplikationen er således blevet ændret væsentligt.

Eksempel 45: En fabrikant tilføjer en ny lognings- og diagnosticeringsfunktion til et eksisterende softwareprodukt med digitale elementer, som gør det muligt at eksportere detaljerede systemlogs med henblik på fejlsøgning. Selv om funktionaliteten kan forekomme begrænset, medfører den, at følsomme driftsdata indsamles og lagres i ukrypteret form. Herved opstår der risici for eksponering af data, som ikke tidligere er blevet vurderet eller imødegået. Ændringen kan derfor have en væsentlig indvirkning på cybersikkerhedsrisikoprofilen for produktet med digitale elementer. Softwareproduktet med digitale elementer er blevet ændret væsentligt.

108. I overensstemmelse med betragtning 39 i CRA skal sikkerhedsopdateringer generelt ikke anses for væsentlige ændringer, da deres primære formål er at reducere niveauet for den cybersikkerhedsrisiko, der er forbundet med produktet med digitale elementer. En sikkerhedsopdatering, der ikke ændrer det pågældende produkts tilsigtede formål og ikke medfører nye cybersikkerhedsrisici, bør derfor ikke betragtes som en væsentlig ændring, selv om denne opdatering kan medføre betydelige tekniske ændringer. Dette omfatter tilfælde, hvor visse funktioner ændres eller begrænses udelukkende med henblik på at afbøde identificerede sårbarheder og sikre fortsat overholdelse af de væsentlige krav.

Eksempel 46: En fabrikant udruller en sikkerhedsopdatering for at afhjælpe en sårbarhed i kodebasen for et produkt med digitale elementer, enten ved at rette en fejl i inputvalideringen, som kan føre til et buffer overflow, eller ved at rette en logisk fejl, der gør det muligt at omgå autentifikationen som følge af utilstrækkelig validering af sessiontokens. Opdateringen ændrer softwarens interne implementering uden at påvirke produktets tilsigtede formål eller skabe nye angrebsflader. Opdateringen har udelukkende til formål at reducere cybersikkerhedsrisikoen. Sikkerhedsopdateringen bør derfor ikke anses for en væsentlig ændring.

Eksempel 47: En fabrikant udruller en sikkerhedsopdatering, der skærper eksisterende sikkerhedskonfigurationer, f.eks. ved at stramme firewallregler, deaktivere ubenyttede netværksporte, ændre politikkerne for standardadgangskoder til administratorkonti eller gøre multifaktorautentifikation obligatorisk, hvor denne funktionalitet allerede var tilgængelig eller forudset. Selv om opdateringen kan påvirke, hvordan brugerne konfigurerer eller tilgår produktet med digitale elementer, ændrer den ikke produktets tilsigtede formål og har udelukkende til formål at styrke dets sikkerhedsniveau. Sikkerhedsopdateringen bør derfor ikke anses for en væsentlig ændring.

Eksempel 48: En fabrikant bringer et softwareprodukt med digitale elementer i omsætning, som sikrer kommunikationen ved hjælp af et konfigurerbart kryptografisk rammeværk, der understøtter flere kryptografiske algoritmer og nøglestørrelser som beskrevet i produktets tekniske dokumentation og risikovurdering. Risikovurderingen omfatter alle de kryptografiske valgmuligheder, som produktet med digitale elementer stiller til rådighed, og tager højde for den fremtidige udfasning af visse algoritmer. Risikovurderingen omfatter også risikobegrænsende foranstaltninger såsom kryptografisk agilitet, intern nøgleforvaltning og kompatibilitetstest. Som følge af nye kryptografiske retningslinjer udruller fabrikanten en sikkerhedsopdatering, der deaktiverer en udfaset algoritme og aktiverer et stærkere alternativ, som allerede understøttes, uden at indføre nye eksterne afhængigheder eller ændre datastrømmene. Da opdateringen gennemfører en sikkerhedsforanstaltning, som var forudset og vurderet som led i det oprindelige design, og ikke medfører nye cybersikkerhedsrisici, bør sikkerhedsopdateringen ikke anses for en væsentlig ændring.

109. Derimod kan en sikkerhedsopdatering betegnes som en væsentlig ændring, hvis opdateringen, uanset dens sikkerhedsmål, medfører, at det tilsigtede formål med produktet med digitale elementer ændres ud over det, der oprindeligt var forudset, eller medfører nye eller øgede cybersikkerhedsrisici. Dette kan f.eks. være tilfældet, hvis en opdatering væsentligt ændrer det pågældende produkts afgrænsning eller afhængighedsstruktur på en måde, der ikke var forudset i risikovurderingen, f.eks. ved væsentligt at ændre datastrømme eller tilføje nye eksternt tilgængelige grænseflader.

Eksempel 49: En fabrikant bringer et softwareprodukt med digitale elementer i omsætning, som er beregnet til lokal kryptering af filer, der lagres på en brugers enhed, og som gør det muligt for brugerne at kryptere og dekryptere filer efter behov. Efter at der er konstateret en sårbarhed i krypteringsprocessen, udruller fabrikanten en sikkerhedsopdatering, der fjerner funktionaliteten til lokal kryptering og i stedet kræver, at alle filer uploades til, lagres hos og behandles af en ekstern krypteringstjeneste, som drives af fabrikanten. Som følge af ændringen foretager produktet med digitale elementer ikke længere lokal kryptering som oprindeligt tilsigtet, men fungerer i stedet som en ekstern krypterings- og databehandlingstjeneste. Selv om opdateringen indføres af sikkerhedsmæssige årsager, ændrer den grundlæggende produktets tilsigtede formål på en måde, som ikke var forudset i risikovurderingen, og udgør derfor en væsentlig ændring.

Eksempel 50: En fabrikant bringer et softwareprodukt med digitale elementer i omsætning, som anvender en etableret krypteringsprotokol og en internt forvaltet livscyklus for kryptografiske nøgler til at sikre kommunikationen mellem produktets komponenter. Som følge af nyligt identificerede kryptografiske svagheder udruller fabrikanten en sikkerhedsopdatering, der erstatter den eksisterende krypteringsmekanisme med en anden protokol, som kræver anvendelse af en ekstern tjeneste til nøgleforvaltning, der drives af en tredjepart. Ændringen medfører, at produktets afhængigheder og datastrømme ændres væsentligt, idet der indføres nye eksterne grænseflader og en afhængighed af tredjepartstjenester, som ikke var taget i betragtning i risikovurderingen. Selv om opdateringen indføres af sikkerhedsmæssige årsager, medfører den nye cybersikkerhedsrisici og udgør derfor en væsentlig ændring.

110. Som anført i punkt 104 ovenfor bør det vurderes i hvert enkelt tilfælde, om en softwareopdatering udgør en væsentlig ændring. Når fabrikanterne foretager denne vurdering, kan de på en ikkeudtømmende måde overveje, om softwareopdateringen:

a) medfører indførelse af nye trusselsvektorer, såsom yderligere grænseflader, kommunikationskanaler, eksekveringsmiljøer eller eksterne afhængigheder, hvorigennem trusler kan opstå

b) muliggør nye angrebsscenarier, herunder f.eks. nye måder, hvorpå uautoriseret adgang, manipulation, indblanding eller misbrug af produktet med digitale elementer eller af data, der behandles af det, med rimelighed kan forekomme

c) ændrer sandsynligheden for tidligere identificerede angrebsscenarier, f.eks. ved at mindske den indsats eller ekspertise, der kræves for at udnytte dem, øge eksponeringen for ikkebetroede aktører eller svække eksisterende sikkerhedsforanstaltninger

d) ændrer tidligere identificerede angrebsscenariers mulige indvirkning, herunder f.eks. omfanget af berørte data eller funktioner, alvoren af driftsmæssige, sikkerhedsmæssige eller økonomiske konsekvenser eller mulighederne for at opdage og inddæmme hændelser og reetablere systemerne efterfølgende.

111. I nogle tilfælde medfører en softwareopdatering ikke nye trusselsvektorer, muliggør ikke nye angrebsscenarier og ændrer ikke væsentligt sandsynligheden for eller indvirkningen af tidligere identificerede angrebsscenarier. Dette kan indikere, at opdateringen ikke medfører nye eller øgede cybersikkerhedsrisici, forudsat at de antagelser og risikobegrænsende foranstaltninger, der blev lagt til grund i risikovurderingen, fortsat er gyldige og effektive. Det er derfor sandsynligt, at opdateringen ikke betegnes som en væsentlig ændring.

112. Omvendt kan en softwareopdatering medføre nye trusselsvektorer, muliggøre nye angrebsscenarier eller væsentligt ændre sandsynligheden for eller indvirkningen af eksisterende angrebsscenarier. I sådanne tilfælde bør fabrikanten revurdere cybersikkerhedsrisiciene ved produktet med digitale elementer og fastslå, om de væsentlige krav fortsat opfyldes, herunder om opdateringen medfører nye eller øgede risici, der ikke var forudset i risikovurderingen.

113. Hvorvidt en softwareopdatering betegnes som en væsentlig ændring, er relevant ved afgørelsen af, om visse forpligtelser i henhold til CRA finder anvendelse, jf. punkt 91. Uanset denne vurderinger fabrikanterne imidlertid fortsat ansvarlige for at garantere sikkerheden ved softwareopdateringer og ved produkterne med digitale elementer i vedligeholdelsesperioden i overensstemmelse med kravene til håndtering af sårbarheder i del II i bilag I til CRA. Uanset om softwareopdateringer betegnes som væsentlige ændringer eller ej, skal fabrikanterne desuden holde risikovurderingen og den tekniske dokumentation nøjagtig, fuldstændig og ajour i overensstemmelse med artikel 13, stk. 7, og artikel 31, stk. 2.

4.4. **Konsekvenser af en væsentlig ændring**

114. Konsekvenserne af en væsentlig ændring, der foretages af en anden aktør end den oprindelige fabrikant af et produkt med digitale elementer, der allerede er bragt i omsætning, behandles i artikel 21 og 22 i CRA. Artikel 21 vedrører importører og distributører, mens artikel 22 vedrører enhver fysisk eller juridisk person, der ikke er fabrikanten, importøren eller distributøren.

115. Hvis den væsentlige ændring foretages af den oprindelige fabrikant af produktet med digitale elementer, følger konsekvenserne af det almindeligt etablerede begreb væsentlig ændring, der er omhandlet i betragtning 41 i CRA, og uddybes yderligere i afsnit 2.1 i den blå vejledning. I nævnte afsnit anføres det, at et produkt, der har været genstand for væsentlige ændringer eller en revision, efter at det er taget i brug, skal betragtes som et nyt produkt, hvis dets oprindelige ydeevne, formål eller type er blevet ændret, arten af faren er ændret eller risikoniveauet er steget, og produktet med digitale elementer gøres tilgængeligt på markedet.

116. Den almindeligt etablerede konsekvens er derfor, at hvis en ændring af et produkt med digitale elementer vurderes som en væsentlig ændring, og det ændrede produkt med digitale elementer gøres tilgængeligt på markedet, skal det behandles som et nyt produkt med digitale elementer for så vidt angår CRA. Som følge heraf udgør tilgængeliggørelsen på markedet af det væsentligt ændrede produkt en ny bringen i omsætning. Dette gælder, uanset om den væsentlige ændring foretages af den oprindelige fabrikant eller af en anden person. For at sikre, at CRA anvendes på en ensartet og forholdsmæssig måde på tværs af de forskellige kategorier af aktører, der kan foretage en væsentlig ændring, behandles i de følgende underafsnit de deraf følgende forpligtelser for den person, der foretager den væsentlige ændring, når det væsentligt ændrede produkt med digitale elementer bringes i omsætning. Konsekvenserne for vedligeholdelsesperioden for produktet med digitale elementer behandles i afsnit *5 Vedligeholdelsesperiode*.

4.4.1. *Væsentlige ændringer foretaget af en anden person end den oprindelige fabrikant*

117. I overensstemmelse med artikel 21 og 22 skal den person, der foretager en væsentlig ændring af et produkt med digitale elementer, der allerede er bragt i omsætning, og gør det ændrede produkt med digitale elementer tilgængeligt på markedet, anses for at være fabrikanten af det ændrede produkt med digitale elementer, hvis den væsentlige ændring foretages af en anden fysisk eller juridisk person end fabrikanten af produktet med digitale elementer, uanset om den pågældende person var involveret i den oprindelige udformning eller bringen i omsætning af produktet.

118. I artikel 22 præciseres det endvidere, at den person, der foretager ændringen, kun er omfattet af forpligtelserne i artikel 13 og 14 for så vidt angår den del af produktet med digitale elementer, der er berørt af den væsentlige ændring, hvis ændringen ikke påvirker cybersikkerheden i produktet med digitale elementer som helhed.

119. Hvis en væsentlig ændring påvirker overholdelsen af de væsentlige krav, men ikke påvirker cybersikkerheden i produktet med digitale elementer som helhed negativt, er den person, der foretager ændringen, kun omfattet af artikel 13 (herunder forpligtelsen til at sikre overholdelse af de væsentlige krav og til at gennemføre en overensstemmelsesvurderingsprocedure) og artikel 14 (indberetningsforpligtelser) for så vidt angår den del af produktet med digitale elementer, der er blevet væsentligt ændret ([16]). Desuden finder den oprindelige fabrikants forpligtelser i henhold til CRA fortsat anvendelse på det oprindelige produkt med digitale elementer, der er bragt i omsætning, hvorved der sikres kontinuitet i håndteringen af sårbarheder og overholdelsen for de uændrede dele.

120. En væsentlig ændring bør ikke forveksles med integration af flere elementer, hvor en person samler komponenter (herunder, hvor det er relevant, ved at ændre dem) til et nyt produkt med digitale elementer, som vedkommende selv bringer i omsætning. I sådanne tilfælde ændrer integratoren ikke et produkt med digitale elementer, der allerede er bragt i omsætning af en anden fabrikant, men bringer derimod integratorens eget nye produkt med digitale elementer i omsætning. Integratoren er fabrikant af det pågældende nye produkt med digitale elementer for så vidt angår CRA og skal overholde forordningen i sin helhed for så vidt angår produktet med digitale elementer som helhed. Hvis fabrikanten integrerer komponenter, der er omfattet af CRA, kan vedkommende støtte sig til komponentfabrikanternes aktiviteter med henblik på overholdelse for at lette sin egen overholdelse af CRA.

Eksempel 51: En virksomhed køber standardmikrocontrollermoduler og konnektivitetskomponenter fra tredjepartsleverandører, udvikler proprietær firmware og en sensorpakke og samler dem til et opkoblet produkt med digitale elementer til landbrugsovervågning. Virksomheden bringer produktet i omsætning under eget navn. Selv om virksomheden har ændret de bagvedliggende mikrocontrollermoduler og kombineret dem med andre komponenter, foretager virksomheden ikke en væsentlig ændring af et produkt med digitale elementer, der allerede er bragt i omsætning. Den bringer derimod et nyt produkt med digitale elementer i omsætning. Virksomheden er fabrikant af landbrugsovervågningsproduktet for så vidt angår CRA og skal overholde forordningen for så vidt angår landbrugsovervågningsproduktet som helhed.

([16]) I overensstemmelse med afsnit 2.1 i den blå vejledning »er det ikke nødvendigt at gentage test og udarbejde ny dokumentation i forbindelse med aspekter, der ikke påvirkes af ændringen. Den fysiske eller juridiske person, der foretager ændringer eller får foretaget ændringer af produktet, skal påvise, at ikke alle elementerne i den tekniske dokumentation skal ajourføres. Den fysiske eller juridiske person, der foretager ændringer eller får foretaget ændringer af produktet, er ansvarlig for det ændrede produkts overensstemmelse og skal udarbejde en overensstemmelseserklæring, selv om vedkommende anvender eksisterende test og teknisk dokumentation«.

121. Hvis en væsentlig ændring, der foretages af en anden person end den oprindelige fabrikant, påvirker cybersikkerheden i produktet med digitale elementer som helhed negativt, f.eks. fordi ændringen ikke længere er målrettet mod eller begrænset til en specifik komponent eller et specifikt delsystem, bør det ændrede produkt med digitale elementer, der gøres tilgængeligt på markedet, behandles som et nyt produkt med digitale elementer, der er omfattet af CRA som helhed. I sådanne tilfælde er produktets samlede cybersikkerhedsrisikoprofil ændret, og ændringen kan ikke vurderes, uden at produktet med digitale elementer betragtes som helhed. Den person, der foretager ændringen, er omfattet af de forpligtelser for fabrikanter, der er fastsat i artikel 13 og 14, for så vidt angår det ændrede produkt med digitale elementer som helhed.

4.4.2. *Væsentlige ændringer foretaget af den oprindelige fabrikant*

122. Hvis den væsentlige ændring foretages af den oprindelige fabrikant, herunder i forbindelse med iterativ udvikling af softwareprodukter med digitale elementer, betragtes den oprindelige fabrikant fortsat som fabrikant for så vidt angår CRA. Det væsentligt ændrede produkt med digitale elementer skal imidlertid anses for at være bragt i omsætning på ny.

123. I overensstemmelse med afsnit 2.1 i den blå vejledning kan den oprindelige fabrikant, der bringer det væsentligt ændrede produkt med digitale elementer i omsætning, genanvende eksisterende dokumentation og test for de aspekter af produktet med digitale elementer, der ikke påvirkes af den væsentlige ændring. Navnlig når fabrikanten bringer væsentligt ændrede versioner af det samme produkt med digitale elementer i omsætning, bør der i proceduren til overensstemmelsesvurderinger sættes fokus på de væsentligt ændrede dele af produktet med digitale elementer. På samme måde bør overensstemmelsesvurderingsorganet, når der foretages en tredjepartsoverensstemmelsesvurdering, fokusere sin vurdering på de væsentligt ændrede dele. For uændrede dele af produktet med digitale elementer kan organet genanvende eksisterende dokumentation og testresultater.

124. De proportionalitetshensyn, der er fastsat i det foregående underafsnit, finder tilsvarende anvendelse på væsentlige ændringer, der foretages af den oprindelige fabrikant af et produkt med digitale elementer, der er bragt i omsætning før den 11. december 2027. En sådan væsentlig ændring, der foretages af den oprindelige fabrikant, kræver ikke i sig selv, at fabrikanten bringer hele det produkt med digitale elementer, der er bragt i omsætning før denne dato, i fuld overensstemmelse med CRA, medmindre ændringen påvirker cybersikkerheden i produktet med digitale elementer som helhed negativt. Hvis ændringen ikke påvirker cybersikkerheden i produktet med digitale elementer som helhed, bør den oprindelige fabrikants forpligtelser med hensyn til ændringen begrænses til de væsentligt ændrede dele.

5. **VEDLIGEHOLDELSESPERIODE**

125. I artikel 13, stk. 8, i CRA fastsættes det, at fabrikanterne skal fastsætte vedligeholdelsesperioden, hvor sårbarheder i produktet med digitale elementer, herunder dets komponenter, håndteres effektivt og i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I, del II. Vedligeholdelsesperioden afspejler det tidsrum, som produktet med digitale elementer forventes at være i brug i (den forventede anvendelsestid), og bør fastsættes i lyset af kriterierne i artikel 13, stk. 8, navnlig rimelige brugerforventninger, produktets art, herunder dets tilsigtede formål, samt relevant EU-ret, der fastsætter levetiden for produkter med digitale elementer ([17]). Samlet set skal der tages hensyn til sådanne kriterier på en måde, der sikrer proportionalitet ved fastsættelse af vedligeholdelsesperioden.

([17]) Yderligere kriterier, der i overensstemmelse med artikel 13, stk. 8, kan tages i betragtning, omfatter vedligeholdelsesperioderne for produkter med digitale elementer, der tilbyder en lignende funktionalitet, og som er bragt i omsætning af andre fabrikanter, tilgængeligheden af driftsmiljøet, vedligeholdelsesperioderne for integrerede komponenter, der leverer kernefunktioner og stammer fra tredjeparter, samt relevant vejledning fra den administrative samarbejdsgruppe for CRA (ADCO) og Kommissionen.

126. Det kræves endvidere i artikel 13, stk. 8, at vedligeholdelsesperioden er på mindst 5 år, medmindre produktet med digitale elementer forventes at være i brug i mindre end 5 år, i hvilket tilfælde vedligeholdelsesperioden skal svare til den forventede anvendelsestid. Den minimale vedligeholdelsesperiode fungerer derfor kun som en sikkerhedsforanstaltning, der sikrer, at sårbarheder håndteres i en tilstrækkeligt lang periode, samtidig med at fabrikanterne kan håndtere produkter med digitale elementer med kortere forventede anvendelsestider. I betragtning 60 gives yderligere vejledning i denne henseende, idet det præciseres, at produkter med digitale elementer, der med rimelighed forventes at være i brug i mere end 5 år, bør have længere vedligeholdelsesperioder. En vedligeholdelsesperiode på 5 år skal derfor ikke betragtes som standarden for alle produkter med digitale elementer. I stedet bør fabrikanten fastsætte den passende vedligeholdelsesperiode i lyset af de kriterier, der er omhandlet i artikel 13, stk. 8.

127. I artikel 13, stk. 19, kræves det, at fabrikanterne på købstidspunktet på en klar og forståelig måde angiver vedligeholdelsesperiodens slutdato (som minimum måned og år). I bestemmelsen kræves det også, at fabrikanterne sender meddelelse til brugerne, når vedligeholdelsesperioden udløber, hvis dette er teknisk muligt under hensyntagen til typen af produkt med digitale elementer. Denne forpligtelse har til formål at give brugerne gennemsigtighed med hensyn til den periode, hvor der kan forventes sikkerhedsvedligeholdelse.

128. For softwareprodukter med digitale elementer, som ofte udvikles og frigives iterativt, og hvor væsentligt ændrede versioner hyppigt kan bringes i omsætning over tid, skal vedligeholdelsesperioden forstås under hensyntagen til denne udviklingsmodel. Hver væsentligt ændret version af et softwareprodukt med digitale elementer, der bringes i omsætning, skal have en angivet vedligeholdelsesperiode, der er i overensstemmelse med artikel 13, stk. 8. Dette omfatter den minimale vedligeholdelsesperiode på mindst 5 år, medmindre den forventede anvendelsestid for den pågældende version bevisligt er kortere, som det også præciseres i betragtning 60. I afsnit *5.1 Væsentlige ændringer og vedligeholdelsesperioden* præciseres det endvidere, at hvis den væsentlige ændring ikke medfører ændringer i de faktorer, der oprindeligt bestemte den forventede anvendelsestid for produktet med digitale elementer, påvirkes den oprindelige vedligeholdelsesperiode ikke (dvs. også i tilfælde, hvor den resterende vedligeholdelsesperiode er mindre end 5 år).

129. Artikel 13, stk. 10, giver fleksibilitet for softwareprodukter med digitale elementer ved under visse betingelser at tillade fabrikanterne kun at sikre overholdelse af kravet til sårbarhedshåndtering i bilag I, del II, nr. 2, (håndtering og afhjælpning af sårbarheder) for den version af softwareproduktet med digitale elementer, der senest er bragt i omsætning. Dette er tilladt, når brugere af tidligere versioner uden vederlag har adgang til den version, der senest er bragt i omsætning, og ikke pådrager sig yderligere omkostninger til at tilpasse det hardware- og softwaremiljø, hvori de anvender produktets oprindelige version.

130. Med henblik på artikel 13, stk. 10, bør begrebet »yderligere omkostninger« fortolkes på en praktisk og forholdsmæssig måde under hensyntagen til normal og forventet praksis for vedligeholdelse og drift af software. Det omfatter ikke en rimelig driftsmæssig indsats, der er uløseligt forbundet med at anvende softwareopdateringer eller opretholde et sikkert driftsmiljø, såsom personaletid, rutinemæssig test, konfigurationsjusteringer eller opgraderinger af underliggende softwareafhængigheder, der er nødvendige for at håndtere komponenter, hvis levetid er udløbet, eller kendte sikkerhedssårbarheder. Derimod henviser »yderligere omkostninger« til udgifter ud over det, der normalt kan forventes i forbindelse med softwareopdateringer, såsom obligatorisk køb af ny hardware, udskiftning af infrastruktur eller grundlæggende ændringer af driftsmiljøet.

131. For softwareprodukter med digitale elementer, der løbende udvikles, kan fabrikanter bringe på hinanden følgende væsentligt ændrede versioner i omsætning med relativt korte intervaller og forvente, at brugerne opgraderer regelmæssigt. I sådanne tilfælde skal den angivne vedligeholdelsesperiode for hver væsentligt ændret version være i overensstemmelse med artikel 13, stk. 8, på det tidspunkt, hvor den bringes i omsætning. Med andre ord skal fabrikanten angive en ny vedligeholdelsesperiode for den pågældende væsentligt ændrede version. Fabrikanter kan dog anvende artikel 13, stk. 10, til at ophøre med at håndtere og afhjælpe sårbarheder i tidligere versioner, når

brugerne kan opgradere til en senere version uden vederlag og uden at pådrage sig yderligere omkostninger som omhandlet ovenfor, selv om dette resulterer i en kortere reel vedligeholdelsesperiode for disse tidligere versioner ([18]). Fabrikanten er fortsat underlagt de øvrige krav til sårbarhedshåndtering i bilag I, del II, samt indberetningsforpligtelserne i artikel 14. Som også forklaret i betragtning 40 omfatter disse krav bl.a. følgende for alle efterfølgende væsentligt ændrede versioner af softwareproduktet med digitale elementer, der bringes i omsætning: i) opretholdelse af en politik for koordineret offentliggørelse af sårbarheder og ii) foranstaltninger, der letter deling af oplysninger om mulige sårbarheder ([19]).

Eksempel 52: En fabrikant bringer en smartphonemodel i omsætning på EU-markedet og angiver en vedligeholdelsesperiode på X år fra den dato, hvor modellen bringes i omsætning, hvor fabrikanten leverer sikkerhedsopdateringer, der afhjælper sårbarheder. I denne periode udsender fabrikanten regelmæssige softwareopdateringer og væsentligt ændrede versioner af operativsystemet, som brugerne kan installere uden vederlag og uden krav om ny hardware.

Fabrikanten kan i overensstemmelse med artikel 13, stk. 10, håndtere og afhjælpe sårbarheder for den seneste version af operativsystemet, der er gjort tilgængelig for den pågældende smartphonemodel, forudsat at tidligere versioner kan opgraderes uden vederlag og uden yderligere omkostninger. I hele vedligeholdelsesperioden er fabrikanten fortsat underlagt de øvrige krav til sårbarhedshåndtering, såsom koordineret offentliggørelse af sårbarheder og foranstaltninger til deling af oplysninger.

Eksempel 53: En fabrikant bringer et softwareprodukt med digitale elementer til virksomheder i omsætning og udsender væsentligt ændrede versioner med få måneders mellemrum, som afspejler sikkerhedsforbedringer, nye funktioner og kompatibilitet med opdaterede operativsystemer og platforme. Hver version bringes i omsætning med en angivet vedligeholdelsesperiode i overensstemmelse med artikel 13, stk. 8. Fabrikanten forventer, at brugerne opgraderer regelmæssigt som led i normal drift, og giver adgang til den seneste version uden vederlag. Gennemførelse af opgraderinger kan kræve en rimelig driftsmæssig indsats, såsom test eller konfigurationsjusteringer, men kræver ikke yderligere omkostninger, såsom køb af ny hardware eller grundlæggende infrastrukturændringer. I denne sammenhæng kan fabrikanten henholde sig til artikel 13, stk. 10, og ophøre med at håndtere og afhjælpe sårbarheder i tidligere versioner, når brugerne kan opgradere til den seneste version, samtidig med at fabrikanten fortsat overholder de øvrige krav til sårbarhedshåndtering for alle efterfølgende væsentligt ændrede versioner.

5.1. **Væsentlige ændringer og vedligeholdelsesperioden**

132. Som anført i afsnit 4.4 *Konsekvenser af en væsentlig ændring*, skal en ændring af et produkt med digitale elementer, hvis den udgør en væsentlig ændring, og det ændrede produkt med digitale elementer gøres tilgængeligt på markedet, behandles som et nyt produkt for så vidt angår CRA, og det at gøre det væsentligt ændrede produkt med digitale elementer tilgængeligt på markedet udgør en ny bringen i omsætning. Det er derfor nyttigt at præcisere, hvilken virkning denne nye bringen i omsætning har på vedligeholdelsesperioden for det væsentligt ændrede produkt med digitale elementer.

133. Vedligeholdelsesperioden for et væsentligt ændret produkt med digitale elementer bør fastsættes med udgangspunkt i produktets forventede anvendelsestid i lyset af kriterierne i artikel 13, stk. 8, i CRA. En væsentlig ændring bør derfor kræve en fornyet vurdering på grundlag af disse kriterier, men medfører ikke automatisk, at vedligeholdelsesperioden nulstilles eller forlænges. Det relevante spørgsmål er, om den væsentlige ændring påvirker de faktorer, der oprindeligt bestemte produktets forventede anvendelsestid og dermed den oprindelige vedligeholdelsesperiode.

([18]) Det bør erindres, at artikel 13, stk. 19, fastsætter krav om, at fabrikanterne, hvor det er teknisk muligt i lyset af arten af produktet med digitale elementer, viser en meddelelse til brugerne om, at deres produkt med digitale elementer har nået slutningen af vedligeholdelsesperioden. Hvis håndteringen og afhjælpningen af sårbarheder i tidligere versioner ophører, forventes det derfor, at brugere, der ikke har opgraderet til den nyeste version, informeres, hvis det er teknisk muligt.

([19]) Det bør bemærkes, at selv om brugerne kan opgradere til den seneste version af softwaren uden yderligere omkostninger, kan fabrikanterne ikke desto mindre vælge at fortsætte med at håndtere og afhjælpe sårbarheder i tidligere versioner af den pågældende software, herunder mod betaling eller i henhold til andre kommercielle ordninger. CRA kræver ikke, at fabrikanterne leverer sikkerhedsopdateringer til sådanne tidligere versioner uden vederlag.

134. Hvis den væsentlige ændring ikke påvirker disse faktorer, angiver kriterierne i henhold til artikel 13, stk. 8, fortsat den samme forventede anvendelsestid som oprindeligt fastsat, og vedligeholdelsesperioden for det ændrede produkt med digitale elementer bør svare til den resterende forventede anvendelsestid for produktet, som det oprindeligt blev bragt i omsætning. Dette vil typisk være tilfældet, når den forventede anvendelsestid primært blev fastsat ud fra faktorer, som ændringen ikke påvirker, såsom hardwarekomponenters fysiske holdbarhed, når den væsentlige ændring kun vedrører softwarefunktionalitet eller backendtjenester.

Eksempel 54: *En fabrikant bringer en robotstøvsuger med en forventet anvendelsestid på X år i omsætning. Anvendelsestiden er fastsat på grundlag af typen af produkt med digitale elementer, herunder hardwarekomponenternes fysiske holdbarhed og slitageegenskaber, og under hensyntagen til rimelige brugerforventninger med hensyn til produktets levetid. Fabrikanten fastsætter en vedligeholdelsesperiode på X år. Efter Y år udsender fabrikanten en softwareopdatering, der udgør en væsentlig ændring, og hvor nye rengøringstilstande og navigationsfunktioner tilføjes. Softwareopdateringen påvirker ikke hardwarens fysiske holdbarhed og ændrer ikke brugernes rimelige forventninger med hensyn til produktets levetid. Kriterierne i henhold til artikel 13, stk. 8, angiver derfor fortsat den samme forventede anvendelsestid. Vedligeholdelsesperioden for det ændrede produkt med digitale elementer svarer til den resterende forventede anvendelsestid som oprindeligt fastsat.*

Eksempel 55: En fabrikant bringer et komplekst industrimaskinprodukt med digitale elementer i omsætning med en cloudbaseret backend, der udgør en fjerndatabehandlingsløsning. Den forventede anvendelsestid er X år, fastsat i lyset af rimelige brugerforventninger og typen af produktet med digitale elementer, såsom maskinhardwarens fysiske holdbarhed og forventet slitage. Vedligeholdelsesperioden fastsættes til at svare til denne forventede anvendelsestid på X år. Efter Y år ændrer fabrikanten arkitekturen for den cloudbaserede backend (fjerndatabehandlingsløsningen) ved at indføre nye API'er og datastrømme på en måde, der udgør en væsentlig ændring af produktet med digitale elementer, men ikke ændrer produktets art eller påvirker brugernes forventninger. Kriterierne i henhold til artikel 13, stk. 8, angiver derfor fortsat den samme forventede anvendelsestid. Vedligeholdelsesperioden for det ændrede produkt med digitale elementer svarer til den resterende forventede anvendelsestid som oprindeligt fastsat.

135. Hvis den væsentlige ændring påvirker de faktorer, der oprindeligt bestemte den forventede anvendelsestid for produktet med digitale elementer, bør fabrikanten genberegne vedligeholdelsesperioden, så den afspejler den nye forventede anvendelsestid, og anvende kriterierne i artikel 13, stk. 8, i overensstemmelse hermed. Dette kan f.eks. være tilfældet ved hardwareændringer, der udgør en fornyelse af produktet og forlænger dets driftslevetid, eller ved en omfattende omprogrammering eller omskrivning af produktets softwarekerne, som ændrer dets forventede anvendelsestid væsentligt ([20]).

Eksempel 56: En fabrikant bringer en programmerbar logisk styreenhed (PLC) med en forventet anvendelsestid på X år i omsætning; anvendelsestiden er primært fastsat på grundlag af typen af produktet med digitale elementer og den underliggende hardwares holdbarhed. Vedligeholdelsesperioden fastsættes i overensstemmelse hermed. Flere år efter at den oprindeligt blev bragt i omsætning, foretager fabrikanten en væsentlig ændring, der består i udskiftning af PLC'ens indlejrede databehandlingsplatform, herunder processor, hukommelse og kørselsmiljø, med en ny generation af komponenter, der er designet med henblik på en betydeligt længere driftslevetid. Som følge af ændringen ændres de rimelige brugerforventninger og typen af produktet med digitale elementer, og brugeren af PLC'en kan nu med rimelighed forvente, at PLC'en forbliver i produktiv brug ud over dens oprindeligt erklærede forventede anvendelsestid, understøttet af den nye databehandlingsplatform. Kriterierne i henhold til artikel 13, stk. 8, angiver derfor en længere forventet anvendelsestid, og fabrikanten genberegner vedligeholdelsesperioden for den specifikke PLC i overensstemmelse hermed.

6. **VIGTIGE OG KRITISKE PRODUKTER MED DIGITALE ELEMENTER**

136. I artikel 7, stk. 1, i CRA fastsættes det, at produkter med digitale elementer, der har den kernefunktionalitet for en produktkategori, som er fastsat i bilag III til forordningen, anses for at være »vigtige produkter med digitale elementer«. Bilag III opdeler desuden vigtige produkter med digitale elementer i klasse I og klasse II. Tilsvarende fastsættes det i artikel 8, stk. 1, at produkter med digitale elementer, der har den kernefunktionalitet for en produktkategori, som er fastsat i bilag IV til CRA, anses for at være »kritiske produkter med digitale elementer« ([21]).

([20]) Det bør erindres, at renovering, vedligeholdelse eller reparation, som anført i afsnit 4.1 *Physical repairs*, generelt ikke anses for at udgøre væsentlige ændringer.

([21]) Kommissionens gennemførelsesforordning (EU) 2025/2392 fastsætter den tekniske beskrivelse af kategorierne af vigtige og kritiske produkter.

137. Klassificeringen af et produkt med digitale elementer som vigtigt eller kritisk eller omvendt som tilhørende »standardkategorien« ([22]) er relevant ved fastlæggelsen af, hvilken overensstemmelsesvurderingsprocedure fabrikanten skal følge i henhold til artikel 32, før fabrikanten kan bringe produktet med digitale elementer i omsætning. Navnlig kan man for produkter med digitale elementer i standardkategorien altid anvende proceduren for intern kontrol baseret på modul A (»selvvurdering«) ([23]). Vigtige produkter med digitale elementer i klasse I eller II og kritiske produkter med digitale elementer er underlagt strengere overensstemmelsesvurderingsprocedurer. Dette omfatter ikke vigtige produkter med digitale elementer i klasse I eller II, der kan betegnes som fri og open source-software, og som bringes i omsætning, for hvilke fabrikanter i henhold til artikel 32, stk. 5, kan følge procedurerne for standardkategorien.

138. Begrebet kernefunktionalitet er derfor afgørende for, at fabrikanten kan fastlægge den gældende overensstemmelsesvurderingsordning. Dette begreb er imidlertid ikke udtrykkeligt defineret i CRA. Produkter med digitale elementer kan udføre en række funktioner, hvoraf nogle kan være underordnede i forhold til produktets kernefunktionalitet og ikke bør påvirke produktets klassificering som standardprodukt/vigtigt produkt i klasse I/vigtigt produkt i klasse II/kritisk produkt. Det er derfor hensigtsmæssigt at give yderligere vejledning for at hjælpe fabrikanterne med at gennemføre de relevante overensstemmelsesvurderingsprocedurer korrekt og bistå markedsovervågningsmyndighederne med at sikre harmoniseret håndhævelse af CRA i hele EU.

6.1. **Kernefunktionalitet**

139. Ved et produkt med digitale elementers kernefunktionalitet forstås produktets hovedtræk og tekniske kapaciteter, uden hvilke det ikke ville kunne opfylde det tilsigtede formål. Den væsentligste funktionalitet kan vurderes på baggrund af produktets specifikke sammenhæng og anvendelsesbetingelser under hensyntagen til bl.a. de oplysninger, som fabrikanten leverer i brugsanvisningen, reklame- eller salgsmaterialer og erklæringer samt i den tekniske dokumentation.

Eksempel 57: Et softwareprodukt med digitale elementer tilvejebringer et abstraktionslag over den underliggende hardware og administrerer afviklingen af softwarekomponenter. Dets hovedfunktioner omfatter initialisering af hardware og perifere enheder, proces- og hukommelsesstyring, I/O-styring, scheduling, ressourceallokering samt eksponering af systemtjenester og applikationsprogrammeringsgrænseflader (API'er), hvorigennem applikationer interagerer med enhedens hardware- og softwareressourcer. Det fremgår af den tekniske dokumentation, at produktet med digitale elementer orkestrerer beregningsressourcer, håndhæver systemkonfigurationer og stiller standardiserede grænseflader til rådighed for softwaremoduler og tilsluttede perifere enheder. Fabrikanten fremhæver disse egenskaber som det, der gør platformen i stand til at fungere som det centrale softwaremiljø, hvori applikationer kan afvikles pålideligt. Produktet med digitale elementer har et operativsystems kernefunktionalitet som beskrevet i bilag I, punkt 11, til gennemførelsesforordning (EU) 2025/2392.

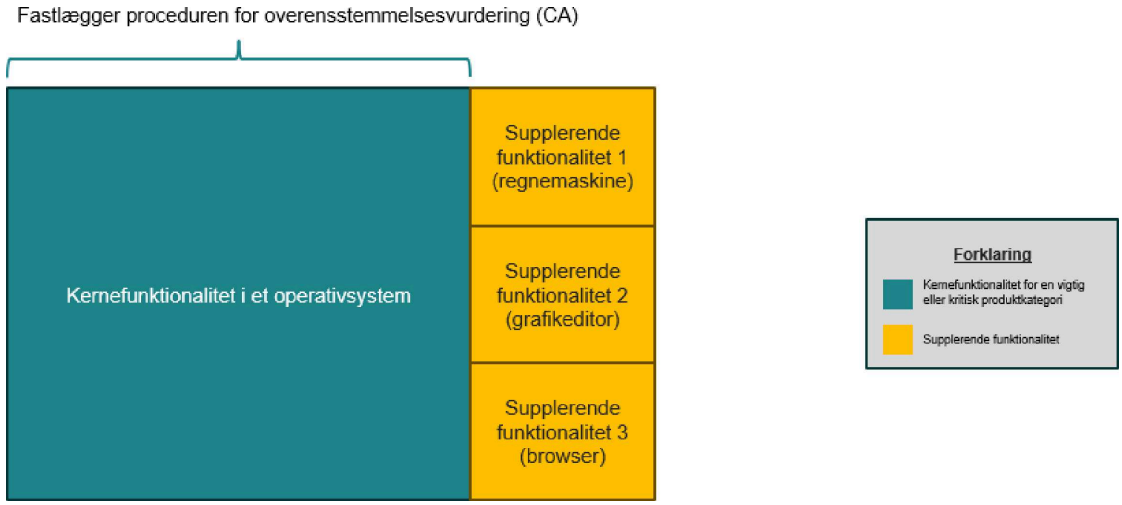
140. Funktionaliteten af et produkt med digitale elementer er sjældent udelukkende begrænset til dets kernefunktionalitet, da produkter med digitale elementer ofte – om ikke altid – udfører yderligere funktioner, som ikke bidrager til produktets kernefunktionalitet. Dette kan også omfatte integration af komponenter, der rummer funktionalitet som et andet vigtigt eller kritisk produkt med digitale elementer. At et produkt med digitale elementer udfører funktioner ud over dem, der er beskrevet i de tekniske beskrivelser for vigtige eller kritiske produkter med digitale elementer, forhindrer dog ikke i sig selv, at produktet har en sådan kernefunktionalitet.

([22]) Udtrykket »standardkategori« er ikke et defineret begreb i CRA. Anvendelsen af begrebet i dette dokument henviser til produkter med digitale elementer, der ikke har den kernefunktionalitet for en produktkategori, som er fastsat i bilag III eller IV til CRA, og som derfor er omfattet af den overensstemmelsesvurderingsordning, der er fastsat i artikel 32, stk. 1.

([23]) Fabrikanten kan dog altid vælge at anvende en strengere overensstemmelsesvurderingsprocedure, jf. artikel 32, stk. 1.

Figur 2:

Illustration af, hvordan kernefunktionaliteten og ikke underordnede funktionaliteter er bestemmende for den gældende overensstemmelsesvurderingsprocedure



141. Et produkt med digitale elementer kan udføre funktioner som tilhører en vigtig eller kritisk produktkategori og samtidig have en kernefunktionalitet, der adskiller sig fra funktionaliteten for en sådan produktkategori. I sådanne tilfælde vil produktet med digitale elementer ikke kunne betegnes som et vigtigt eller kritisk produkt med digitale elementer. Som det udtrykkeligt fremgår af artikel 7, stk. 1, i forordningen om cyberrobusthed for vigtige produkter med digitale elementer (og ved anvendelse af samme logik for kritiske produkter med digitale elementer), medfører den blotte integration af et vigtigt eller kritisk produkt med digitale elementer ikke i sig selv, at produktet med digitale elementer bliver et vigtigt eller kritisk produkt med digitale elementer.

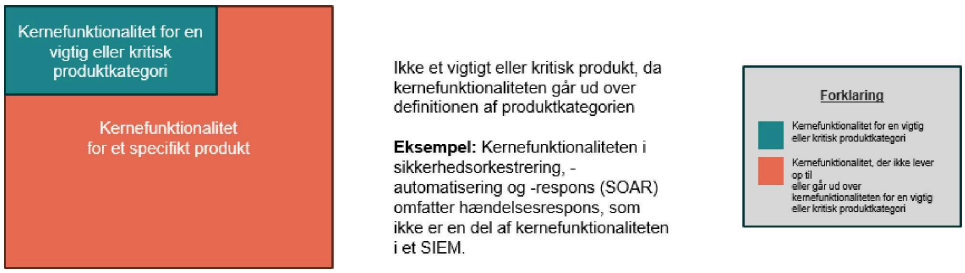
Eksempel 58: En smartphone har et integreret operativsystem, der tilvejebringer de funktionaliteter, der er beskrevet i bilag I, punkt 11, i gennemførelsesforordning (EU) 2025/2392. Selv om operativsystemet muliggør styring af hardwareressourcer og udførelse af softwareapplikationer, har smartphonen som helhed en anden kernefunktionalitet (f.eks. at gøre det muligt for brugerne at kommunikere og få adgang til oplysninger og tjenester). Integration af et operativsystem betyder ikke, at smartphonen har et operativsystems kernefunktionalitet.

142. Nogle produkter med digitale elementer kan ligne en vigtig eller kritisk produktkategori eller tilhøre samme generelle produktfamilie, men deres kernefunktionalitet kan være bredere eller smallere end kernefunktionaliteten for den pågældende kategori. Dette er ikke tilfældet, hvis et produkt med digitale elementer omfatter yderligere funktionaliteter, som blot supplerer eller forbedrer kernefunktionaliteten, der i sig selv svarer til funktionaliteten for en vigtig eller kritisk produktkategori. I sådanne tilfælde anses produktet med digitale elementer for at have den kernefunktionalitet, der svarer til den pågældende kategori og klassificeres i overensstemmelse hermed. Denne vurdering bør baseres på produktets hovedtræk og tekniske kapaciteter, vurderet objektivt i lyset af dets tilsigtede formål, og ikke på den måde, hvorpå produktet med digitale elementer beskrives eller markedsføres, hvis denne beskrivelse ikke afspejler produktets faktiske tekniske karakteristika.

Eksempel 59: Software til sikkerhedsorganisering, -automatisering og -reaktion (SOAR) kan ofte udføre funktionerne i produkter med digitale elementer i kategorien »systemer til sikkerhedsinformations- og hændelseshåndtering (SIEM)«, dvs. indsamle data, analysere dem og præsentere dem som anvendelige oplysninger til sikkerhedsformål. Softwarens kernefunktionalitet går imidlertid væsentligt videre end et SIEM-systems funktionalitet, idet tjenester såsom håndtering af hændelser indgår som centrale elementer i dens tekniske kapaciteter. SOAR-software anses derfor generelt ikke for at have SIEM-systemers kernefunktionalitet.

Figur 3:

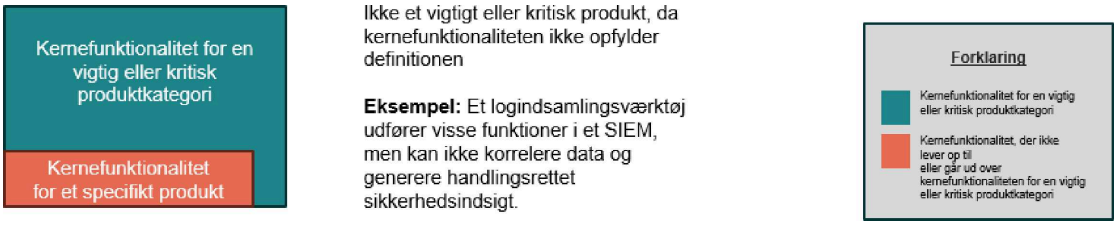
Illustration af, at et produkt med digitale elementers kernefunktionalitet går væsentligt videre end definitionen af en vigtig eller kritisk produktkategori



Eksempel 60: Visse værktøjer til logindsamling og visualisering giver mulighed for at modtage logdata og præsentere grundlæggende dashboards, der viser systemhændelser. Selv om disse værktøjer kan understøtte sikkerhedsovervågningsaktiviteter, er deres kernefunktionalitet lavere end funktionaliteten i SIEM-systemer, da de ikke udfører korrelation af data eller leverer anvendelige oplysninger til sikkerhedsformål Sådanne værktøjer anses derfor generelt ikke for at have SIEM-systemers kernefunktionalitet.

Figur 4:

Illustration af, at kernefunktionaliteteni et produkt med digitale elementer ikke opfylder definitionen af en vigtig eller kritisk produktkategori

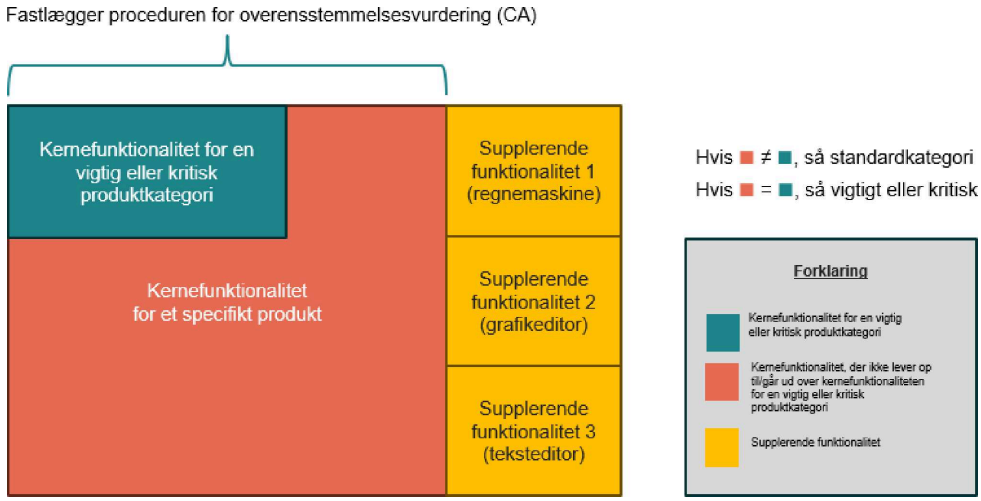


143. En fabrikant må ikke give en urigtig fremstilling af kernefunktionaliteten for et produkt med digitale elementer på en måde, der omgår den overensstemmelsesvurderingsordning, der gælder for vigtige eller kritiske produkter med digitale elementer, f.eks. ved uretmæssigt at fremhæve eller nedtone visse funktionaliteters rolle, således at produktet dækker væsentligt bredere eller smallere en given kernefunktionalitet. Dette vil f.eks. være tilfældet, hvis der er klare uoverensstemmelser mellem reklamematerialer, brugsanvisningen og den tekniske dokumentation.

144. Et produkt med digitale elementer må ikke have mere end én kernefunktionalitet med henblik på at fastlægge den gældende overensstemmelsesvurderingsordning. I overensstemmelse med bilag VII til CRA skal fabrikanter som en del af den tekniske dokumentation for et produkt beskrive det tilsigtede formål med produktet med digitale elementer og den overensstemmelsesvurderingsprocedure, de har fulgt. Produktets kernefunktionalitet bør derfor identificeres klart. Dette gør det muligt at identificere den gældende overensstemmelsesvurderingsordning korrekt og giver markedsovervågningsmyndighederne mulighed for at føre tilsyn med og kontrollere, at forordningen anvendes korrekt.

Figur 5:

Illustration af, hvordan et bestemt produkt med digitale elementers kernefunktionalitet bestemmer produktklassen og dermed den gældende overensstemmelsesvurderingsprocedure



145. Nogle produkter med digitale elementer bringes i omsætning som enkeltprodukter med digitale elementer, men består af særskilte moduler med separate funktionaliteter. Hvis en fabrikant også gør disse moduler tilgængelige på markedet separat, f.eks. hvis de tilbydes til særskilt køb, licensering eller abonnement, udgør disse moduler enkeltstående produkter med digitale elementer. Som sådanne skal de klassificeres på grundlag af deres respektive kernefunktionaliteter (og er derfor underlagt den relevante overensstemmelsesvurderingsordning på grundlag af hvert moduls kernefunktionalitet). Dette berører ikke moduler, der udelukkende leveres som komponenter i et integreret produkt med digitale elementer og ikke gøres tilgængelige separat. I sådanne tilfælde fastlægges kernefunktionaliteten på niveauet for det integrerede produkt med digitale elementer.

Eksempel 61: En fabrikant bringer en samlet sikkerhedssuite i omsætning, som kombinerer flere moduler, herunder et SIEM-system, et system til opdagelse af indtrængen og et analysemodul. Fabrikanten tilbyder også disse moduler som særskilte abonnementer. I dette scenarie er hvert modul et særskilt produkt med digitale elementer og klassificeres på grundlag af modulets væsentligste funktionalitet. SIEM-modulet er omfattet af overensstemmelsesvurderingsordningen for vigtige produkter med digitale elementer i klasse I, da dets kernefunktionalitet er funktionaliteten for »systemer til sikkerhedsinformations- og hændelseshåndtering«. Systemet til opdagelse af indtrængen er omfattet af overensstemmelsesvurderingsordningen for vigtige produkter med digitale elementer i klasse II, da dets kernefunktionalitet er funktionaliteten for »firewalls, systemer til opdagelse og forebyggelse af indtrængen«. Analysemodulet er omfattet af overensstemmelsesvurderingsordningen for produkter med digitale elementer i »standardkategorien«, da dets kernefunktionalitet ikke er funktionaliteten for en vigtig eller kritisk produktkategori.

146. Manglende overholdelse af forpligtelserne i artikel 32 i CRA kan medføre administrative bøder i henhold til artikel 64, stk. 3.

6.2. Overensstemmelsesvurdering af vigtige og kritiske produkter med digitale elementer

147. Når fabrikanten har fastlagt kernefunktionaliteten for fabrikantens produkt med digitale elementer, skal fabrikanten gennemføre en af de gældende overensstemmelsesvurderingsprocedurer. Fabrikanten skal sikre, at produktet med digitale elementer som helhed opfylder de væsentlige krav, idet der, hvor det er relevant, tages hensyn til sikkerheden af de komponenter eller funktionaliteter, der er integreret i det.

148. En strengere overensstemmelsesvurderingsprocedure med inddragelse af en tredjepart (baseret på modul B+C, modul H eller cybersikkerhedscertificeringsordninger) er obligatorisk for vigtige produkter med digitale elementer i klasse II (med undtagelse af dem, der kan betegnes som fri og open source-software, jf. artikel 32, stk. 5) og for kritiske produkter med digitale elementer ([24]). Omvendt skal vigtige produkter med digitale elementer i klasse I (med undtagelse af dem, der kan betegnes som fri og open source-software, jf. artikel 32, stk. 5) kun underkastes en tredjepartsoverensstemmelsesvurderingsprocedure, hvis fabrikanten ikke har anvendt eller kun delvist har anvendt relevante harmoniserede standarder, hvis referencer er offentliggjort i *Den Europæiske Unions Tidende* (i det følgende benævnt »harmoniserede standarder«), fælles specifikationer eller europæiske cybersikkerhedscertificeringsordninger på et tillidsniveau, der som minimum er »betydeligt« ([25]).

149. For at et vigtigt produkt med digitale elementer i klasse I kan være omfattet af den interne kontrolprocedure, skal i) alle de gældende krav i en relevant harmoniseret standard derfor anvendes, og ii) standardens anvendelsesområde skal mindst dække alle de cybersikkerhedsrisici, der er forbundet med produktets kernefunktionalitet.

150. Anvendelsesområdet for produktet med digitale elementer kan være bredere end det anvendelsesområde, der er forudset i den relevante harmoniserede standard, og sådanne yderligere funktioner kan udgøre andre eller yderligere cybersikkerhedsrisici. Fabrikanten skal altid foretage en risikovurdering i henhold til artikel 13, stk. 2, og bør derfor kontrollere, om anvendelsen af en harmoniseret standard dækker alle risici, der er forbundet med produktet med digitale elementer. Hvis anvendelsen af standarden ikke dækker alle risici, bør fabrikanten på anden vis sikre, at det pågældende produkt med digitale elementer er i overensstemmelse med de væsentlige krav.

151. Hvis fabrikanten af et vigtigt produkt med digitale elementer i klasse I har anvendt en relevant harmoniseret standard, der dækker de risici, der er forbundet med produktets kernefunktionalitet, kan fabrikanten derfor beslutte at anvende den interne kontrolprocedure til at påvise produktets overensstemmelse. Som led i fabrikantens overensstemmelsesvurderingsaktiviteter skal denne stadig påvise, at alle risici, der gør sig gældende for fabrikantens produkt med digitale elementer, er håndteret. Hvis der er en forskel mellem dækningen i den harmoniserede standard og anvendelsesområdet for produktet med digitale elementer som helhed, skal fabrikanten derfor fortsat dokumentere, hvilke supplerende foranstaltninger denne har indført for at håndtere disse risici.

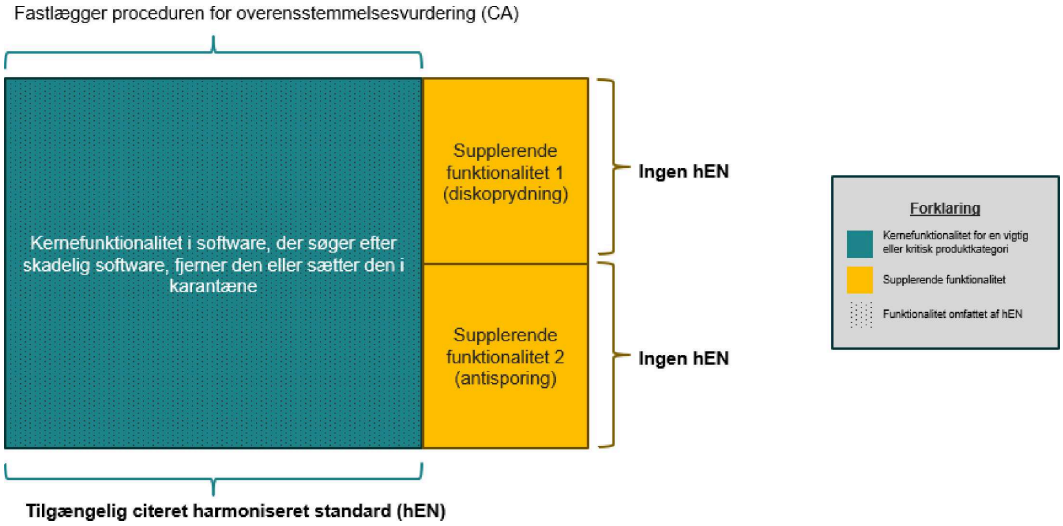
Eksempel 62: En antivirussoftware har som kernefunktionalitet at søge efter, fjerne eller sætte ondsindet software i karantæne, som beskrevet i bilag I, punkt 4, i gennemførelsesforordning (EU) 2025/2392. Dette produkt med digitale elementer omfatter også yderligere funktioner, nemlig en diskoprydnings- og en antitrackingfunktion, der beskytter brugeren under navigation på nettet. Fabrikanten foretager en risikovurdering, der dækker produktet med digitale elementer som helhed, herunder antivirussoftwarens kernefunktionalitet, diskoprydnings- og antitrackingfunktioner. Fabrikanten anvender en harmoniseret standard, der dækker de risici, der er forbundet med antivirussoftwarens kernefunktionalitet, og supplerende foranstaltninger til at håndtere risici, der følger af yderligere funktioner. Fabrikanten kan anvende den interne kontrolprocedure til fabrikantens overensstemmelsesvurdering, der dækker produktet med digitale elementer som helhed, herunder diskoprydningsfunktionen og antitrackingfunktionen.

([24]) Dette gælder også, når der gøres brug af en europæisk cybersikkerhedscertificeringsordning på et tillidsniveau, der som minimum er »betydeligt«, eftersom det kræver inddragelse af et tredjepartscertificeringsorgan.

([25]) For kortheds skyld henvises der i resten af dette afsnit kun til harmoniserede standarder, for hvilke referencer er offentliggjort i *Den Europæiske Unions Tidende*. Den samme vejledning finder dog også anvendelse på fælles specifikationer, der er vedtaget i overensstemmelse med artikel 27, stk. 2, og på europæiske cybersikkerhedscertificeringsordninger, hvor dette er fastsat af Kommissionen ved delegerede retsakter i overensstemmelse med artikel 27, stk. 9.

Figur 6:

Illustration af, hvordan anvendelsen af en harmoniseret standard, for hvilken en reference er offentliggjort, og som kun dækker kernefunktionaliteten, bestemmer den gældende overensstemmelsesvurderingsprocedure



152. Dette er også tilfældet, hvor produktet med digitale elementer integrerer en yderligere funktion, som i sig selv svarer til funktionen i et andet vigtigt eller kritisk produkt med digitale elementer. Det er nemlig produktet med digitale elementers kernefunktionalitet som helhed og ikke funktionaliteten i de integrerede komponenter betragtet isoleret, der afgør, om produktet med digitale elementer tilhører en vigtig eller kritisk produktkategori (og dermed den gældende overensstemmelsesvurderingsordning). Hvis eksempelvis et produkt med digitale elementer har samme kernefunktionalitet som et vigtigt produkt med digitale elementer i klasse I, er produktet som helhed omfattet af den overensstemmelsesvurderingsordning, der gælder for vigtige produkter med digitale elementer i klasse I, selv om det har en integreret komponent, der i sig selv er et kritisk produkt med digitale elementer. I disse tilfælde kan fabrikanten, når denne anvender en harmoniseret standard, der dækker de risici, der er forbundet med produktets kernefunktionalitet, anvende den interne kontrolprocedure.

Eksempel 63: Et hardwareprodukt med digitale elementer har en routers kernefunktionalitet, som beskrevet i bilag I, punkt 12, i gennemførelsesforordning (EU) 2025/2392. Dette produkt med digitale elementer omfatter også yderligere funktionaliteter, herunder firewallfunktioner, idet det har en integreret firewallkomponent. Fabrikanten foretager en risikovurdering, der dækker produktet med digitale elementer som helhed, herunder routerens kernefunktionalitet og firewallfunktionaliteten. Fabrikanten anvender en harmoniseret standard, som dækker de risici, der er forbundet med routerens kernefunktionalitet, og supplerende foranstaltninger til at håndtere risici, der følger af yderligere funktioner. Fabrikanten kan f.eks. anvende den harmoniserede standard for firewalls til at dække de risici, der er forbundet med firewallfunktionaliteten. Fabrikanten kan anvende den interne kontrolprocedure til overensstemmelsesvurderingen, der dækker produktet med digitale elementer som helhed, herunder firewallfunktionaliteten.

6.3. Betydning for formodningen om overensstemmelse

153. I artikel 27, stk. 1, i CRA fastsættes det, at produkter med digitale elementer og de processer, som fabrikanten har indført, og som er i overensstemmelse med harmoniserede standarder eller dele heraf, for hvilke referencer er offentliggjort i *Den Europæiske Unions Tidende (EUT)*, formodes at være i overensstemmelse med de væsentlige krav i CRA, der er omfattet af disse standarder eller dele heraf ([26]). Artikel 27, stk. 5, indebærer en udvidelse af den samme

([26]) Som det klart fremgår af afsnit 4.1.2.2 i den blå vejledning, er en fabrikant i henhold til risikorelateret harmoniseringslovgivning [...] altid, også selv om han anvender harmoniserede standarder, fuldt ud ansvarlig for at vurdere alle de risici, der er forbundet med hans produkt, med henblik på at fastlægge, hvilke væsentlige (eller andre) krav der gælder. Efter denne vurdering kan en fabrikant derefter vælge at anvende tekniske specifikationer, der er anført i harmoniserede standarder, hvis referencer er offentliggjort i *Den Europæiske Unions Tidende*, til at gennemføre »risikobegrænsende foranstaltninger«, som er specificeret i harmoniserede standarder.

formodning om overensstemmelse til at omfatte produkter med digitale elementer og processer, som fabrikanten har indført, og som er i overensstemmelse med fælles specifikationer, der er vedtaget af Kommissionen ved gennemførelsesretsakter, og artikel 27, stk. 8, fastlægger formodningen om overensstemmelse for produkter med digitale elementer og processer, som fabrikanten har indført, for hvilke der er udstedt en EU-overensstemmelseserklæring eller et certifikat i henhold til en europæisk cybersikkerhedscertificeringsordning vedtaget i henhold til forordning (EU) 2019/881, hvis dette er fastsat ved delegerede retsakter i overensstemmelse med artikel 27, stk. 9 ([27]).

154. Hvis fabrikanten har anvendt en harmoniseret standard, for hvilken referencer er offentliggjort i EUT, opnår fabrikanten derfor en formodning om overensstemmelse for de risici, der er dækket af den pågældende standard. Dette kan f.eks. være tilfældet, hvor den harmoniserede standard, der henvises til, omhandler alle de risici, som er forbundet med et produkt med digitale elementers kernefunktionalitet, og der ikke er yderligere funktionaliteter, der udgør cybersikkerhedsrisici. Det forventes f.eks., at den harmoniserede standard for routere mindst omhandler de risici, der er forbundet med disse produkter med digitale elementers kernefunktionalitet. Hvis et sådant produkt ikke indeholder yderligere funktionaliteter, eller hvis disse yderligere funktionaliteter ikke udgør risici, som ikke er omhandlet i standarden, kan produktet med digitale elementer være omfattet af en formodning om overensstemmelse.

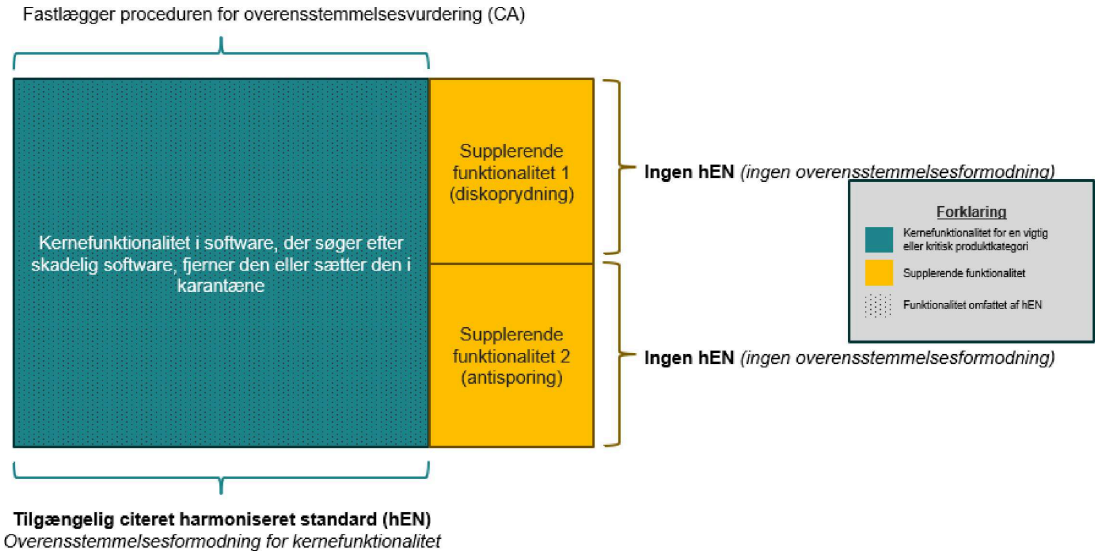
155. I de tilfælde, der er behandlet i punkt 151 og 152, kan fabrikanten anvende den interne kontrolprocedure, fordi den harmoniserede standard dækker de risici, der er forbundet med produktet med digitale elementers kernefunktionalitet. De produkter med digitale elementer, der er beskrevet i disse eksempler, kan dog have et bredere anvendelsesområde end de harmoniserede standarders anvendelsesområde, og yderligere funktionaliteter kan udgøre cybersikkerhedsrisici, der ikke er omhandlet i en sådan harmoniseret standard. Disse produkter med digitale elementer er derfor muligvis ikke omfattet af en formodning om overensstemmelse for disse yderligere funktionaliteter.

Eksempel 64: Antivirussoftware har som kernefunktionalitet at søge efter, fjerne eller sætte ondsindet software i karantæne, og de risici, der er forbundet med denne kernefunktionalitet, er dækket af den harmoniserede standard. Dette produkt med digitale elementer omfatter også yderligere funktionaliteter, nemlig en diskoprydningsfunktion og en antitrackingfunktionalitet, der beskytter brugeren under navigation på nettet, og de risici, der er forbundet med disse funktionaliteter, er ikke dækket af den harmoniserede standard. Hvis den harmoniserede standard anvendes, kan fabrikanten anvende den interne kontrolprocedure til overensstemmelsesvurderingen. Produktet er dermed omfattet af en formodning om overensstemmelse for de risici, der er forbundet med produktets kernefunktionalitet, men ikke for de risici, der er forbundet med yderligere funktionaliteter.

([27]) Som ovenfor henvises der for kortheds skyld i resten af dette afsnit kun til harmoniserede standarder, for hvilke referencer er offentliggjort i *Den Europæiske Unions Tidende*. Den samme vejledning finder dog også anvendelse på fælles specifikationer og på europæiske cybersikkerhedscertificeringsordninger.

Figur 7:

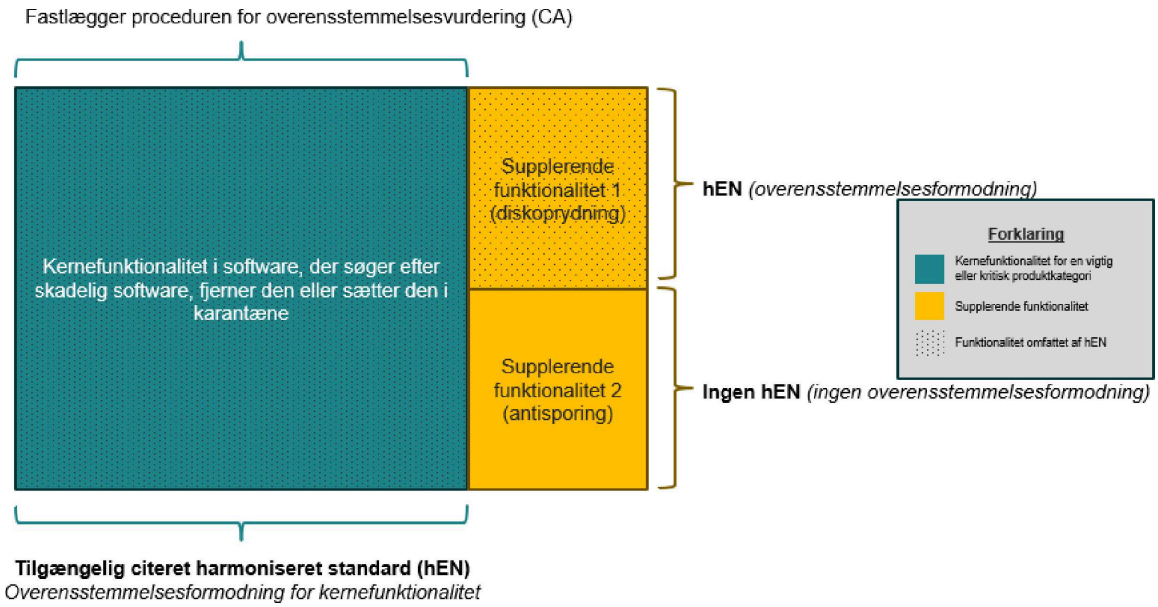
Den harmoniserede standard indebærer formodning om overensstemmelse (PoC) for kernefunktionaliteten, da den omhandler alle risici, der er forbundet med denne kernefunktionalitet, men ikke for accessoriske funktionaliteter



Eksempel 65: I samme scenarie som i det foregående eksempel er den harmoniserede standard nu blevet ajourført, så den også dækker risici, der er forbundet med den ene af de yderligere funktionaliteter, nemlig diskoprydningsfunktionen, men ikke risici forbundet med den anden (dvs. antitrackingfunktionen). Hvis den harmoniserede standard anvendes, kan fabrikanten anvende den interne kontrolprocedure til overensstemmelsesvurderingen. Produktet er omfattet af en formodning om overensstemmelse for de risici, der er forbundet med produktets kernefunktionalitet og diskoprydningsfunktionaliteten, men ikke for de risici, der er forbundet med antitrackingfunktionaliteten.

Figur 8:

Den harmoniserede standard indebærer formodning om overensstemmelse for kernefunktionaliteten og den accessoriske funktionalitet 1, da den omhandler alle risici, der er forbundet med disse to funktionaliteter, men ikke for den accessoriske funktionalitet 2



7. CYBERSIKKERHEDSRISIKOVURDERING OG INTEGRATION AF PRODUKTER MED DIGITALE ELEMENTER OG KOMPONENTER

7.1. Om vurdering og behandling af cybersikkerhedsrisici

156. Gennem den cybersikkerhedsrisikovurdering, der er omhandlet i artikel 13, stk. 2, i CRA, pålægges fabrikanter at identificere relevante risici og vurdere deres mulige indvirkning på produktet med digitale elementer. Fabrikanterne skal også gennemføre passende foranstaltninger til at imødegå disse risici i overensstemmelse med de væsentlige krav i bilag I.

157. I organisatorisk risikostyring vurderes risici almindeligvis ud fra acceptkriterier, der er afledt af organisationens interne mål eller risikovillighed. I henhold til CRA skal den resterende cybersikkerhedsrisiko derimod vurderes på baggrund af kravet om, at det produkt med digitale elementer, der bringes i omsætning, sikrer et passende cybersikkerhedsniveau på grundlag af de foreliggende risici, idet der tages hensyn til produktets tilsigtede formål og rimeligt forventelige anvendelse.

158. Fabrikantens interne risikotolerance, forretningsstrategi eller blotte omkostningsovervejelser er derfor ikke relevante for afgørelsen af, om de foreliggende risici er blevet imødegået. Med henblik på artikel 13, stk. 2 og 3, skal fabrikanter være i stand til at afgøre, om identificerede cybersikkerhedsrisici er blevet tilstrækkeligt imødegået gennem gennemførelsen af de væsentlige krav i bilag I, del I, i lyset af det tilsigtede formål, den rimeligt forventelige anvendelse og anvendelsesbetingelserne, herunder, hvor det er relevant, driftsmiljøet (f.eks. de tilsigtede brugere af produktet med digitale elementer) og de aktiver, der skal beskyttes, idet der tages hensyn til, hvor længe produktet med digitale elementer forventes at være i brug.

159. Den resterende cybersikkerhedsrisiko er et iboende resultat af risikovurdering og risikobehandling. Det anerkendes, at cybersikkerhedsrisici i praksis ikke kan elimineres fuldstændigt. Forekomst af restrisiko indebærer imidlertid ikke, at enhver risiko kan accepteres efter fabrikantens skøn. Et produkt med digitale elementer må kun bringes i omsætning, hvis de resterende risici, når der er truffet passende foranstaltninger, er blevet tilstrækkeligt imødegået gennem gennemførelsen af de væsentlige krav, under hensyntagen til det tilsigtede formål med og den rimeligt forventelige anvendelse af produktet med digitale elementer.

160. I overensstemmelse med artikel 13, stk. 3, skal fabrikanter, når cybersikkerhedsrisici identificeres, imødegå dem ved hjælp af passende foranstaltninger, herunder på produktniveau. Afhængigt af omstændighederne kan dette f.eks. indebære, at angrebsfladen reduceres, at tekniske beskyttelsesforanstaltninger gennemføres, at funktionaliteten begrænses eller tilpasses, eller at det tilsigtede formål med produktet med digitale elementer defineres mere præcist. Fabrikanterne kan også træffe foranstaltninger til at påvirke den rimeligt forventelige anvendelse af produktet med digitale elementer, f.eks. gennem risikokommunikation, brugervejledning eller brugergrænsefladedesign, med henblik på at styre brugeradfærden, så sikre anvendelsesmønstre foretrækkes.

161. CRA giver ikke mulighed for at overføre cybersikkerhedsrisiko eller ansvar til brugere eller tredjeparter for at kompensere for mangler i produktdesignet eller for at retfærdiggøre, at cybersikkerhedsrisici ikke håndteres. Forpligtelsen til at bringe et sikkert produkt med digitale elementer i omsætning og til at påvise overensstemmelse med de væsentlige krav påhviler fortsat fabrikanten.

162. Oplysninger og instruktioner til brugerne kan anvendes til at understøtte sikker implementering og drift af produktet med digitale elementer, herunder hvis fabrikanten har valgt at begrænse det tilsigtede formål med det pågældende produkt til pålidelige miljøer, og til at informere brugerne om restrisici på en måde, der er passende i forhold til typen af produkt med digitale elementer og produktets tilsigtede brugere.

Eksempel 66: En fabrikant udvikler en industriel sensor til brug i pålidelige miljøer. Fabrikanten træffer ikke foranstaltninger til at beskytte mod fysiske angreb på selve sensoren for at sikre, at sensoren kan udføre funktionaliteten korrekt,. For at afbøde de tilknyttede risici, der er identificeret i risikovurderingen, begrænser fabrikanten sensorens tilsigtede formål til brug udelukkende i pålidelige miljøer, hvor uautoriseret fysisk adgang til produktet med digitale elementer forhindres. Oplysninger og instruktioner til brugerne giver klar information om disse begrænsninger for brugen af sensoren på en måde, der er passende i forhold til typen af produkt med digitale elementer og de tilsigtede brugere.

Eksempel 67: En fabrikant udvikler en softwareapplikation til erhvervsmæssig anvendelse på administrerede stationære og mobile enheder. Applikationen behandler lokalt lagrede følsomme data og brugergenereret indhold. Under risikovurderingen identificerer fabrikanten risikoen for uautoriseret adgang til sådanne data, hvis de lagres i ren tekst på enheden. I stedet for at designe og implementere en proprietær krypteringsmekanisme i selve applikationen vælger fabrikanten at benytte de krypterings- og nøgleforvaltningsfunktioner, som indbygget stilles til rådighed af det operativsystem, som applikationen er beregnet til at køre på, da operativsystemets indbyggede kryptografiske tjenester er modne og vedligeholdes regelmæssigt.

163. Hvis der i cybersikkerhedsrisikovurderingen identificeres risici, der ikke kan imødegås tilstrækkeligt gennem passende foranstaltninger, kan overholdelse af CRA kræve ændringer af design, funktionalitet eller det tilsigtede formål for produktet med digitale elementer. Overvejelser, der udelukkende vedrører omkostninger eller kommerciel gennemførlighed, udgør ikke et tilstrækkeligt grundlag for at lade sådanne risici være ubehandlede, hvis dette ville forhindre produktet med digitale elementer i at opfylde de væsentlige krav.

7.2. Om design, udvikling og produktion af produkter med digitale elementer på en sådan måde, at de sikrer et passende cybersikkerhedsniveau på grundlag af risiciene

164. Det væsentlige cybersikkerhedskrav, der er omhandlet i bilag I, del I, punkt 1, til CRA, medfører, at produkter med digitale elementer skal designes, udvikles og produceres på en sådan måde, at de sikrer et passende cybersikkerhedsniveau på grundlag af de foreliggende risici.

165. Dette væsentlige krav har til formål at imødegå alle cybersikkerhedsrisici, der er identificeret som led i cybersikkerhedsrisikovurderingen. Dette omfatter navnlig cybersikkerhedsrisici, der ikke på anden måde imødegås tilstrækkeligt som led i gennemførelsen af de væsentlige krav i bilag I, del I, bortset fra punkt 1. Dette væsentlige krav adskiller sig fra den retlige forpligtelse til at foretage en cybersikkerhedsrisikovurdering, som skal foretages i henhold til artikel 13, stk. 2.

166. Hvis alle relevante cybersikkerhedsrisici vedrørende et produkt med digitale elementer håndteres ved at gennemføre passende foranstaltninger til at opfylde de gældende væsentlige krav, bortset fra punkt 1, anses det væsentlige krav, der er omhandlet i bilag I, del I, punkt 1, for at være opfyldt. Omvendt skal fabrikanter, hvis cybersikkerhedsrisikovurderingen identificerer yderligere risici, som ikke imødegås fuldt ud af sådanne foranstaltninger, gennemføre passende foranstaltninger på produktet med digitale elementer for at imødegå disse risici, således at produktet opfylder det væsentlige krav, der er omhandlet i bilag I, del I, punkt 1. I praksis forventes overholdelse af de øvrige væsentlige krav i de fleste tilfælde at føre til overholdelse af dette krav.

7.3. Risikovurdering og due diligence i forbindelse med eksterne afhængigheder og integrerede komponenter

167. Ved CRA fastsættes to særskilte og gensidigt supplerende forpligtelser for fabrikanter i forbindelse med styring af cybersikkerhedsrisici. For det første pålægges fabrikanterne i kraft af artikel 13, stk. 2, at foretage en cybersikkerhedsrisikovurdering af selve produktet med digitale elementer. For det andet pålægges de i kraft af artikel 13, stk. 5, en forpligtelse til at udvise due diligence med hensyn til integrerede komponenter. Tilsammen har disse to forpligtelser til formål at sikre, at et produkt med digitale elementer forbliver sikkert, herunder når det baserer sig på fjerndatabehandlingsløsninger, fjerntjenester eller software- eller hardwarekomponenter fra tredjepart.

168. Cybersikkerhedsrisikovurderingen vedrører identifikation og håndtering af relevante risici, der kan påvirke produktet med digitale elementer, herunder risici, der hidrører fra forhold uden for selve produktet, såsom eksterne netværk, miljøfaktorer eller andre eksterne aspekter, der kan påvirke produktet med digitale elementer, eller som produktet baserer sig på. For sådanne eksterne risici indeholder CRA ikke krav om, at fabrikanterne kontrollerer eller styrer det eksterne miljø. Fabrikanterne skal derimod identificere sådanne risici og afbøde dem gennem design og udvikling af selve produktet med digitale elementer. Dermed skal de relevante væsentlige krav i bilag I, del I, gennemføres, og brugerne skal, hvor det er nødvendigt, gives oplysninger og instruktioner om integrations- eller implementeringsrisici.

169. En fabrikant kan f.eks. identificere en risiko for, at uautoriserede personer kan få adgang til backendsystemer, der ikke er en del af selve produktet med digitale elementer, mens produktet er i drift, og forsøge at sende skadelige kommandoer til produktet med digitale elementer. Sådanne backendsystemer udgør, hvis de ikke er designet og udviklet af fabrikanten eller under dennes ansvar, eller hvis de ikke understøtter en af funktionerne i produktet med digitale elementer, ikke fjerndatabehandlingsløsninger og falder derfor uden for anvendelsesområdet for produktet med digitale elementer for så vidt angår CRA. Ikke desto mindre indeholder CRA krav om, at fabrikanten imødegår den risiko, sådanne systemer kan udgøre, gennem foranstaltninger på produktniveau, f.eks. ved at kræve kryptografisk autentificering af fjernkommandoer, verificere integriteten af konfigurationsændringer eller generere sikkerhedsrelevante logfiler eller advarsler, når unormal adfærd opdages. Tilsvarende kan der i henhold til CRA, hvis en fabrikant identificerer en risiko som følge af, at en sådan ekstern tjeneste bliver utilgængelig, f.eks. på grund af strømafbrydelser eller infrastruktursvigt, stilles krav om risikobegrænsende foranstaltninger på produktniveau mod sådanne cybersikkerhedsrisici, f.eks. ved at sikre, at afbrydelsen ikke får produktet med digitale elementer til at gå i usikker tilstand. I sådanne tilfælde regulerer CRA, hvordan produktet med digitale elementer skal reagere ved sådanne eksterne risici. CRA pålægger ikke forpligtelser med hensyn til, hvordan backendinfrastrukturen organiseres, bemandes eller drives, og behandler heller ikke denne infrastruktur som en del af produktet med digitale elementer.

170. Due diligence vedrører elementer, der udgør en del af selve produktet med digitale elementer, navnlig integrerede software- eller hardwarekomponenter, der leveres af en tredjepart. Fabrikanterne skal træffe passende foranstaltninger til at sikre, at sådanne komponenter ikke underminerer produktet med digitale elementers overensstemmelse med de væsentlige krav. Dette kan kun opnås ved at fastslå, hvad et produkt med digitale elementer indebærer af krav til komponenterne for at opfylde cybersikkerhedsmålene, og ved på en risikobaseret måde at verificere, at disse komponenter er i overensstemmelse med produktets behov, jf. også betragtning 34.

171. I overensstemmelse med cybersikkerhedsrisikovurderingen skal fabrikanten identificere de krav, som den integrerede komponent bør opfylde. Hvis produktet med digitale elementer f.eks. baserer sig på kryptografiske funktioner, opdateringsmekanismer eller sikker kommunikation, der leveres af en komponent, skal fabrikanten som led i due diligence-proceduren identificere disse behov og verificere, at komponenten opfylder dem. Dokumentation til dette formål kan bestå af dokumentation indhentet fra komponentfabrikanten, såsom tekniske specifikationer, sikkerhedsdokumentation eller anden relevant dokumentation for overensstemmelse eller sikkerhed. Hvor det er relevant, kan fabrikanten også foretage test for at verificere, at disse komponenter i tilstrækkelig grad udfører de relevante funktioner. Selv om due diligence er en særskilt retlig forpligtelse, støtter og underbygger det fabrikantens mulighed for at påvise overensstemmelse med de væsentlige krav for produktet med digitale elementer som helhed.

172. Ved vurderingen af risici for produktet med digitale elementer som helhed skal elementer uden for produktet, såsom miljøelementer, ekstern infrastruktur, andre systemer eller netværk, indgå i cybersikkerhedsrisikovurderingen og, hvor det er relevant, imødegås gennem foranstaltninger på produktniveau for at sikre, at produktet med digitale elementer er i overensstemmelse med de væsentlige krav. Komponenter, der er fysisk eller logisk integreret i produktet med digitale elementer, men hidrører fra en tredjepart, skal også tages i betragtning som led i risikovurderingen. Med henblik på overholdelse bør fabrikanten imidlertid behandle disse som eksternt leverede komponenter, hvis egenskaber verificeres gennem due diligence ved integrationen, da fabrikanten måske ikke har redesignet eller genudviklet dem.

173. Den samme logik gælder ved udvikling og integration af komponenter. Hvis fabrikanten selv udvikler funktionaliteter, skal fabrikanten gennemføre de væsentlige krav direkte. Hvis fabrikanten integrerer komponenter, der er udviklet af andre, skal fabrikanten gennem due diligence sikre, at disse komponenter kan anvendes på en måde, der muliggør, at produktet med digitale elementer som helhed overholder kravene. I begge tilfælde er målet det samme: at produktet med digitale elementer, således som det bringes i omsætning, opnår et passende cybersikkerhedsniveau som krævet i henhold til CRA, under hensyntagen til de risici, der er identificeret i cybersikkerhedsrisikovurderingen.

7.4. **Genbrug af risikovurderinger og overensstemmelsesdokumentation for familier af produkter med digitale elementer**

174. Fabrikanter kan bringe lignende produkter med digitale elementer i omsætning, f.eks. forskellige varianter, modeller eller konfigurationer af samme produktfamilie. Hvis sådanne produkter med digitale elementer har samme arkitektur, sikkerhedsrelevante design og tilsigtede formål og er udsat for de samme cybersikkerhedsrisici, kræver CRA ikke, at fabrikanter behandler hver variant som et helt særskilt produkt med digitale elementer med henblik på risikovurdering og overensstemmelsesvurdering.

175. I sådanne tilfælde kan fabrikanterne, forudsat at alle de berørte varianter er tilstrækkeligt dækket med hensyn til relevante risici og væsentlige krav, basere sig på: i) en enkelt cybersikkerhedsrisikovurdering foretaget i overensstemmelse med artikel 13, stk. 2, i CRA, ii) et enkelt sæt teknisk dokumentation og iii) en enkelt overensstemmelsesvurderingsprocedure. Dette gør det også muligt at udstede én enkelt EU-overensstemmelseserklæring for gruppen af produkter med digitale elementer, så længe den klart identificerer de produktvarianter, den finder anvendelse på.

176. Den afgørende faktor er, om forskellene mellem varianterne er relevante for cybersikkerheden. Variationer, der ikke påvirker cybersikkerhedsegenskaberne for produktet med digitale elementer, såsom forskellig farve, form, hukommelsesstørrelse eller andre ikke-sikkerhedsrelevante karakteristika, kræver ikke særskilte risikovurderinger eller overensstemmelsesvurderinger. Omvendt kan varianter i nogle tilfælde adskille sig på måder, der påvirker gennemførelsen af væsentlige krav, f.eks. gennem forskellige kommunikationsgrænseflader, softwarestakke, opdateringsmekanismer eller fjernkonnektivitet. I sådanne tilfælde skal disse forskelle afspejles i risikovurderingen og, hvor det er nødvendigt, i overensstemmelsesvurderingen og den tekniske dokumentation.

177. Fabrikanterne er fortsat ansvarlige for at sikre, at risikovurderingen og den tilhørende dokumentation nøjagtigt afspejler de produkter med digitale elementer, der bringes i omsætning. Hvis en ny variant indebærer nye cybersikkerhedsrisici eller betyder ændring af den måde, hvorpå væsentlige krav gennemføres, skal den eksisterende risikovurdering og overensstemmelsesdokumentation ajourføres i overensstemmelse hermed. Det er kun muligt at basere sig på en enkelt overensstemmelsesvurdering i det omfang, at produkterne med digitale elementer ikke frembyder forskelle med hensyn til deres cybersikkerhedsegenskaber.

8. **FJERNDATABEHANDLING**

178. I artikel 3, nr. 1), i CRA defineres et produkt med digitale elementer som »et software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der bringes i omsætning separat«. I lyset heraf skal fabrikanten betragte produktet med digitale elementer som en helhed, herunder dets fjerndatabehandlingsløsninger (RDPS). For eksempel skal der ved påvisning af, at produktet med digitale elementer opfylder de væsentlige krav i bilag I, tages hensyn til RDPS, begyndende med risikovurderingen (artikel 13, stk. 2). Det samme gælder, når livscyklusforpligtelser tages i betragtning, såsom rapportering af aktivt udnyttede sårbarheder og alvorlige hændelser (artikel 14).

179. Formålet med denne vejledning er at yde fabrikanter yderligere støtte til at afgøre, om deres produkt med digitale elementer omfatter RDPS som defineret i CRA, og hvordan de opfylder deres overholdelsesforpligtelser i den henseende. Efter en indledende analyse af definitionerne og betragtningerne i CRA indeholder denne vejledning spørgsmål, der kan vejlede fabrikanterne i at afklare, om deres produkt med digitale elementer omfatter RDPS (se afsnit *8.1 Hvad anses for at være en fjerndatabehandlingsløsning for et produkt med digitale elementer?*). Derefter uddybes de tekniske konsekvenser af RDPS, og hvordan overholdelsen af CRA skal vurderes (se afsnit *8.2 Praktiske og tekniske konsekvenser af fjerndatabehandlingsløsninger og afhængighed af tredjepartsløsninger*).

180. Faktisk defineres begrebet »fjerndatabehandling« i artikel 3, nr. 2), som »databehandling, der foretages eksternt, til hvilken softwaren er designet og udviklet af fabrikanten eller under fabrikantens ansvar, og hvis fravær ville forhindre produktet med digitale elementer i at udføre en af sine funktioner«. RDPS defineres derfor som softwareelementerne (»den del af et elektronisk informationssystem, der består af computerkode«, jf. artikel 3, nr. 4)) i databehandling eksternt. Det er ikke hensigten, at den hardware, som fjerndatabehandling kan bygge på, skal være omfattet af anvendelsesområdet for produktet med digitale elementer.

181. I betragtning 11 og 12 gives der yderligere forklaringer på, hvordan dette begreb bør fortolkes. I betragtning 11 præciseres det, at formålet med at omfatte fjerndatabehandlingsløsninger er, at »produkter er tilstrækkeligt sikret i deres helhed af deres fabrikanter, uanset om data behandles eller lagres lokalt på brugerens enhed eller eksternt af fabrikanten«. Det fastslås også, at »kravene vedrørende fjerndatabehandlingsløsninger, der er omfattet af denne forordnings anvendelsesområde, omfatter derfor ikke tekniske, operationelle eller organisatoriske foranstaltninger, der har til formål at styre de risici, der er forbundet med sikkerheden i en fabrikants net- og informationssystemer som helhed«.

182. Det følger derfor af betragtning 11, at hensigten ikke er, at kravene i CRA skal omfatte en organisations samlede IT-infrastruktur, men kun softwarekomponenter, der muliggør udførelsen af databehandlingsløsningen. For eksempel bør interne systemer vedrørende fabrikantens personaleadministration, lønbehandling, kunderelationsstyring, pipelines til kontinuerlig integration/kontinuerlig levering (CI/CD) og distribution af sikkerhedsopdateringer til edge-lokationer ikke anses for at være RDPS. Ligeledes falder systemer, der er knyttet til revisions- og testaktiviteter, såsom penetrationstest, threat hunting og red teaming, uden for anvendelsesområdet for et produkt med digitale elementer for så vidt angår CRA. Det er vigtigt at bemærke, at selv om anvendelse af effektive og regelmæssige test og gennemgange af sikkerheden i produktet med digitale elementer er et væsentligt krav, der er fastsat i bilag I, del II, punkt 3, til CRA, betyder det ikke, at sådanne aktiviteter skal anses for at være RDPS for produktet med digitale elementer.

183. Betragtning 12 omhandler cloudtjenester og det uddybes, under hvilke omstændigheder cloudtjenester kan anses for at være RDPS. Betragtningen fastslår til sidst, at cloudcomputingtjenester og cloudtjenestemodeller er omfattet af anvendelsesområdet for direktiv (EU) 2022/2555 (NIS 2) ([28]), som fastsætter krav til styring af cybersikkerhedsrisici for udbydere af cloudcomputingtjenester. Disse krav præciseres yderligere i Kommissionens gennemførelsesforordning (EU) 2024/2690 ([29]).

8.1. **Hvad anses for at være en fjerndatabehandlingsløsning for et produkt med digitale elementer?**

184. Definitionen af fjerndatabehandling i artikel 3, nr. 2), bygger således på tre elementer: i) om databehandlingen sker »eksternt« ii) om fraværet af en sådan databehandling ville forhindre produktet med digitale elementer i at udføre en af funktionerne og iii) om softwaren er designet og udviklet af fabrikanten eller under dennes ansvar. I de næste tre underafsnit behandles disse elementer nærmere.

([28]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Kommissionens gennemførelsesforordning (EU) 2024/2690 af 17. oktober 2024 om regler for anvendelsen af direktiv (EU) 2022/2555 for så vidt angår tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici og yderligere præcisering af de tilfælde, hvor en hændelse anses for at være væsentlig, for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester (EUT L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Begrebet »eksternt«*

185. Begrebet »eksternt« i artikel 3, nr. 2), er relevant, men ikke tilstrækkeligt til at afgøre, om et produkt med digitale elementer omfatter RDPS. Desuden er det, i betragtning af den række forskellige løsninger, der kan være omfattet af dette begreb, ikke muligt at give en udtømmende definition af »eksternt«. Der er behov for en vurdering fra sag til sag foretaget af fabrikanten.

186. I betragtning 11 til CRA omtales data, der behandles eller lagres »eksternt af fabrikanten«, i modsætning til data, der behandles eller lagres »lokalt på brugerens enhed«. Fjerndatabehandling finder typisk sted uden for brugermiljøet for et produkt med digitale elementer eller en organisations driftsmiljø (for en professionel bruger). Dette forhindrer dog ikke, at behandlingen også kan finde sted tæt på enheden (»at the edge«). Overførslen af data kan ske kablet (f.eks. via ethernet-kabel) eller trådløst (f.eks. via Wi-Fi eller Bluetooth). Cloudcomputing, herunder edgecomputing, er et typisk eksempel på databehandling, der finder sted »eksternt«. For eksempel finder en del af databehandlingen i tilfælde af en cloudbaseret funktion, som brugeren tilgår fra en mobilapplikation, sted i cloudmiljøet uden for brugermiljøet.

187. Det er vigtigt at bemærke, at RDPS ikke nødvendigvis afvikles på tredjepartscloudinfrastruktur. Fjerndatabehandling, der afvikles på lokale servere på fabrikantens lokaliteter, kan også udgøre RDPS. Med andre ord kan en løsning som kører on-premise og privat cloud ligeså vel kvalificeres som en RDPS som en løsning, der kører på en offentlig cloud eller off-premise.

188. De to afgørende og kumulative spørgsmål, der afgør, om databehandling er omfattet af CRA som en fjerndatabehandlingsløsning, er angivet nedenfor i afsnit *8.1.2* og *8.2*. Hvis begge spørgsmål besvares bekræftende, anses fjerndatabehandlingen som RDPS.

8.1.2. *Ville fraværet af en sådan databehandling forhindre produktet med digitale elementer i at udføre en af funktionerne?*

189. Som fastsat i definitionen af »fjerndatabehandling« i artikel 3, nr. 2), er det en betingelse for, at databehandling på afstand kan betragtes som RDPS, at fraværet heraf ville forhindre produktet med digitale elementer i at udføre en af sine funktioner. Begrebet »funktioner« i denne definition er ikke begrænset til »kernefunktionaliteten« eller det »tilsigtede formål« for produktet med digitale elementer, da CRA ikke pålægger en sådan begrænsning. De funktioner, der er omfattet af CRA, er både funktioner, der direkte opfylder produktet med digitale elementers tilsigtede formål, sådan som brugerne oplever det, og funktioner, der understøtter produktets samlede ydeevne.

190. Eksempler på funktioner, hvor databehandling eksternt kan finde sted, og hvor fraværet heraf ville forhindre et produkt med digitale elementer i at udføre en af funktionerne, omfatter: i) at sende kommandoer til en enhed, ii) at synkronisere filer, iii) at onboarde brugeren, iv) konfiguration (personalisering af produktet med digitale elementer), v) automatiseret distribution af opdateringer, herunder funktionsopdatering og sikkerhedrettelse, vi) identitets- og adgangsstyring.

191. I nogle tilfælde kan brugeren anvende en funktion både eksternt og manuelt (f.eks. tænde eller slukke en lyspære med en app eller manuelt). Denne mulighed udelukker ikke, at den databehandling, der er forbundet med fjernudførelsen af funktionen, kvalificerer som RDPS. Fjernudførelse af denne funktion anses også for at være en del af de funktioner, som produktet med digitale elementer tilbyder.

192. I modsætning hertil anses en sådan behandling ikke som RDPS som omhandlet i CRA, hvis fraværet af en bestemt databehandling ikke forhindrer produktet med digitale elementer i at udføre en af funktionerne. Dette omfatter f.eks. fjernanalyse af telemetridata, der udelukkende er indsamlet til statistiske formål eller med henblik på fremtidig produktudvikling.

193. Ikke desto mindre kan fabrikanter, selv når databehandling ikke understøtter en funktion i et produkt med digitale elementer, være nødt til i deres cybersikkerhedsrisikovurdering at overveje, om disse fjernkomponenter medfører risici for produktet med digitale elementer (f.eks. på grund af produktets driftsmiljø), og afbøde sådanne risici i overensstemmelse hermed (f.eks. gennem afbødende foranstaltninger på produktniveau).

194. Websteder er et særligt tilfælde, der fortjener yderligere præcisering, se *afsnit 2.1 Markedsføring*. Websteder falder ikke ind under RDPS, hvis de ikke understøtter en funktion i et produkt med digitale elementer, som forklaret i betragtning 11 til CRA. At et websted indeholder oplysninger om et produkt med digitale elementer er ikke tilstrækkeligt for, at det kan anses som RDPS, heller ikke selv om produktet omdirigerer til et sådant websted. For eksempel udgør omdirigering af brugere til en ekstern webside, der giver brugerne oplysninger og instruktioner, ikke RDPS. I modsætning hertil kan et websted være omfattet af RDPS, hvis det muliggør eller understøtter en funktion i et produkt med digitale elementer. For eksempel vil en autentificeringsportal, der udsteder legitimationsoplysninger eller tokens, som er nødvendige for, at produktet med digitale elementer kan fungere, blive anset for RDPS (forudsat at de øvrige kriterier i definitionen også er opfyldt).

8.1.3. *Er softwaren designet og udviklet af fabrikanten eller under dennes ansvar?*

195. Definitionen af »fjerndatabehandling« i artikel 3, nr. 2), i CRA præciserer endvidere, at softwaren til en sådan databehandling eksternt skal være designet og udviklet af fabrikanten eller under dennes ansvar. Fjerndatabehandling, der udelukkende er udviklet og designet af fabrikanten (internt), betragtes naturligvis som RDPS. Det vil også være tilfældet, hvis fabrikanter benytter en ekstern tjenesteudbyder til udvikling og design af en løsning (dvs. »under deres ansvar«). Udtrykket »under fabrikantens ansvar« henviser til fjerndatabehandlingsløsninger, der er skræddersyet til fabrikanten. Det er tilfælde, hvor fabrikanten ikke blot licenserer et eksisterende produkt med digitale elementer eller en eksisterende tjeneste, som en tjenesteudbyder tilbyder sine kunder, eller let ændrede versioner heraf. »[U]nder fabrikantens ansvar« indebærer, at softwaren udelukkende udvikles af eller på vegne af fabrikanten på grundlag af design og specifikationer, som fabrikanten har leveret.

196. For forståelsen af RDPS er begrebet »hvem der driver løsningen« ikke en afgørende faktor, da definitionen i CRA kun henviser til design og udvikling af RDPS. Dette er i overensstemmelse med CRA, hvor krav og forpligtelser påhviler fabrikanterne og ikke driften af produktet med digitale elementer. Hvis fabrikanter designer og udvikler løsninger, som derefter drives af en tredjepart, er de fortsat ansvarlige for overholdelsen af de væsentlige krav i CRA for det produkt med digitale elementer, som de bringer i omsætning.

197. Det er nødvendigt at skelne mellem de tilfælde, hvor design og udvikling udføres af fabrikanterne (eller under deres ansvar), og tilfælde, hvor der anvendes tredjepartsløsninger, som ikke er designet og udviklet af fabrikanterne (eller under deres ansvar). Som eksempel er det nyttigt at se på de mest almindelige cloudtjenestemodeller, som giver forskellige grader af brugerkontrol, og som også nævnes i betragtning 12 til CRA, nemlig Software as a Service (SaaS), Platform as a Service (PaaS) og Infrastructure as a Service (IaaS).

198. I tilfælde af en IaaS-løsning fra en tredjepart forvalter eller kontrollerer fabrikanten ikke de underliggende fysiske og virtuelle ressourcer (såsom den underliggende hardware og cloudtjenesteudbyderens hypervisor), men kan implementere og køre vilkårlig software ved hjælp af sådanne ressourcer, såsom operativsystemer og applikationer. Sådan software er designet og udviklet af fabrikanten eller under dennes ansvar og kan derfor betragtes som RDPS (hvis den opfylder de øvrige elementer i definitionen).

199. I tilfælde af en PaaS-løsning fra en tredjepart implementerer fabrikanten sin egen (udviklede eller erhvervede) applikation ved hjælp af programmeringssprog og eksekveringsmiljøer, der leveres af cloudtjenesteudbyderen, og integrerer applikationen i sit produkt med digitale elementer. Fabrikanten har kontrol over applikationen og eventuelt over konfigurationsindstillingerne for eksekveringsmiljøet. Applikationen er derfor designet og udviklet af fabrikanten eller under dennes ansvar og kan derfor betragtes som RDPS (hvis den opfylder de øvrige elementer i definitionen).

200. I tilfælde af en SaaS-løsning fra en tredjepart tilbyder SaaS-udbyderen fabrikanten en fuldt udviklet applikation, der skal integreres i fabrikantens produkt med digitale elementer. Fabrikanten har begrænset mulighed for at administrere brugerspecifikke konfigurationsindstillinger for applikationen. Applikationen er derfor ikke designet og udviklet af fabrikanten eller under dennes ansvar.

201. Ikke desto mindre bør visse elementer, der ikke betragtes som RDPS (f.eks. hypervisoren i tilfælde af en IaaS-infrastruktur fra en tredjepart, operativsystemet i tilfælde af en PaaS-løsning fra en tredjepart eller SaaS-applikationen fra en tredjepart), men som er integreret i produktet med digitale elementer på en måde, der påvirker dets sikkerhed, anses for at svare til tredjepartskomponenter. Fabrikanten skal identificere og vurdere risici i forbindelse med integrationen af disse elementer og håndtere dem ved at gennemføre de væsentlige krav i selve produktet med digitale elementer. Dette kan, hvor det er relevant, understøttes af de sikkerhedsfunktioner, som cloudtjenesteudbyderen stiller til rådighed gennem dennes model for delt ansvar, når fabrikanten bruger eller konfigurerer disse funktioner til at håndtere de identificerede risici. Desuden forventes fabrikanten at udøve en forpligtelse svarende til forpligtelsen til at udvise due diligence, jf. artikel 13, stk. 5, vedrørende sikkerheden i disse komponenter på en måde, der står i et rimeligt forhold til den risiko, som fjernløsningen udgør for produktet med digitale elementers sikkerhed.

202. Det kan derfor sammenfattes således:

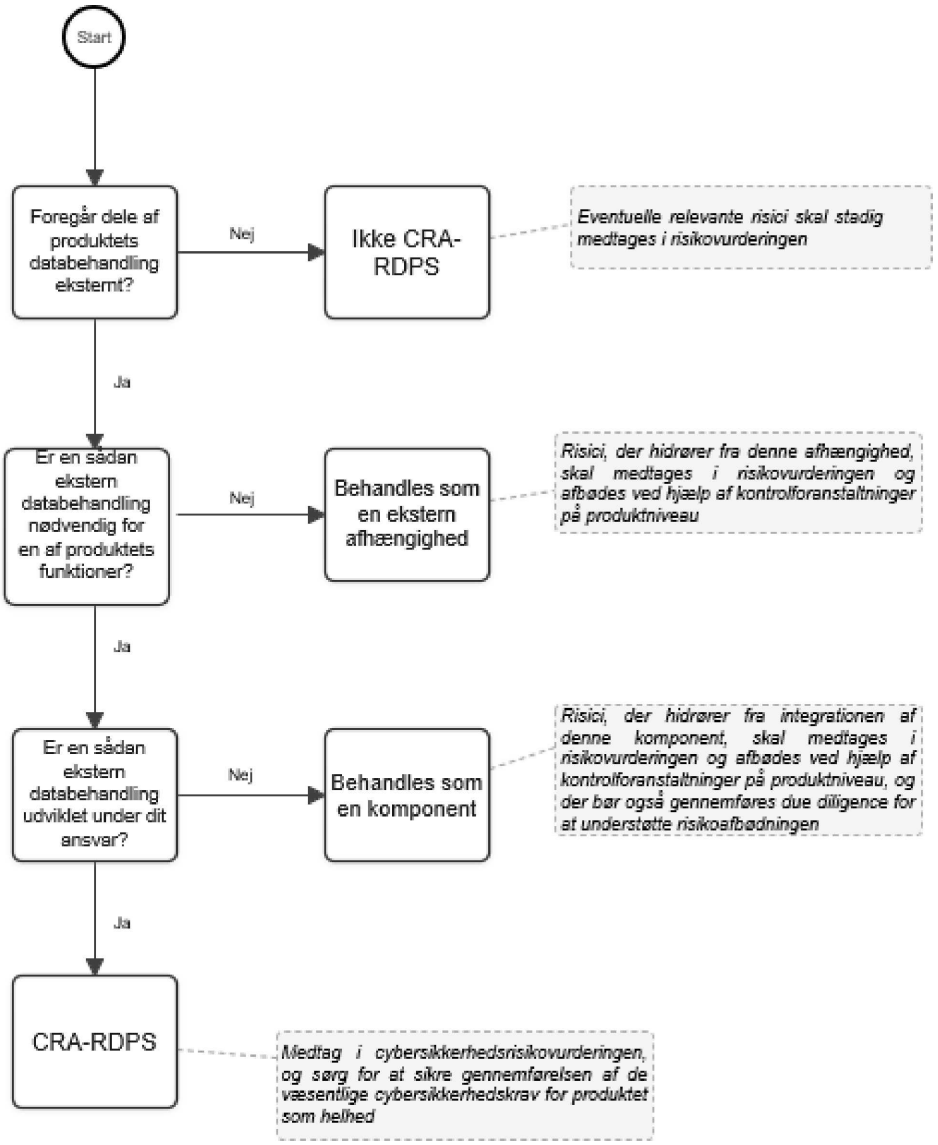
a) For at databehandling kan betragtes som RDPS, skal svaret på begge spørgsmål i afsnit *8.1.2 Ville fraværet af en sådan databehandling forhindre produktet med digitale elementer i at udføre en af funktionerne?* og *8.1.3 Er softwaren designet og udviklet af fabrikanten eller under dennes ansvar?* være bekræftende.

b) Hvis svaret på spørgsmålet i afsnit *8.1.2 Ville fraværet af en sådan databehandling forhindre produktet med digitale elementer i at udføre en af funktionerne?* er negativt, bør fabrikanterne som led i deres risikovurdering vurdere de risici, der følger af, at en sådan databehandling finder sted.

c) Hvis svaret på spørgsmålet i afsnit *8.1.2 Ville fraværet af en sådan databehandling forhindre produktet med digitale elementer i at udføre en af funktionerne?* er bekræftende, men svaret på spørgsmålet i *8.1.3 Er softwaren designet og udviklet af fabrikanten eller under dennes ansvar?* er negativt, bør fabrikanterne behandle tredjepartsløsningen som en komponent. Som led i risikovurderingen bør fabrikanterne vurdere de risici, der følger af at integrere en sådan løsning, og afbøde dem i overensstemmelse hermed. Desuden bør fabrikanterne udvise due diligence.

Figur 9:

Stiliseret flowdiagram, der viser, om et produkt med digitale elementer indeholder RDPS



8.2. Praktiske og tekniske konsekvenser af fjerndatabehandlingsløsninger og afhængighed af tredjepartsløsninger

203. CRA følger en risikobaseret tilgang, som er fastsat i artikel 13, stk. 2 og 3, samt i det første væsentlige krav i del I i bilag I, ifølge hvilket »produkter med digitale elementer skal designes, udvikles og produceres på en sådan måde, at de sikrer et passende cybersikkerhedsniveau baseret på risiciene«. Der bør derfor anlægges en risikobaseret tilgang ved anvendelse af kravene i CRA på RDPS og ved behandling af risici, der hidrører fra tredjepartstjenester, som er integreret i produktet med digitale elementer.

204. For det første bør fabrikanterne i) angive i den tekniske dokumentation, at deres produkt med digitale elementer omfatter RDPS eller er afhængigt af fjernløsninger fra tredjeparter, og ii) beskrive sådanne løsninger. Hvis den samme RDPS understøtter flere produkter med digitale elementer, skal den pågældende RDPS angives i den tekniske dokumentation for hvert produkt. Dokumentationen vedrørende RDPS, der benyttes til flere produkter med digitale elementer, kan genanvendes fra én produktoverensstemmelsesvurdering til en anden.

205. Som angivet i betragtning 11 bør de RDPS, der indgår i produktet med digitale elementer og derfor er omfattet af produktets overensstemmelsesvurdering, begrænses til de softwaremoduler, der sikrer funktionaliteten i produktet med digitale elementer, og til de grænseflader, som disse moduler anvender i forbindelse med eksterne tjenester. Yderligere backendsystemer, som udfører efterfølgende behandling, og som produktet med digitale elementer ikke interagerer direkte med, anses ikke for at være RDPS.

206. Disse backendsystemer betragtes dog fortsat som eksterne afhængigheder, der skal vurderes som led i cybersikkerhedsrisikovurderingen og afbødes ved hjælp af foranstaltninger på produktniveau. Risikovurderingen, som fabrikanten foretager, bør således omfatte: i) risici vedrørende RDPS, ii) risici vedrørende afhængighed af tredjepartsfjernløsninger (svarende til tredjepartskomponenter) og iii) risici vedrørende produktmiljøet (f.eks. underliggende hardware). Fabrikanterne bør gennemføre sikkerhedskontroller på selve produktet med digitale elementer for at afbøde disse risici.

207. Som led i overensstemmelsesvurderingen og/eller opfyldelse af due diligence-forpligtelser vedrørende fjerntjenester fra tredjeparter kan følgende ikke-udtømmende liste over assuranceartefakter desuden genanvendes til støtte for fabrikantens vurdering:

a) dokumentation for opfyldelse af forpligtelser i henhold til Kommissionens gennemførelsesforordning (EU) 2024/2690

b) dokumentation for opfyldelse af forpligtelser i henhold til forordning (EU) 2022/2554 (DORA)

c) overensstemmelseserklæring eller attest opnået i henhold til en europæisk cybersikkerhedscertificeringsordning (vedtaget i henhold til forordning (EU) 2019/881 forordningen om cybersikkerhed), og

d) dokumentation for overensstemmelse med ISO/IEC 27017:2015 eller ISO/IEC 27001:2022.

208. Endelig skal fabrikanterne i deres interaktioner med tredjepartsudbydere af fjerntjenester gennemføre de mest passende sikkerhedsforanstaltninger på grundlag af deres risikovurdering (og, hvor det er relevant, understøttet af udbyderens model for delt ansvar). Disse risikobegrænsende foranstaltninger bør omfatte sikkerhedskontroller for de pågældende produkter med digitale elementer og verifikation af sikkerhedsforanstaltninger, som tredjepartsudbyderne selv stiller til rådighed (due diligence). Et redskab til at afbøde sådanne risici kan være at indarbejde sikkerhedsgarantier i serviceniveauaftaler (SLA) med tredjepartsudbydere, herunder garantier for, at udbyderne håndterer sårbarheder på passende vis. En større ændring i de løsninger, der leveres af tredjepartsudbydere af fjerntjenester, bør ikke betragtes som en væsentlig ændring af produktet med digitale elementer, da disse elementer ikke hører under fabrikantens ansvar. Som led i deres due diligence-forpligtelser og for på korrekt vis at afbøde risici, der stammer fra brugen af tredjepartsudbydere, opfordres fabrikanterne imidlertid til at sikre, at deres tredjepartsudbydere af cloudcomputingtjenester holder dem tilstrækkeligt informeret om ændringer, som de gennemfører i deres løsninger. På grundlag af sådanne oplysninger kan fabrikanterne være nødt til at revidere deres risikovurdering. I den ajourførte risikovurdering bør der tages hensyn til, om tredjepartstjenesteudbyderne fortsat giver tilstrækkelige garantier med hensyn til cybersikkerhed, og om sikkerhedskontrollerne på produktniveau fortsat er tilstrækkelige. I nogle tilfælde kan fabrikanterne være nødt til at ændre sådanne kontroller eller skifte tredjepartstjenesteudbydere.

8.3. **Anvendelsestilfælde for fjerndatabehandlingsløsninger**

Som en yderligere praktisk vejledning til fabrikanterne indeholder dette afsnit en række fiktive anvendelsestilfælde, som beskriver typiske produkter med digitale elementer, der er afhængige af fjerndatabehandling, og eksemplerne illustrerer, om en sådan behandling betragtes som fjerndatabehandlingsløsninger som omhandlet i CRA.

8.3.1. *Mobilbankapplikation*

En finansiel enhed bringer en mobilbankapplikation i omsætning. Appens backendsystemer understøtter bl.a. autentificering, autorisation, kontostyring og betalinger. Den finansielle enhed anvender en hybrid strategi, der bygger på intern infrastruktur samt fjernløsninger fra tredjeparter til at understøtte appens funktionaliteter. Disse omfatter bl.a.:

Selvhostet infrastruktur udviklet af den finansielle enhed:

— Kunden åbner mobilbankapplikationen og autentificeres via bankgrænsefladen, der er en selvhostet løsning udviklet af den finansielle enhed, og som modtager anmodninger fra appen og returnerer de tilsvarende svar. Bankgrænsefladen verificerer kundens identitet ved forespørgsel til kontostyringssystemet og giver adgang til applikationen.

— Kunden initierer en overførsel via appen. Appen sender instruksen til bankgrænsefladen, som indgiver en tilsvarende anmodning til ledgersystemet.

— Kontostyringssystemet og ledgersystemet, som begge er selvhostede, men logisk adskilt fra bankgrænsefladen, registrerer transaktionen.

— Ledgersystemet returnerer transaktionens status til bankgrænsefladen, som præsenterer resultatet for kunden.

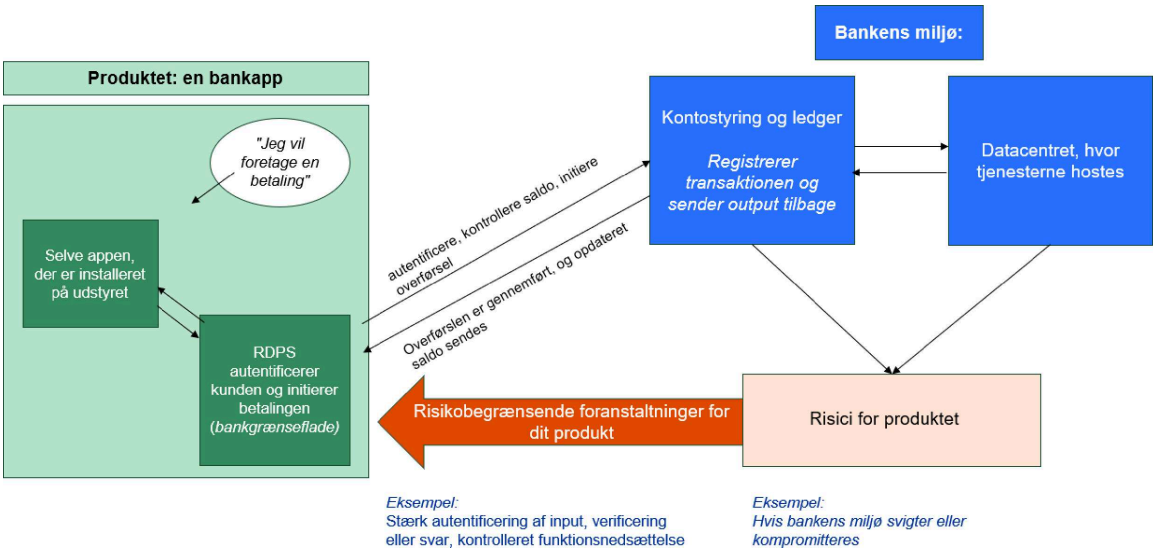
Betydning vedrørende RDPS:

— Bankgrænsefladen er nødvendig for, at appen kan udføre funktionerne, nemlig at autentificere kunden, indsende kundens instrukser, herunder betalings- og overførselsinstrukser, og returnere den deraf følgende status. Bankgrænsefladen er designet og udviklet under fabrikantens ansvar. Da svaret på begge spørgsmål, der er præsenteret i tidligere afsnit, er bekræftende, skal bankgrænsefladen anses som RDPS. Den skal derfor indgå i cybersikkerhedsrisikovurderingen og i gennemførelsen af de væsentlige krav for produktet med digitale elementer som helhed. Den efterfølgende behandling af en instruks, når den er indgivet, navnlig registreringen af transaktionen i kontostyrings- og ledgersystemerne samt afvikling og clearing, foretages af systemer, som appen ikke interagerer direkte med, og udgør på dette grundlag ikke en RDPS.

— Kontostyringssystemet og ledgersystemet betragtes ikke som RDPS for bankapplikationen. Appen interagerer ikke direkte med dem (men interagerer i stedet med bankgrænsefladen, som til gengæld er afhængig af dem). Selv om deres tilgængelighed kan være nødvendig for, at en funktion kan fuldføres, omfatter CRA kun de dele af systemet, som interagerer direkte med produktet med digitale elementer. De falder derfor uden for definitionen af RDPS for så vidt angår CRA. Disse systemer forbliver dog eksterne afhængigheder, som kan give anledning til betydelige cybersikkerhedsrisici for produktet med digitale elementer. F.eks. kan kompromittering af ledgersystemet gøre det muligt for en angriber at påvirke transaktionsresultater, der efterfølgende vises i applikationen. Fabrikanten skal derfor identificere og vurdere disse risici som led i cybersikkerhedsrisikovurderingen og afbøde dem ved hjælp af foranstaltninger på produktniveau, såsom stærk autentificering af backendgrænseflader, integritetsbeskyttelse af transaktionsdata, sikre kommunikationskanaler og verifikation af svar modtaget af appen.

Figur 10:

Stiliseret fremstilling af en bankapp, der bygger på RDPS



Tredjeparts-SaaS til kundesupport:

— Den finansielle enhed integrerer i sin app en chatløsning til kundesupport, der er udviklet og drives af en tredjepartsudbyder. Tredjepartsudbyderen har skrevet chatserverkoden, opbygget brugergrænsefladen og driver den infrastruktur, hvor chatten er implementeret (dvs. SaaS-model).

— Når kunden igangsætter en supportforespørgsel, forbinder appen kunden med tredjepartstjenesten for at etablere en chatsession og håndtere meddelelsesflow uden at give tredjeparten adgang til centrale banksystemer.

Betydning vedrørende RDPS:

— Chatsupportløsningen er nødvendig for, at produktet med digitale elementer kan udføre en af funktionerne, men den er ikke designet og udviklet af den finansielle enhed eller under dennes ansvar, og derfor er den ikke RDPS. Den bør dog behandles som en tredjepartskomponent. Afhængigheden af denne tredjepartstjeneste kan skabe cybersikkerhedsrisici for bankapplikationen, f.eks. hvis en angriber bruger chatkanalen til at udgive sig for at være banken eller til at levere skadeligt indhold til brugerne. Den finansielle enhed skal tage disse risici i betragtning i cybersikkerhedsrisikovurderingen og afbøde dem ved hjælp af foranstaltninger på produktniveau, såsom at isolere chatfunktionen fra centrale bankfunktioner, kontrollere datastrømme og validere indhold. Der bør også udvises due diligence i forbindelse med den pågældende SaaS.

8.3.2. *Intelligent termostat*

En intelligent termostat gør det muligt for brugerne at styre temperaturen i deres hjem via en mobilapplikation. Mobilapplikationen og den intelligente termostat benytter fjerndatabehandling for at udveksle data (f.eks. en anmodning om at hæve temperaturen) og lagre data (f.eks. brugerpræferencer). Disse funktioner er udviklet og designet under fabrikantens ansvar, men kører på en underliggende fysisk og virtuel infrastruktur, der stilles til rådighed af en tredjepart (tredjeparts-IaaS).

Da den intelligente termostat ikke ville kunne udføre de intelligente funktioner uden fjerndatabehandling, ville fraværet heraf forhindre produktet med digitale elementer i at udføre en eller flere af funktionerne. Desuden er softwaren udviklet og designet under fabrikanten af den intelligente termostats ansvar. Fjerndatabehandlingen betragtes derfor som RDPS som defineret i CRA.

Med henblik på overholdelse af CRA skal fabrikanten af den intelligente termostat dokumentere den pågældende RDPS samt afhængigheden af tredjeparts-IaaS i den tekniske dokumentation for produktet med digitale elementer, herunder oplysninger om den aftalte tjeneste. Fabrikanten skal tage disse elementer i betragtning i risikovurderingen, som omfatter det tilsigtede formål og den anvendelse af produktet med digitale elementer, der med rimelighed kan forudses. Fabrikanten gennemfører de væsentlige krav i CRA i forhold til den pågældende RDPS på grundlag af risiciene. Med hensyn til den pågældende tredjeparts-IaaS skal fabrikanten sikre, at de sikkerhedsforanstaltninger, som tredjepartsudbyderen stiller til rådighed, er passende, og/eller træffe relevante foranstaltninger i forhold til infrastrukturen. For så vidt angår førstnævnte kan fabrikanten f.eks. anmode om dokumentation for, at NIS 2-forpligtelserne er opfyldt.

8.3.3. *E-bogslæser*

Fabrikanten af en e-bogslæsersoftware anvender en tredjeparts-SaaS-lagringstjeneste til at lagre elektroniske bøger, som kunderne har købt, og give kunderne adgang til bøgerne. Fraværet af denne lagringstjeneste ville forhindre produktet med digitale elementer i at udføre en af funktionerne, men tredjeparts-SaaS-lagringstjenesten er ikke udviklet af eller under fabrikantens ansvar. SaaS-udbyderen gør den tilgængelig for kunderne ved alle anvendelser.

SaaS-lagringstjenesten opfylder ikke definitionen af RDPS. Fabrikanten af e-bogslæseren er imidlertid afhængig af denne eksterne tjeneste for, at produktet med digitale elementer kan fungere, og fabrikanten skal derfor tage de dermed forbundne risici i betragtning i cybersikkerhedsrisikovurderingen. Fabrikanten af e-bogslæseren bør behandle den pågældende SaaS som en komponent. Fabrikanten skal gennemføre passende sikkerhedsforanstaltninger på produktniveau, såsom sikker autentificering, kryptering og integritetsbeskyttelse af kommunikation med lagringstjenesten. Due diligence ved udvælgelse og integration af SaaS-udbyderen vil også understøtte fabrikantens forpligtelser, således at produktet med digitale elementer som helhed kan opfylde de væsentlige krav.

8.3.4. *Industrirobot*

En industrirobot har til opgave at samle dele op. Robotten sender oplysninger, der er indsamlet via kameraer, til en fjerntjeneste, der er designet og udviklet af fabrikanten. Denne tjeneste kører på en underliggende fysisk og virtuel infrastruktur, der stilles til rådighed af en tredjepartstjenesteudbyder (tredjeparts-IaaS). Cloudtjenesten beregner delenes position på grundlag af kamerafeeds og sender kommandoer tilbage til robotten om at samle delene op.

Fraværet af denne databehandling ville forhindre industrirobotten i at samle dele op og dermed i at udføre en af funktionerne. Desuden er den software, der kører på infrastrukturen, designet og udviklet af fabrikanten. Den software, der er designet og udviklet af fabrikanten, opfylder definitionen af RDPS.

Fabrikanten af industrirobotten skal dokumentere den pågældende RDPS samt afhængigheden af tredjeparts-IaaS i den tekniske dokumentation for produktet med digitale elementer (herunder oplysninger om den aftalte tjeneste). Fabrikanten skal også tage disse elementer i betragtning i risikovurderingen, som omfatter det tilsigtede formål og den anvendelse af produktet med digitale elementer, der med rimelighed kan forudses. Fabrikanten gennemfører de væsentlige krav i CRA for produktet med digitale elementer, herunder dets RDPS, på grundlag af risiciene. Due diligence i forbindelse med udvælgelsen af IaaS-udbyderen understøtter også fabrikantens forpligtelser. Fabrikanten kan f.eks. anmode om dokumentation for, at NIS 2-forpligtelserne er opfyldt.

8.3.5. *Mobilnet*

En smartphone benytter 5G-internet til at give brugerne internetforbindelse samt telefon- og beskedfunktioner (mobilkonnektivitet). Mobilnettet er udviklet og designet af teleoperatører. Netværket omfatter småceller og mobilmaster samt andet netværksudstyr.

Produktet med digitale elementer bør kunne oprette korrekt forbindelse til et netværk, da det er en af produktets funktioner. Hvorvidt netværket er i drift eller ej, er imidlertid ikke relevant for at fastslå, om produktet med digitale elementer fungerer korrekt. Netværket er alene en kommunikationskanal og er ikke nødvendigt for, at produktet med digitale elementer kan udføre funktionen med »at oprette korrekt forbindelse til et netværk«. Tilsvarende anses et ethernetkabel, en router eller et Wi-Fi-signal ikke for databehandling, hvis fravær ville forhindre produktet med digitale elementer i at udføre en af funktionerne, men snarere som en muliggørende faktor for kommunikation/konnektivitet.

Mobilnettet opfylder derfor ikke definitionen af RDPS. Netværket bør ikke behandles som en tredjepartskomponent, da der ikke er nogen software integreret i produktet med digitale elementer, og produktet i stedet blot benytter dette netværk. Som følge heraf er det ikke nødvendigt for fabrikanten at opfylde due diligence-forpligtelser over for netudbyderen.

9. **YDERLIGERE ELEMENTER**

9.1. **Indberetningsforpligtelser**

209. I henhold til artikel 14, stk. 1 og 3, i CRA skal en fabrikant samtidig underrette den CSIRT, der er udpeget som koordinator, og ENISA om i) enhver aktivt udnyttet sårbarhed i fabrikantens produkt med digitale elementer, som fabrikanten får kendskab til, og ii) enhver alvorlig hændelse, der har indvirkning på sikkerheden i fabrikantens produkt med digitale elementer, som fabrikanten får kendskab til.

210. I overensstemmelse med artikel 69, stk. 3, og artikel 71, stk. 2, andet punktum, finder forpligtelsen til at overholde artikel 14 anvendelse fra den 11. september 2026 på alle produkter med digitale elementer, der er omfattet af anvendelsesområdet for CRA, herunder produkter med digitale elementer, der er bragt i omsætning inden den 11. december 2027. Endvidere finder indberetningsforpligtelserne, i modsætning til forpligtelserne vedrørende håndtering af sårbarheder, som kun gælder i produktets vedligeholdelsesperiode, fortsat anvendelse, efter at et produkt med digitale elementer ikke længere understøttes. Hvis et produkt med digitale elementer er bragt i omsætning inden den 11. december 2027, eller hvis dets vedligeholdelsesperiode er udløbet, er fabrikanten ikke forpligtet til at overholde forpligtelserne vedrørende håndtering af sårbarheder, der er fastsat i del II i bilag I.

211. Det bør erindres, at forpligtelsen til at underrette om sådanne forhold finder anvendelse, når fabrikanten får kendskab til, at en sårbarhed udnyttes aktivt, eller at der er indtruffet en alvorlig hændelse, som har medført, at sikkerheden i fabrikantens produkt med digitale elementer er blevet kompromitteret. Vejledningen om, hvornår en fabrikant anses for at have fået kendskab, skal derfor hjælpe fabrikanterne med at fastslå det tidspunkt, hvor de gældende indberetningsfrister begynder at løbe.

212. Fabrikanter kan være underlagt sammenlignelige indberetningsforpligtelser i henhold til forskellige EU-retsakter. For at sikre, at begrebet »at få kendskab« fortolkes ensartet, og for at lette fabrikanternes overholdelse af disse forpligtelser er denne vejledning tilpasset betragtning 31 i Kommissionens gennemførelsesforordning (EU) 2024/2690 og afsnit II(A) i retningslinjerne 9/2022 om anmeldelse af brud på persondatasikkerheden i henhold til databeskyttelsesforordningen.

213. I visse tilfælde opdager en fabrikant en mistænkelig hændelse, eller en tredjepart, såsom en enkeltperson, en kunde, en enhed, en myndighed, en medieorganisation eller en anden kilde, gør fabrikanten opmærksom på en mulig hændelse eller sårbarhed. I sådanne tilfælde bør fabrikanten straks vurdere den mistænkelige hændelse for at fastslå, om den udgør en aktivt udnyttet sårbarhed eller en alvorlig hændelse, der har indvirkning på produktet med digitale elementers sikkerhed. Fabrikanten anses derfor for at have fået kendskab, når fabrikanten efter en sådan indledende vurdering med en rimelig grad af sikkerhed kan fastslå, at: i) en sårbarhed i fabrikantens produkt med digitale elementer udnyttes aktivt, eller ii) en alvorlig hændelse er indtruffet og har medført, at sikkerheden i fabrikantens produkt med digitale elementer er blevet kompromitteret.

214. Det tidspunkt, hvor en fabrikant kan anses for at have fået kendskab hertil, afhænger derfor af omstændighederne ved den specifikke aktivt udnyttede sårbarhed eller alvorlige hændelse. I visse tilfælde er det fra begyndelsen relativt klart, at en sårbarhed udnyttes aktivt, eller at en alvorlig hændelse har indvirkning på produktet med digitale elementers sikkerhed. I andre tilfælde kan det tage noget tid at fastslå, om et produkt med digitale elementer er berørt af en sårbarhed, og om denne sårbarhed udnyttes af en ondsindet aktør, eller om en hændelse har indvirkning på et produkt med digitale elementers sikkerhed. Der bør dog lægges vægt på hurtig handling for at foretage den indledende vurdering med henblik på at fastslå, om disse betingelser faktisk er opfyldt, navnlig hvis sårbarheden kan udgøre en væsentlig risiko, og i givet fald på at træffe afhjælpende foranstaltninger og foretage underretning i overensstemmelse med CRA.

215. Endvidere indebærer indberetningsforpligtelsernes struktur, at fabrikanterne skal opdatere deres underretninger løbende, efterhånden som de interne undersøgelser skrider frem, og deres viden om den aktivt udnyttede sårbarhed eller hændelse bliver mere detaljeret. Fabrikanterne skal navnlig indgive en tidlig varsling, der indeholder begrænsede oplysninger, uden unødig forsinkelse og under alle omstændigheder senest 24 timer efter, at de har fået kendskab hertil. Der kræves efterfølgende yderligere oplysninger som led i den underretning, der skal indgives uden unødig forsinkelse og under alle omstændigheder inden for 72 timer efter, at fabrikanten har fået kendskab hertil (»72-timersunderretning«). Den endelige rapport skal indgives senest 14 dage efter, at en korrigerende eller afbødende foranstaltning er gjort tilgængelig, for så vidt angår aktivt udnyttede sårbarheder, eller senest en måned efter 72-timersunderretningen, for så vidt angår alvorlige hændelser.

216. Som det også er nævnt i afsnit *3.3.1 Vedvarende støtte og sikring af levedygtigheden af* en FOSS, skal open source-softwareforvaltere også indberette aktivt udnyttede sårbarheder i overensstemmelse med artikel 24, stk. 3 ([30]). Denne forpligtelse finder anvendelse, når der er opnået kendskab til en aktivt udnyttet sårbarhed, og ikke blot når der findes en sårbarhed i kodebasen for FOSS, som den pågældende enhed er forvalter for. I praksis vil en forvalter, fordi FOSS-komponenter typisk integreres downstream i andre produkter med digitale elementer, sandsynligvis få kendskab til aktiv udnyttelse gennem rapporter fra tredjeparter, som identificerer udnyttelse af FOSS-komponenter, der er integreret i andre produkter med digitale elementer. Dette kan f.eks. være tilfældet, hvis en fabrikant af et produkt med digitale elementer opdager aktiv udnyttelse vedrørende en FOSS-komponent, der er integreret i fabrikantens eget produkt, og indberetter dette til komponentens forvalter, eller hvis en bruger eller en sikkerhedsfagmand finder bevis for udnyttelse af en FOSS-komponent, der er integreret i et produkt med digitale elementer, og indberetter denne aktive udnyttelse til komponentens forvalter.

217. Det bør også præciseres, at eftersom forpligtelsen til at indberette aktivt udnyttede sårbarheder finder anvendelse, når fabrikanten får kendskab til aktiv udnyttelse, er fabrikanten ikke forpligtet til at indberette sårbarheder, hvis aktive udnyttelse fabrikanten allerede havde fået kendskab til inden den 11. september 2026 (den dato, hvor indberetningsforpligtelsen finder anvendelse). CRA kræver derfor ikke, at sådanne sårbarheder indberettes med tilbagevirkende kraft. Derimod finder forpligtelsen anvendelse, hvis fabrikanten havde kendskab til en sårbarhed inden den 11. september 2026, men på det tidspunkt ikke havde kendskab til nogen aktiv udnyttelse af den (enten fordi en sådan udnyttelse endnu ikke havde fundet sted, eller fordi fabrikanten ikke havde fået kendskab til det). Hvis aktiv udnyttelse efterfølgende finder sted efter den 11. september 2026, eller fabrikanten får kendskab til hertil, anses sårbarheden for at være en aktivt udnyttet sårbarhed, der er omfattet af indberetningsforpligtelsen.

218. Tilsvarende er en fabrikant kun forpligtet til at indberette aktivt udnyttede sårbarheder, der vedrører fabrikantens produkt med digitale elementer. Hvis et produkt med digitale elementer omfatter en aktivt udnyttet sårbarhed, der stammer fra en tredjepartskomponent, skal fabrikanten af produktet med digitale elementer underrette om denne aktivt udnyttede sårbarhed. Hvis en fabrikant imidlertid har kendskab til, at en tredjepartskomponent indeholder en sårbarhed, men denne sårbarhed enten i) ikke kan udnyttes i fabrikantens produkt med digitale elementer (f.eks. fordi den sårbare kode ikke kan nås) eller ii) ikke er blevet udnyttet i fabrikantens produkt med digitale elementer, udgør denne sårbarhed ikke en aktivt udnyttet sårbarhed i fabrikantens produkt med digitale elementer og er derfor ikke omfattet af obligatorisk indberetning for den pågældende fabrikant. Fabrikanten kan dog indberette sårbarheden frivilligt i overensstemmelse med artikel 15 i CRA. Fabrikanten er også forpligtet til at overholde kravene vedrørende håndtering af sårbarheder i del II i bilag I til CRA samt til at indberette sårbarheden til den person eller enhed, der fremstiller eller vedligeholder komponenten, i overensstemmelse med artikel 13, stk. 6, og som nærmere forklaret i afsnit *9.2.1 Indberetning upstream og deling af rettelser* af sikkerhedsfejl.

([30]) I det omfang forvalteren er involveret i udviklingen af et produkt med digitale elementer.

219. Efter at have fået kendskab til en aktivt udnyttet sårbarhed eller en alvorlig hændelse skal fabrikanter i overensstemmelse med artikel 14, stk. 8, også informere berørte brugere og, hvor det er relevant, alle brugere. Hvis de ikke gør dette rettidigt, kan de CSIRT, der har modtaget underretningen, give brugerne sådanne oplysninger, når dette anses for forholdsmæssigt og nødvendigt for at forhindre eller afbøde virkningen af den pågældende sårbarhed eller hændelse.

220. I overensstemmelse med den risikobaserede tilgang i medfør af CRA skal forpligtelsen til at informere brugerne, der er fastsat i artikel 14, stk. 8, anvendes på en risikobaseret og forholdsmæssig måde. Navnlig indebærer formidling af oplysninger om en aktivt udnyttet sårbarhed eller en alvorlig hændelse ikke, at sådanne oplysninger skal offentliggøres eller videregives ukritisk. Hvor det er relevant, og i lyset af arten af produktet med digitale elementer, de berørte brugere og sårbarhedens eller hændelsens mulige indvirkning, kan fabrikanter begrænse videregivelsen af detaljerede oplysninger til de relevante brugere eller kunder, der er berørt. Dette er navnlig tilfældet for produkter med digitale elementer, der anvendes i følsomme eller kritiske miljøer, hvor offentliggørelse af tekniske detaljer i sig selv kan medføre øgede cybersikkerhedsrisici eller lette yderligere udnyttelse.

221. Når sårbarheden er blevet tilstrækkeligt håndteret eller afbødet, kan en bredere offentliggørelse være hensigtsmæssig. Dette vil f.eks. være tilfældet, hvis offentliggørelsen bidrager til at øge det generelle kendskab eller gør det muligt for brugerne at kontrollere, at deres produkter med digitale elementer ikke længere er berørt. I sådanne tilfælde bør detaljeringsgraden og tidspunktet for en eventuel bredere offentliggørelse fortsat være forholdsmæssige og tage hensyn til de resterende risici for udnyttelse, arten af produktet med digitale elementer og de berørte brugeres interesser. Endvidere kræves det i punkt 4) i del II i bilag I, at fabrikanter offentliggør oplysninger om afhjulpne sårbarheder, når en sikkerhedsopdatering er blevet gjort tilgængelig.

9.2. **Håndtering af sårbarheder**

9.2.1. *Indberetning upstream og deling af rettelser af sikkerhedsfejl*

222. I henhold til artikel 13, stk. 6, i CRA skal fabrikanterne indberette sårbarheder i integrerede komponenter til den person eller enhed, der fremstiller eller vedligeholder den pågældende komponent (»indberetning upstream«).

223. Fabrikanterne er kun forpligtede til at indberette upstream vedrørende den version af komponenten, som de integrerer. Hvis den person eller enhed, der fremstiller eller vedligeholder komponenten, har fastlagt sikkerhedspolitikker, processer for koordineret offentliggørelse af sårbarheder eller udpegede kanaler til indberetning af sårbarheder, bør fabrikanterne indberette i overensstemmelse hermed, navnlig hvis for tidlig offentliggørelse af sårbarheder, for hvilke der ikke foreligger en rettelse, kan øge cybersikkerhedsrisiciene. For at mindske byrden for reparatører upstream, navnlig i open source-projekter, er fabrikanter desuden ikke forpligtede til at indberette upstream, hvis de kan bekræfte, at den person eller enhed, der fremstiller eller vedligeholder en komponent, er bekendt med, at der findes en sårbarhed. Fabrikanterne opfordres til at træffe rimelige foranstaltninger for at undgå indgivelse af dobbeltindberetninger, f.eks. ved at kontrollere offentligt tilgængelige sårbarhedsdatabaser, projektspecifikke sikkerhedsmeddelelser eller etablerede systemer til problemsporing, inden de foretager indberetning upstream.

224. Fabrikanterne skal kun indberette de sårbarheder upstream, der findes i selve den integrerede komponent, og ikke sårbarheder, der opstår som følge af integrationen mellem komponenten og anden kode, som er udviklet af fabrikanten, eller som følge af integrationen af andre komponenter. Ikke desto mindre kan der opstå situationer, hvor integrationen af en komponent i et specifikt produkt med digitale elementer afslører visse former for adfærd, interaktioner eller sikkerhedsrelevante egenskaber ved den pågældende komponent, som ikke var tydelige eller ikke let kunne identificeres isoleret. I sådanne tilfælde opfordres fabrikanterne til at videregive disse oplysninger til den person eller enhed, der fremstiller eller vedligeholder komponenten, for at fremme god praksis for håndtering af sårbarheder, der har til formål at lette effektiv afhjælpning og forbedre komponentøkosystemets samlede sikkerhed.

225. Endelig er fabrikanterne heller ikke forpligtede til at indberette sårbarheden upstream, hvis komponenten ikke længere har en reparatør, eller hvis fabrikanten ikke længere benytter den oprindelige reparatør til nye versioner eller rettelser af sikkerhedsfejl. I sådanne tilfælde opfordres fabrikanten ikke desto mindre til at informere brugerne af den pågældende komponent via rimelige alternative foranstaltninger, f.eks. gennem eksisterende fællesskabsmekanismer (såsom mailinglister eller issue-tickets) eller gennem offentlige sårbarhedsregistre.

226. I henhold til artikel 13, stk. 6, skal fabrikanter, der har udviklet en softwareændring for at afhjælpe en sårbarhed i en integreret komponent, desuden dele den pågældende softwareændring (»rettelse af sikkerhedsfejl«) med den person eller enhed, der fremstiller eller vedligeholder komponenten (»deling upstream«).

227. Hvis fabrikanterne er forpligtede til at dele en rettelse af sikkerhedsfejl i henhold til artikel 13, stk. 6, bør rettelsen, hvor det er relevant, leveres i et maskinlæsbart format på en måde, som let kan verificeres og, hvor det er relevant, integreres af den person eller enhed, der fremstiller eller vedligeholder komponenten. Hvis komponenten er en fri og open source-komponent, bør rettelsen af sikkerhedsfejl deles på en måde, der er forenelig med den pågældende komponents licens, f.eks. ved at dele den under samme licens eller under en licens, der gør det muligt for reparatøren at distribuere rettelsen under dennes egen licens. Hvis reparatøren af den pågældende komponent har retningslinjer for, hvordan rettelser af sikkerhedsfejl bør deles, bør fabrikanten følge disse retningslinjer.

228. CRA kræver dog ikke, at fabrikanterne sikrer, at deres rettelser af sikkerhedsfejl nødvendigvis accepteres af den person eller enhed, der fremstiller eller vedligeholder komponenten. De er heller ikke forpligtede til at sikre, at disse rettelser nødvendigvis integreres i komponentens kodelager, f.eks. hvis reparatøren foretrækker en anden løsning til at afhjælpe problemet. Tilsvarende er fabrikanter ikke forpligtet til at acceptere en foreslået rettelse, som komponentens reparatør har udviklet, og de kan foretrække at afbøde problemet på andre egnede måder.

229. I visse tilfælde kan den person eller enhed, der fremstiller eller vedligeholder komponenten, allerede have leveret en rettelse af sikkerhedsfejl til afhjælpning af sårbarheden, men en fabrikant gennemfører en anden afbødningsstrategi (f.eks. ved at ændre en anden konfiguration). I sådanne tilfælde kræver CRA ikke, at fabrikanten deler ændringen af en anden del af systemet upstream. Fabrikanten opfordres dog til at gøre dette, hvis det kan støtte den person eller enhed, der vedligeholder komponenten.

9.2.2. *Kendte sårbarheder, der kan udnyttes*

230. Et af de væsentlige krav i del I i bilag I til CRA indebærer, at produkter med digitale elementer på grundlag af den cybersikkerhedsrisikovurdering, der er omhandlet i artikel 13, stk. 2, og hvor det er relevant, skal gøres tilgængelige på markedet uden kendte sårbarheder, der kan udnyttes.

231. I artikel 3, nr. 41), defineres »sårbarhed, der kan udnyttes« som »en sårbarhed, der potentielt kan udnyttes effektivt af en modstander under praktiske operationelle forhold«. Ikke alle sårbarheder kan udnyttes under praktisk operationelle forhold, og nogle sårbarheder kan kun udnyttes under teoretiske forhold (f.eks. i et laboratorium eller i en simulering) og/eller ikke under forhold, der ville forekomme i driftsmiljøet for et produkt med digitale elementer.

232. I henhold til CRA skal fabrikanterne have passende politikker og procedurer til håndtering og afhjælpning af potentielle sårbarheder, der indberettes fra interne eller eksterne kilder (artikel 13, stk. 8). CRA præciserer imidlertid ikke udtrykkeligt, hvornår en sårbarhed, der kan udnyttes, bør anses for at være kendt af fabrikanten, således at forpligtelsen til at overholde dette væsentlige krav udløses, når produktet bringes i omsætning.

233. En sårbarhed bør anses for at være kendt, når den er opført i relevante offentligt tilgængelige sårbarhedsdatabaser, såsom den europæiske sårbarhedsdatabase, der er oprettet ved artikel 12, stk. 2, i direktiv (EU) 2022/2555, eller andre almindeligt kendte sårbarhedsdatabaser.

234. Desuden kan en sårbarhed også være kendt, når fabrikanten er blevet gjort opmærksom på den via ikke-offentlige oplysninger, f.eks. ved koordineret offentliggørelse foretaget af en sikkerhedsforsker eller gennem fabrikantens egne interne test og analyser, herunder f.eks. ved anvendelse af AI-drevne tjenester. Ligeledes kan en sårbarhed være kendt, når den er blevet offentligt og fremtrædende omtalt i pålidelige medier, herunder specialiserede cybersikkerhedspublikationer eller almindelige massemedier.

235. Ikke desto mindre betyder alene det forhold, at en sårbarhed indberettes eller findes, ikke i sig selv, at den kan udnyttes i praksis eller er relevant for det specifikke berørte produkt med digitale elementer. Fabrikanten skal undersøge sårbarheden og bekræfte rigtigheden af sådanne oplysninger samt deres relevans for fabrikantens eget produkt med digitale elementer. Der kan derfor gå et begrænset tidsrum mellem den første indberetning af sårbarheden og bekræftelsen heraf. Som angivet i afsnit 9.1 *Indberetningsforpligtelser* bør der lægges vægt på hurtig indsats for at undersøge en sårbarhed og iværksætte en reaktion.

236. Desuden finder fabrikanternes forpligtelse til at overholde de væsentlige krav i del I i bilag I anvendelse på det tidspunkt, hvor produktet bringes i omsætning, jf. artikel 13, stk. 1. I praksis kan det forekomme, at nye sårbarheder, der potentielt kan udnyttes, opdages i de sidste faser af udviklingslivscyklussen for produktet med digitale elementer, herunder kort før det indgår i distributionskæden (og derfor bringes i omsætning).

237. Da forpligtelsen til at bringe produkter med digitale elementer i omsætning uden kendte sårbarheder, der kan udnyttes, er en risikobaseret forpligtelse, påhviler det fabrikanten på grundlag af cybersikkerhedsrisikovurderingen at afgøre, om produktet med digitale elementer på en sikker måde kan bringes i omsætning i overensstemmelse med CRA. Alternativt kan fabrikanten fastslå, at en ny sårbarhed, der kan være blevet kendt, skal afhjælpes, før produktet med digitale elementer kan bringes i omsætning. Ved denne afgørelse bør fabrikanterne tage hensyn til sårbarhedens alvor, udnyttelighed og mulige indvirkning samt de risici, der opstår for selve produktet med digitale elementer, når det er i brug. De kan også tage hensyn til risiciene ved at udsætte frigivelsen af produktet, indtil sårbarheden er afhjulpet, f.eks. fordi den nye version også afhjælper andre sårbarheder, der kan udnyttes, eller er nødvendig for den fortsatte drift af kritiske systemer. Under alle omstændigheder forbliver fabrikanten, når et produkt med digitale elementer er bragt i omsætning, omfattet af forpligtelsen til at håndtere sårbarheder effektivt og i overensstemmelse med kravene til håndtering af sårbarheder i del II i bilag I.

9.2.3. *Effektive og regelmæssige test og gennemgange*

238. Punkt (3) i del II i bilag I kræver, at fabrikanterne gennemfører effektive og regelmæssige test og gennemgange af produktet med digitale elementer i hele dets vedligeholdelsesperiode. Anvendelse af regelmæssige test indebærer ikke automatisk gentagelse med faste intervaller af en uændret testrutine. Det indebærer en regelmæssig gennemgang af, om nye input, såsom nyidentificerede trusler eller nyopdagede sårbarheder, kræver, at de eksisterende test ajourføres, og at test gennemføres i overensstemmelse hermed.

239. Hyppigheden, omfanget og indholdet af gennemgangen bør stå i et rimeligt forhold til cybersikkerhedsrisikoprofilen for produktet med digitale elementer, dets udvikling over tid og trusselsbilledets tilstand. Hvis gennemgangen identificerer relevante nye input, der påvirker testrutinen, bør der udarbejdes og gennemføres nye eller ændrede test af produktet for at sikre, at alle sårbarheder bliver afhjulpet. Dette kan omfatte, at eksisterende test gennemføres på ny, hvis en ændring af produktet med digitale elementer gør sådanne typer afprøvninger hensigtsmæssige, såsom regressionstest.

240. Hvis gennemgangen ikke identificerer sådanne input, behøver der ikke at blive udarbejdet yderligere test. Andre forpligtelser vedrørende håndtering af sårbarheder, herunder forpligtelsen til at håndtere og afhjælpe sårbarheder i forhold til de risici, de udgør, finder fortsat anvendelse parallelt.

9.3. **Samspil med anden lovgivning**

9.3.1. *Forordning (EU) 2019/2144 og forordning (EU) nr. 168/2013*

241. I artikel 2, stk. 2, litra c), i CRA fastsættes det, at forordningen ikke finder anvendelse på produkter med digitale elementer, som forordning (EU) 2019/2144 finder anvendelse på. Forordning (EU) 2019/2144 finder anvendelse på »køretøjer i klasse M, N og O som defineret i artikel 4 i forordning (EU) 2018/858 og på systemer, komponenter og separate tekniske enheder, der er konstrueret og fremstillet til sådanne køretøjer«.

242. Tilsvarende er produkter med digitale elementer, der er omfattet af anvendelsesområdet for forordning (EU) nr. 168/2013, blevet udelukket fra anvendelsesområdet for CRA ved Kommissionens delegerede forordning (EU) 2025/1535. Forordning (EU) nr. 168/2013 finder anvendelse på køretøjer i klasse L og »på systemer, komponenter og separate tekniske enheder samt dele og udstyr konstrueret og fremstillet til sådanne køretøjer« (artikel 2, stk. 1).

243. Køretøjer, som nævnte forordninger finder anvendelse på, er ikke omfattet af CRA. Der er desuden behov for yderligere præciseringer af anvendelsesområdet for undtagelsen for systemer, komponenter, separate tekniske enheder, dele og udstyr (i dette afsnit »komponenter«), der er konstrueret og fremstillet til sådanne køretøjer, og som anses for produkter med digitale elementer som omhandlet i CRA.

244. Sådanne komponenter anses ikke for at være omfattet af CRA, forudsat at de udelukkende er konstrueret og fremstillet med henblik på integration i køretøjer, der er omfattet af forordning (EU) 2019/2144 og forordning (EU) nr. 168/2013. Dette gælder, uanset om komponentens fabrikant sælger den direkte til køretøjsfabrikanten eller til en anden erhvervsdrivende i bilindustriens forsyningskæde, så længe komponenten klart kun er tiltænkt og egnet til endelig integration i disse køretøjer.

245. Derimod er en fabrikant omfattet af CRA, når denne sælger generiske komponenter, som er produkter med digitale elementer, der kan integreres i forskellige typer produkter og ikke udelukkende i køretøjer, der er omfattet af nævnte forordninger.

246. Vurderingen af, om en komponent er bragt i omsætning som omhandlet i CRA, skal baseres på de objektive betingelser, hvorunder den gøres tilgængelig. Hvis en fabrikant udbyder en komponent, der ikke udelukkende er egnet til endelig integration i disse køretøjer, via distributionskanaler, der er åbne for kunder uden for bilindustriens forsyningskæde, såsom almindelige detailforretninger eller onlinesalgskanaler, der modtager ordrer fra offentligheden, er komponenten omfattet af anvendelsesområdet for CRA, uanset eventuelle erklæringer om den tilsigtede anvendelse. Under sådanne omstændigheder kan komponenten ikke anses for udelukkende at være konstrueret og fremstillet med henblik på integration i køretøjer, der er omfattet af forordning (EU) 2019/2144 og forordning (EU) nr. 168/2013, og fabrikanten er forpligtet til at overholde CRA. Derimod kan anvendelse af begrænsede distributionskanaler mellem virksomheder, der er afgrænset til bilindustriens forsyningskæde, tyde på, at komponenten udelukkende er konstrueret og fremstillet med henblik på en sådan integration.

9.3.2. *EU-typeafprøvningsattesters gyldighed (artikel 69, stk. 1)*

247. I artikel 69, stk. 1, i CRA hedder det, at »udstedte EU-typeafprøvningsattester og afgørelser om godkendelse vedrørende cybersikkerhedskrav til produkter med digitale elementer, der er omfattet af anden EU-harmoniseringslovgivning end denne forordning, forbliver gyldige indtil 11. juni 2028, medmindre de udløber inden denne dato, eller medmindre andet er angivet i sådan anden EU-harmoniseringslovgivning, i hvilket tilfælde de forbliver gyldige som omhandlet i den pågældende lovgivning«.

248. Den fortsatte gyldighed af sådanne attester og afgørelser om godkendelse bør forstås således, at den er begrænset til de cybersikkerhedsrisici og tilsvarende krav, der er omfattet af den respektive EU-harmoniseringslovgivning, på grundlag af hvilken de blev udstedt. For så vidt angår disse risici er fabrikanterne ikke forpligtede til på ny at vurdere eller på ny at påvise overensstemmelse udelukkende med henblik på CRA i den gyldighedsperiode, der er omhandlet i artikel 69, stk. 1, for produkter med digitale elementer, som de agter at bringe i omsætning fra og med den 11. december 2027 og indtil den 11. juni 2028 ([31]). Dette gælder for attester og afgørelser om godkendelse, der er udstedt, når den gældende EU-harmoniseringslovgivning kræver, at fabrikanten gennemfører overensstemmelsesvurderingsproceduren via et bemyndiget organ, samt når fabrikanten frivilligt har valgt at gøre det.

249. Følgelig fritager eksistensen af en gyldig attest eller afgørelse om godkendelse i henhold til anden EU-harmoniseringslovgivning ikke fabrikanterne fra at foretage en omfattende cybersikkerhedsrisikovurdering i henhold til CRA (eller fra andre forpligtelser i henhold til den). Dette giver dem i stedet mulighed for at basere sig på eksisterende certificeringer som dokumentation for overensstemmelse i forbindelse med deres overensstemmelsesvurderingsprocedure, i det omfang de tilsvarende cybersikkerhedsrisici allerede er dækket. Hvis attesten eller afgørelsen om godkendelse er gyldig i henhold til anden EU-harmoniseringslovgivning, der rækker ud over den 11. juni 2028, kan fabrikanten ikke desto mindre kun basere sig på en sådan attest eller afgørelse for så vidt angår CRA indtil den 11. juni 2028.

250. Hvis der i den cybersikkerhedsrisikovurdering, der foretages i overensstemmelse med artikel 13, stk. 2, identificeres yderligere risici, som ikke er omfattet af de cybersikkerhedskrav, der ligger til grund for den eksisterende attest eller afgørelse om godkendelse, er fabrikanterne fortsat ansvarlige for at håndtere disse risici i overensstemmelse med CRA. I sådanne tilfælde kræver overholdelse, at de identificerede mangler vurderes og afhjælpes, uanset den fortsatte gyldighed af den eksisterende attest eller afgørelse om godkendelse.

251. Dette kan illustreres ved at se på det tilfælde, hvor et produkt med digitale elementer er omfattet af de cybersikkerhedskrav, der er fastsat i Kommissionens delegerede forordning (EU) 2022/30 om supplerende regler til direktiv 2014/53/EU (den delegerede retsakt til radioudstyrsdirektivet (RED)), og hvor der er udstedt en EU-typeafprøvningsattest eller en afgørelse om godkendelse på grundlag af disse krav. I så fald forbliver attesten eller afgørelsen gyldig i overensstemmelse med artikel 69, stk. 1, for de cybersikkerhedsrisici, der er omfattet af attesten og vedrører de væsentlige cybersikkerhedskrav i direktiv 2014/53/EU (radioudstyrsdirektivet eller »RED«).

252. I sådanne tilfælde er fabrikanterne ikke forpligtede til for så vidt angår CRA at foretage en ny vurdering eller på ny påvise overensstemmelse med hensyn til de risici, der allerede er håndteret i disse attester, så længe den relevante attest eller afgørelse om godkendelse er gyldig, og under alle omstændigheder ikke efter den 11. juni 2028. Dette omfatter f.eks. cybersikkerhedsrisici vedrørende netværksbeskyttelse, beskyttelse af personoplysninger og privatlivets fred eller forebyggelse af svig, som vedrører cybersikkerhedskravene i RED og afspejles i overensstemmelsesvurderingen (i det omfang disse risici er omfattet af attesten).

253. Hvis der i den cybersikkerhedsrisikovurdering, der foretages i overensstemmelse med artikel 13, stk. 2, i CRA, identificeres yderligere cybersikkerhedsrisici, som ikke er omfattet af disse attester, er fabrikanterne dog fortsat ansvarlige for at håndtere disse risici i overensstemmelse med CRA. Dette kan f.eks. omfatte risici vedrørende processer for håndtering af sårbarheder, dataminimering og reduktion af angrebsfladen eller andre produktspecifikke cybersikkerhedsaspekter, der ikke er håndteret i disse attester eller under alle omstændigheder ikke er omfattet af de væsentlige cybersikkerhedskrav i RED.

254. Følgelig påviser eksistensen af en gyldig EU-typeafprøvningsattest eller afgørelse om godkendelse i henhold til RED for så vidt angår direktivets væsentlige krav vedrørende cybersikkerhed ikke i sig selv fuld overensstemmelse med CRA. Den gør det i stedet muligt for fabrikanterne at basere sig på den pågældende attest eller afgørelse som dokumentation for overensstemmelse med hensyn til de tilsvarende risici, samtidig med at de sikrer, at eventuelle resterende eller nyligt identificerede risici vurderes og afhjælpes i overensstemmelse med CRA.

([31]) Produkter med digitale elementer, der er bragt i omsætning inden den 11. december 2027, er omfattet af den EU-lovgivning, der fandt anvendelse på det tidspunkt, hvor de blev bragt i omsætning, og hvis de var i overensstemmelse med denne, kan de sælges og tages i brug, medmindre de underkastes væsentlige ændringer pr. den 11. december 2027 eller derefter. Vedrørende begreberne »bringen i omsætning« og »tilgængeliggørelse på markedet« se også afsnit *2.1 Placing on the market* i dette dokument samt kapitel 2 i den blå vejledning.

255. Tilsvarende gælder det, at hvis et produkt med digitale elementer er omfattet af de cybersikkerhedsrelaterede væsentlige sikkerheds- og sundhedskrav, der er fastsat i forordning (EU) 2023/1230 (maskinforordningen), som finder fuldt ud anvendelse fra den 20. januar 2027, og hvis der er udstedt en EU-typeafprøvningsattest eller en afgørelse om godkendelse på grundlag af disse krav, forbliver attesten eller afgørelsen om godkendelse gyldig i overensstemmelse med artikel 69, stk. 1, i CRA for de cybersikkerhedsrisici, der er omfattet af maskinforordningen.

256. Dette vedrører navnlig cybersikkerhedsaspekter i forbindelse med beskyttelse mod korruption og styresystemers sikkerhed og pålidelighed, jf. afsnit 1.1.9 og 1.2.1 i bilag III til maskinforordningen. For så vidt angår disse risici er fabrikanterne ikke forpligtede til med henblik på CRA at foretage en ny vurdering eller på ny påvise overensstemmelse, så længe den relevante attest eller afgørelse om godkendelse er gyldig, og under alle omstændigheder ikke efter den 11. juni 2028. Dette gælder, i det omfang disse risici er blevet håndteret som led i overensstemmelsesvurderingen i henhold til maskinforordningen.

257. Som med de væsentlige cybersikkerhedskrav i RED, der er nævnt ovenfor, gælder det, at hvis der i den cybersikkerhedsrisikovurdering, der er foretaget i henhold til artikel 13, stk. 2, i CRA, identificeres yderligere cybersikkerhedsrisici, som ikke er omfattet af den relevante attest, der er udstedt i henhold til maskinforordningen, og som vedrører de cybersikkerhedsrelaterede sikkerhedskrav i nævnte forordning, er fabrikanterne fortsat ansvarlige for at håndtere disse risici i overensstemmelse med CRA.