ERHVERVSMINISTERIET

GRUND- OG NÆRHEDSNOTAT TIL FOLKETINGETS EUROPAUDVALG

18. november 2022

Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020, KOM (2022) 454

1. Resumé

Forordningsforslaget fastsætter horisontale cybersikkerhedskrav for producenter og udviklere af produkter med digitale elementer med henblik på at højne cybersikkerhedsniveauet på tværs af EU. Kravene skal gøre produkter, der er forbundet til internettet, sikrere, og gøre producenter ansvarlige for cybersikkerhed gennem hele produktets livscyklus. Forordningen skal også forbedre forbrugernes adgang til information om cybersikkerhed.

I forslaget lægges der op til at fastsætte en række krav, der skal sikre et minimumsniveau for cybersikkerhed i produkter. Der er lagt op til at specificere kravene yderligere gennem harmoniserede standarder, der skal udvikles i samarbejde med industrien. Kommissionen har udarbejdet en liste over særligt kritiske produkter, der skal certificeres af en tredjepart, før de kan sælges på det indre marked. Der lægges op til, at Kommissionen får bemyndigelse til at specificere og opdatere denne liste.

Både erhvervsliv og medlemsstater har overordnet taget positivt imod forslaget. Det gælder særligt det høje ambitionsniveau, hvor forslaget dækker produktområdet bredt. Der ses dog et behov for yderligere klarhed over forordningens anvendelsesområde, fx i forhold til om digitale tjenester og processer er omfattet.

Forslaget kan medføre behov for ændring af gældende regler for tilsyn med produktsikkerhed. Det vurderes, at forslaget vil medføre omkostninger for virksomhederne og få statsfinansielle konsekvenser som følge af nye forpligtelser for myndighederne.

Regeringen hilser forslaget og det høje ambitionsniveau velkomment. Kravene bør finde en passende balance mellem et højt cybersikkerhedsniveau, den digitale udvikling samt omkostninger for erhvervslivet.

2. Baggrund

Europa-Kommissionen (Kommissionen) har den 15. september 2022 fremsat et forslag til en forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer[1] (herefter 'forslaget'). Forslaget har til formål at fastsætte fælles krav til cybersikkerhed i alle produkter med digitale elementer[2] (herefter 'produkter') for at øge cybersikkerheden på tværs af EU og styrke det indre markeds funktion.

Forslaget blev oversendt til Rådet i dansk sprogversion den 24. oktober 2022. Forslaget har retsgrundlag i artikel 114 TFEU, som indeholder bestemmelser om vedtagelse af foranstaltninger med henblik på at sikre det indre markeds oprettelse og funktion. Forslaget behandles efter den almindelige beslutningsprocedure og vedtages med kvalificeret flertal i Rådet.

Kommissionen er i stigende grad blevet opmærksom på, at cybersikkerheden i EU bør styrkes, og har i 2020 udarbejdet en strategi på området[3]. Strategiens fokus er at sikre et globalt og åbent internet og samtidig beskytte borgernes sikkerhed, grundlæggende rettigheder og friheder. Der er i de senere år igangsat en række tiltag herom, fx regulering af kritisk infrastruktur, radioudstyr, certificering af cybersikkerhedsprodukter samt styrkelse af cybersikkerhed på tværs af Unionen.

Forslaget bunder i, at selvom brugen af produkter med digitale elementer (inkl. software) er stærkt stigende, er cybersikkerheden i disse produkter ofte lav eller ikke eksisterende. Det udgør en betydelig risiko, der overordnet kan sammenfattes således:

1. Produkterne kan anvendes som springbræt til at få adgang til netværk, som de er koblet på, og derved også til andre systemer, som er forbundet til disse netværk. Det kan fx være, at man får adgang til servere via et web-kamera, en mobiltelefon eller en robotstøvsuger, som er forbundet til det samme netværk.

[1] KOM (2022) 454 – EUROPA-PARLAMENTETS OG RÅDETS FORORDNING
om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020)
[2] Defineret som: ethvert software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der skal bringes i omsætning separat
[3] JOIN (2020) 18 – Final - EU's strategi for cybersikkerhed for det digitale årti

2. Produkter, der er kompromitterede, kan i nogle tilfælde bruges til koordinerede storskalaangreb. Fx kan mange produkter sættes til samtidigt at rette en datastrøm mod en bestemt modtager for at overbelaste modtagerens system, der derved ikke kan fungere som tiltænkt. Det kan fx være handelsplatforme, myndighedsportaler eller andre digitale tjenester, der bliver gjort ubrugelige eller utilgængelige. Dette kaldes "Distributed Denial of Service" -angreb (DDoS).

Disse risici øger omkostningerne for brugerne og samfundet og skyldes ifølge Kommissionens undersøgelser primært:

1. Et lavt niveau af cybersikkerhedsforanstaltninger og utilstrækkelige sikkerhedsopdateringer
2. En utilstrækkelig forståelse for cybersikkerhed hos brugerne og hertil utilstrækkelig adgang til information om cybersikkerhed i produkter, som forhindrer brugerne i at vælge sikre produkter og bruge dem på en sikker måde.

Kommissionens konsekvensanalyse viser, at 60 procent af alle sikkerhedsbrud i de kritiske sektorer såsom sundhed og telekommunikation skyldes sårbarheder i hardware og software. En lignende andel af forbrugerprodukter har kritiske sårbarheder. Vellykkede cyberangreb blev estimeret til at koste ca. 41 milliarder danske kroner globalt i 2021[4].

Der opdages ca. 20.000 nye digitale sårbarheder hvert eneste år. De kan true sikkerheden i eksisterende produkter, da sårbarhederne ikke var kendt, da produkterne blev lavet. Derfor ser Kommissionen et behov for, at reguleringen tager hånd om denne udfordring gennem produktets livscyklus. Det betyder fx, at produktet løbende opdateres, når der findes nye sårbarheder.

Ifølge Kommissionen er der en række strukturelle forhold som gør, at ny EU-regulering er særlig relevant på området:

- Markedet efterspørger ikke aktivt cybersikkerhed, og leverandørerne prioriterer det derfor ikke nødvendigvis. Dertil er der et vist pres mod bunden, hvor det handler om at producere billigt og udvikle hurtigt og ikke nødvendigvis gennemlyse alle de komponenter, et produkt består af, med hensyn til cybersikkerhed.
- Cybersikkerheden i produkter går på tværs af landegrænser, da produkter fremstillet i ét land ofte bruges i andre lande. Hændelser kan, inden for få minutter, spredes over hele det indre marked.
- Cybersikkerheden i de fleste hardware- og softwareprodukter er i øjeblikket ikke omfattet af EU-lovgivning. Især behandler den nuværende EU-ret ikke cybersikkerheden af software, der ikke indgår i et

[4] Kilde: Europa-Kommissionens Fælles Forskningscenter (JRC), 2020: "Cybersecurity – Our Digital Anchor, a European perspective", s. 7.

fysisk produkt, som fx computerspil og andre programmer. Det er selvom cybersikkerhedsangreb i stigende grad retter sig mod sårbarheder i disse produkter, hvilket forårsager betydelige samfundsmæssige og økonomiske omkostninger.

Forordningen skal harmonisere EU's regler og undgå overlappende krav på området for cybersikkerhed. Forordningen skal især supplere NIS2-direktivet[5], som for nylig blev vedtaget af Europa-Parlamentet og Rådet.

Radioudstyr vil også være dækket af forslaget. Indtil forordningen er forhandlet færdig og træder i kraft, er raditioudstyr reguleret af en delegerede retsakt[6] under radioudstyrsdirektivet[7] om cybersikkerhed, der vil blive ophævet efterfølgende.

3. Formål og indhold

Hovedformålene med forslaget er at øge cybersikkerheden i EU og forbedre det indre markeds funktion. Dette skal ske ved at:

- strømline og supplere de eksisterende regler; og
- forhindre yderligere fragmentering af cybersikkerhedskravene til produkter med digitale elementer gennem en horisontal forordning.

Dette skal overordnet opnås gennem horisontale krav til cybersikkerheden i produkter og krav til, at producenter tager sikkerhed seriøst gennem hele produktets livscyklus. Derudover skal der være de rette betingelser for, at brugerne kan tage hensyn til cybersikkerhed, når de udvælger og bruger produkter med digitale elementer.

I forslaget lægger Kommissionen op til at tage udgangspunkt i den såkaldte 'Ny Metode'[8]. Det betyder, at forordningen fastlægger nogle overordnede krav, som efterfølgende skal detaljeres i en række harmoniserede standarder. Derved kan reguleringen holdes på et overordnet niveau og samtidig bliver industrien involveret i udarbejdelsen af de detaljerede tekniske krav igennem standardiseringsorganisationerne.

---

[5] 2020/0359 (COD): Forslag om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148

[6] 2022/30/EU

[7] 2014/53/EU

[8] New Legislative Framework: vedtaget i 2008, har til formål at forbedre det indre marked for varer og styrke betingelserne for at bringe en bred vifte af produkter på EU-markedet. Det er en pakke af foranstaltninger, der har til formål at forbedre markedsovervågningen og øge kvaliteten af overensstemmelsesvurderinger. Det tydeliggør også brugen af CE-mærkning og skaber en værktøjskasse med foranstaltninger til brug i produktlovgivningen. Den Ny Metode er også anvendt i andre igangværende forslag, fx i AI-forordningen (2021/0106(COD)) og Maskinforordningen (2021/0105(COD)).

Produkter er som udgangspunkt alene underlagt producenternes egen evaluering af, hvorvidt de lever op til kravene. Kommissionen har dog udarbejdet en liste over produkter, der har en særlig kritisk karakter eller anvendelse, som vil være underlagt krav om egentlig certificering. Det kan fx være routere. Forslaget dækker ikke produkter, som allerede er underlagt cybersikkerhedskrav i eksisterende sektorspecifikke EU-regler, fx medicinsk udstyr, luftfart og køretøjer. Forslaget dækker heller ikke produkter, der udelukkende udvikles til nationale sikkerhedsformål eller militære formål, eller produkter, der er specifikt designet til at behandle klassificerede oplysninger.

Kapitel I: Almindelige bestemmelser

Forslaget fastsætter nogle væsentlige krav[9] til produkter med digitale elementer, for at de må gøres tilgængelige på markedet i EU:

a) krav til design, udvikling og produktion og forpligtelser for producenter, udviklere, importører og distributører med hensyn til cybersikkerhed;
b) krav til de processer for håndtering af sårbarheder, som producenter skal indføre for at sikre cybersikkerheden i produktets livscyklus; og
c) regler om markedsovervågning og håndhævelse.

Forslaget finder anvendelse på produkter med digitale elementer hvis anvendelse omfatter en dataforbindelse til en anden enhed eller et netværk. Software er omfattet, også når det ikke indgår i et fysisk produkt. Tjenester er som udgangspunkt ikke omfattet, men fjerndatabehandling[10] (fx cloudløsninger) er inkluderet, hvis de udgør en del af et omfattet produkt.

Forslaget etablerer specifikke procedurer for at foretage vurderinger af, om 'kritiske produkter' lever op til reglerne. Kritiske produkter er fx antivirusprogrammer. Kritiske produkter inddeles i klasse I og II, alt efter hvor kritiske de er for cybersikkerheden. Klasse II anses som de mest kritiske og omfatter bl.a. operativsystemer og firewalls til industriel brug. Produkterne klassificeres efter produktets betydning for cybersikkerheden generelt, samt hvorvidt produktet indgår i kritiske sammenhænge, som fx de samfundskritiske sektorer efter NIS-direktivet.

Kapitel II: Forpligtigelser for økonomiske aktører

Forslaget indeholder krav og forpligtelser for producenter, importører og distributører, som er tilpasset i forhold til deres rolle og ansvar i forsyningskæden. Produkter må kun gøres tilgængelige på markedet, hvis de opfylder de væsentlige cybersikkerhedskrav, der er fastsat i forordningen, forudsat

[9] "essential requirements", jf. bilag 1 til forordningen.
[10] Defineret som: enhver databehandling på afstand, som softwaren er designet og udviklet til af fabrikanten eller under fabrikantens ansvar, hvis fravær ville forhindre produktet med digitale elementer i at udføre en af sine funktioner

at de er korrekt leveret, installeret og vedligeholdt og anvendes til det tilsigtede formål eller på måder, som med rimelighed kan forudses.

Ifølge de 'væsentlige krav' skal producenterne tage højde for og udvise den fornødne omhu i forhold til cybersikkerhed i forbindelse med design, udvikling og produktion af produkter med digitale elementer. Producenterne skal også sørge for sikkerhedsinformation til kunder og for sikkerhedssupport (fx software-opdateringer) på en hensigtsmæssig måde samt opfylde krav til håndtering af sårbarheder.

Forslaget stiller også forpligtelser til producenter om rapportering til EU's cybersikkerhedsagentur (ENISA) vedr. kendskab til aktivt udnyttede sårbarheder eller hændelser, der indvirker sikkerheden i produkter med digitale elementer. Rapportering skal ske senest 24 timer efter kendskab, hvorefter ENISA videresender rapporteringen til relevante CSIRT'er[11]. Forbrugere af produktet med digitale elementer skal ligeledes underrettes om hændelsen, herunder også modtage information om mitigerende handlinger de kan foretage

Kapitel III: Overensstemmelse af produkter med digitale elementer

Produkter, som er i overensstemmelse med harmoniserede standarder eller fælles specifikationer, formodes at være i overensstemmelse med de væsentlige krav i forordningen, uden at det kræver certificering af en tredjepart.

Kommissionen kan vedtage fælles specifikationer ved hjælp af gennemførelsesretsakter i tilfælde, hvor:

1. Der ikke findes harmoniserede standarder
2. Disse standarder er utilstrækkelige
3. Standarderne er unødigt forsinkede i standardiseringsproceduren, eller
4. Kommissionens anmodning om udarbejdelse af standarder ikke er blevet imødekommet af de europæiske standardiseringsorganisationer.

Desuden formodes produkter at leve op til reglerne, hvis de er blevet certificeret, eller der er udstedt en EU-overensstemmelseserklæring eller attest i henhold til en europæisk cybersikkerhedscertificeringsordning[12]. Certificeringsordningerne opfylder kun forslagets krav, hvis Kommissionen har taget stilling til det i en gennemførelsesretsakt.

Producenten skal foretage en vurdering af, om produktet og producentens proces for håndtering af sårbarheder er i overensstemmelse med reglerne.

[11] Computer Security Incident Response Team

[12] Jf. Cyber Security Act (CSA), forordning 2019/881/EU om ENISA (EUs Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi.

Producenten skal følge en af de procedurer, der er fastsat i bilag VI. Producenter af kritiske produkter i klasse II skal inddrage en tredjepart i deres overensstemmelsesvurdering, mens produkter i klasse I kan undtages fra dette krav, hvis de anvender harmoniserede standarder.

Kapitel IV: Notifikation af overensstemmelsesvurderingsorganer

Forslaget indeholder en række krav til de nationale myndigheder med ansvar for organer, som kan foretage overensstemmelsesvurderinger; de såkaldte bemyndigede organer[13]. Medlemsstaterne skal udpege en bemyndigende myndighed, som er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering og notifikation af bemyndigede organer samt overvågning af disse.

Kapitel V: Markedsovervågning og håndhævelse

I overensstemmelse med den gældende forordning for markedsovervågning og produktoverensstemmelse[14] skal de nationale markedsovervågningsmyndigheder udføre markedsovervågning i den pågældende medlemsstat. Medlemsstaterne kan vælge at udpege enhver eksisterende eller ny myndighed som markedsovervågningsmyndighed, herunder eksisterende nationale kompetente myndigheder under NIS2 eller udpegede nationale cybersikkerhedscertificeringsmyndigheder efter artikel 58 i Cybersikkerhedsforordningen[15]. Virksomhederne anmodes om at samarbejde fuldt ud med markedsovervågningsmyndighederne og andre kompetente myndigheder.

I tilfælde af manglende efterlevelse kan myndighederne:

1. Kræve, at producenten bringer overtrædelserne til ophør og eliminerer risikoen
2. Forbyde eller begrænse adgangen til markedet for produkt
3. Beordre, at produktet trækkes tilbage fra markedet eller tilbagekaldes fra kunderne.

Myndighederne skal samtidig kunne pålægge virksomheder, der ikke overholder reglerne, sanktioner.

Kapitel VI: Delegerede beføjelser og udvalgsprocedure

For at sikre, at lovgivningen kan tilpasses om nødvendigt, bemyndiges Kommissionen til at vedtage *delegerede retsakter*[16] til:

- opdatering af listen over kritiske produkter i klasse I og II i bilag III og præcisering af definitionerne af disse produkter;

[13] I overensstemmelse afgørelse 768/2008/EF om fælles rammer for markedsføring af produkter.
[14] 2019/1020/EU
[15] Cyber Security Act, forordning 2019/881/EU
[16] Jf. artikel 290 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF)

- præcisering af, om en begrænsning eller udelukkelse er nødvendig for produkter, der er omfattet af anden EU-lovgivning, som stiller krav om samme beskyttelsesniveau som dette forslag;
- tildeling af mandat til certificering af visse meget kritiske produkter med digitale elementer baseret på de kriterier, der er fastsat i forordningen; og
- præcisering af, hvad EU-overensstemmelseserklæringen som minimum skal indeholde, og supplering af de elementer, der skal indgå i den tekniske dokumentation.

Kommissionen tillægges desuden beføjelser til at vedtage *gennemførelsesretsakter* med henblik på at:

- præcisere formatet for eller typen af oplysninger i producenternes forpligtelse om rapportering af sårbarheder og udarbejdelse af en liste over softwarekomponenter, der skal gives informationer om;
- præcisere de europæiske cybersikkerhedscertificeringsordninger, der kan anvendes til at påvise overensstemmelse med forordningens væsentlige krav eller dele heraf;
- vedtage 'fælles specifikationer' i tilfælde af manglende standarder;
- fastsætte tekniske specifikationer for CE-mærkningen; og
- vedtage korrigerende eller restriktive foranstaltninger på EU-plan under ekstraordinære omstændigheder, der berettiger et hurtigt indgreb for at bevare et velfungerende indre marked.

Kapitel VII: Fortrolighed og sanktioner

Forslaget pålægger alle parter tavshedspligt omkring oplysninger og data, der indhentes under udførelsen af deres opgaver og arbejde omfattet af forordningen.

For at sikre en effektiv håndhævelse fastsætter forslaget, at markedsovervågningsmyndigheder skal have beføjelse til at pålægge eller anmode om, at de nationale domstole pålægger bøder for overtrædelse af reglerne i forordningen. er. På samme måde fastsætter forordningen maksimumsniveauer for bøder.

Producenter kan således straffes med bøde, hvis de ikke opfylder forordningens væsentlige cybersikkerhedskrav og forpligtelserne i artikel 10 (producentens forpligtelser) og 11 (rapporteringsforpligtelser). Bøderne kan være på op til ca. 112 millioner danske kroner eller 2,5 procent af en virksomheds samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst. Tilsvarende kan manglende overholdelse af andre forpligtelser straffes med bøde på op til ca. 75 millioner danske kroner eller op til 2 procent af den samlede globale årsomsætning. Ukorrekte, ufuldstændige eller vildledende oplysninger til bemyndigede organer og markedsovervågningsmyndigheder som svar på en anmodning

kan straffes med bøder på op til ca. 37 millioner danske kroner eller op til 1 procent af den samlede globale årsomsætning.

I forslaget er der indsat mulighed for, at medlemsstaterne kan beslutte, om og i hvilket omfang offentlige myndigheder skal kunne pålægges bøder.

Kapitel VIII: Transition og afsluttende bestemmelser
Forordningen vil finde anvendelse 24 måneder efter dens ikrafttrædelse, med undtagelse af rapporteringspligten for producenter (artikel 11), som ville gælde fra 12 måneder efter datoen for ikrafttrædelse.

4. Europa-Parlamentets udtalelser

I Europa-Parlamentet har udvalget for industri, transport, forskning og energi (ITRE) hovedansvaret for forslagets behandling. Der er på nuværende tidspunkt ikke udarbejdet en holdning til forslaget.

5. Nærhedsprincippet

Kommissionen vurderer, at forslaget er i overensstemmelse med nærhedsprincippet.

Det er Kommissionens opfattelse, at den generelle grænseoverskridende karakter af cybersikkerhed, de stigende risici og antallet af sikkerhedshændelser, som har afsmittende virkninger på tværs af grænser, sektorer og produkter, betyder, at målene for dette forslag ikke effektivt kan nås af medlemsstaterne alene. Kommissionen vurderer desuden, at nationale tilgange til at løse problemerne, og især tilgange, der indfører obligatoriske krav, vil skabe yderligere juridisk usikkerhed og barrierer på det indre marked. Således mener Kommissionen, at handling på EU-plan er nødvendig for at sikre en høj grad af tillid blandt brugerne. Endelig påpeger Kommissionen, at forslaget også vil gavne det digitale indre marked og det indre marked generelt ved at give retssikkerhed og lige vilkår for producenter af produkter med digitale elementer.

Regeringen er samlet set enig i Kommissionens vurdering af, at forslaget er i overensstemmelse med nærhedsprincippet.

6. Gældende dansk ret

Gældende dansk produktlovgivning indeholder ikke regler, der direkte regulerer cybersikkerhed. Det er på nuværende tidspunkt ikke klart, hvorledes forslaget er relateret til lovgivning såsom Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester[17], samt

[17] Lov nr. 436 af 08/05/2018, der implementerer EU direktiv (EU) 2016/1148 (NIS)

GDPR[18]. Produktloven[19] indeholder generelle regler om, hvilke krav mange produkter skal leve op til, før de gøres tilgængeligt på markedet. Hertil kommer regler i mere sektorspecifik produktlovgivning. Reglerne fra dette forslag vil supplere disse.

7. Konsekvenser

Lovgivningsmæssige konsekvenser
En ny forordning om horisontale krav til cybersikkerheden i produkter med digitale elementer vil være direkte gældende i dansk ret. En vedtagelse af forslaget kan, afhængigt af hvilke(n) myndighed(er) der får ansvaret for reglerne, medføre behov for tilpasning af bestemmelser om kontrolbeføjelser og sanktioner i eksisterende dansk lovgivning, som fx Produktloven[19]. Det er endnu ikke besluttet, hvordan forslaget skal implementeres, og hvordan myndighedsopgaverne skal fordeles.

Økonomiske konsekvenser

Statsfinansielle konsekvenser
Det forventes, at forslaget vil få statsfinansielle konsekvenser. Omkostningerne kan omfatte:
1. oprettelse af nye myndigheder eller nye opgaver til eksisterende myndigheder;
2. kendskab til og oplæring i de nye krav til eksisterende eller nye myndigheder, og
3. tilsyn og håndhævelse af de nye krav, herunder løbende som en del af livscyklustilgangen.

På sigt kan der opstå omkostningsbesparelser takket være en horisontal tilgang til cybersikkerhedskrav, så der fx ikke skal håndhæves efter flere regelsæt parallelt for forskellige produkttyper eller sektorer. Det er under forudsætning af, at der opereres med et begrænset antal standarder, der udmønter de konkrete cybersikkerhedskrav.

Der kan ligeledes være løbende omkostninger i form af yderligere tilsyn og håndhævelse af de nye krav, såfremt offentlige produkter eller tjenester, der indgår i, anvendes af eller eksisterer i konkurrence med produkter fra kommercielle aktører, er omfattet.

Kommissionen estimerer i sin konsekvensanalyse, at de sammenlagte årlige meromkostninger for tilsynsmyndighederne, vil beløbe sig til ca. 57

[18] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)
[19] Lov nr. 799 af 9. juni 2020

milliarder danske kroner i hele EU. Det bemærkes, at afledte nationale udgifter som følge af EU-retsakter afholdes inden for de berørte ministeriers eksisterende bevillingsramme, jf. budgetvejledningens bestemmelser herom.

Samfundsøkonomiske konsekvenser
Forslaget vurderes at kunne få både positive og negative samfundsøkonomiske konsekvenser.

Det vurderes, at kravene vil være med til at løfte cybersikkerhedsniveauet for produkter på det indre marked. Dette vil kunne medføre en reduktion af cybersikkerhedshændelser og cyberkriminalitet, og dermed løfte cybersikkerhedsniveauet på tværs af EU, herunder i Danmark. Det vil have positive økonomiske konsekvenser og tillige øge beskyttelsen af fundamentale rettigheder, særligt for privatlivs- og persondatabeskyttelsen. Forslaget vil bidrage til at myndigheder, virksomheder og borgere er bedre beskyttet i cyberspace.

Omvendt kan forslaget få negative samfundsøkonomiske konsekvenser, såfremt de nye krav og forpligtelser for producenterne skaber uhensigtsmæssige omkostninger, fx i form af høje certifikationsomkostninger, overlap af forskellige standarder eller lange produktgodkendelsesprocesser. Det vil især have betydning for SMV'er og iværksættervirksomheder og kan i sidste ende påvirke udbuddet og prisen på de omfattede produkter.

Erhvervsøkonomiske konsekvenser
Det forventes, at forslaget vil medføre økonomiske og administrative konsekvenser for dansk erhvervsliv. Særligt må det forventes, at de nye produktkrav vil medføre øgede udgifter til design og produktion, samt løbende vedligeholdelse og opdateringer som følge af livscyklustilgangen. Ligeledes forventes krav til rapportering, uddybende brugerinformation og særligt certificering at bidrage til omkostninger.

Kommissionen estimerer i konsekvensanalysen, at de samlede omkostninger for overholdelse forventes at blive op til ca. 216 mia. danske kroner for alle softwareudviklere og hardwareproducenter i EU. Kommissionen skønner, at forslaget hovedsageligt vil betyde øgede omkostninger for virksomheder, herunder producenter, distributører og importører, til produktudvikling gennem hele livscyklussen, informationsmateriale til slutbrugere, overensstemmelsesvurderinger og rapporteringsforpligtelser.

Således estimerer Kommissionen, at udgifter til produktudvikling vil stige med godt 30,5 procent. Det anslås dog, at ca. 50 procent af producenterne allerede lever op til minimumskravene og derfor vil opleve mindre eller ingen merudgifter. Udgifter til dokumentation og rapportering forventes at

stige med ca. 9 procent. De overensstemmelsesvurderinger, som producenterne selv skal foretage, forventes at koste ca. 137.000 danske kroner for det gennemsnitlige produkt med et digitalt element, og tredjepartsvurderinger for kritiske produkter ca. 186.000 danske kroner. Sidstnævnte vil ifølge Kommissionens vurdering alene udgøre ca. 10 procent af alle omfattede produkter.

Omvendt skønnes det også, at erhvervslivet vil nyde godt af et højere cybersikkerhedsniveau med færre sikkerhedshændelser og dertil hørende tab af omsætning og omdømme. I Kommissionens konsekvensanalyse anslås det, at forordningen kan reducere cybersikkerhedshændelser med 20-30 procent, hvilket svarer til ca. 1-2 milliarder danske kroner i årlige tab. Ligeledes forventes horisontale regler på tværs af EU at lette visse byrder, som følge af anden lovgivning, herunder fx NIS2. Desuden kan det være med til at lette adgangen til det indre marked og udjævne konkurrencefordele mellem store og små virksomheder. Det skyldes bl.a., at det på nuværende tidspunkt i højere grad er store virksomheder, som har råd og mulighed for at sikre sig mod og modvirke skader fra cybersikkerhedshændelser.

Med afsæt i Kommissionens estimater har Erhvervsstyrelsen udført en indledende estimering af de forventede administrative omkostninger for danske producenter af produkter med digitale elementer. Erhvervsstyrelsens foreløbige skøn er, at forslaget vil medføre administrative omstillingsomkostninger på ca. 1 milliarder danske kroner og løbende administrative omkostninger på ca. 175 millioner danske kroner om året. Beregningen skal dog tages med flere betydelige forbehold. For det første er de estimerede omkostninger baseret på en antagelse om, at danske virksomheder vil afholde samme omkostninger til at efterleve reglerne som andre europæiske virksomheder. Dernæst antages det i Kommissionens beregninger, som Erhvervsstyrelsens skøn bygger på, at enhver omfattet producent vil lancere ét produkt med digitale elementer årligt, hvilket formentlig resulterer i en underestimering af de forventede administrative omkostninger. Afslutningsvis omfatter beregningerne ikke distributører og importører, som også kan forventes at opleve øgede administrative omkostninger.

Andre konsekvenser og beskyttelsesniveauet

Det forventes, at forslaget vil øge cybersikkerheden i Danmark, til gavn for både virksomheder og forbrugere, men også for den nationale sikkerhed De horisontale cybersikkerhedskrav forventes at mindske antallet af sårbarheder og angrebsflader, og dermed også mindske antallet af hændelser i produkter med digitale elementer, der placeres på det indre marked, igennem hele deres livscyklus. Cybersikkerhedslovgivning der sætter krav til alle produkter med digitale elementer vil derfor bidrage til at myndigheder, virksomheder og borgere er bedre beskyttet i cyberspace.

Forslaget forventes derudover at forbedre beskyttelsen af grundlæggende rettigheder og friheder såsom privatlivets fred, beskyttelse af personoplysninger eller personlig værdighed og integritet. Således forventes det, at horisontale cybersikkerhedskrav vil bidrage til sikkerheden af personoplysninger ved at beskytte fortroligheden, integriteten og tilgængeligheden af oplysninger i produkter med digitale elementer.

8. Høring

Forslaget har været sendt i høring i EU-specialudvalget for konkurrenceevne, vækst og forbrugerspørgsmål med frist for bemærkninger den 14. oktober 2022. Der er indkommet høringssvar fra Dansk Erhverv, Dansk Industri, Landbrug & Fødevarer, Forsikring & Pension, Finans Danmark og Forbrugerrådet Tænk.

Generelle bemærkninger

Dansk Erhverv (DE) støtter som udgangspunkt fælleseuropæiske tiltag, der sikrer høje standarder for kvalitet i europæiske produkter, hvilket er med til at øge efterspørgslen på europæiske produkter og skabe en konkurrencefordel. Dog ser DE også, at de ekstra omkostninger forbundet med sikkerhedskravene kan få priserne på europæiske digitale produkter til at stige i et omfang, der skader mulighederne for at eksportere udenfor EU.

Dansk Industri (DI) ser behovet for at styrke cybersikkerheden af produkter, og bakker op om horisontal lovgivning baseret på Ny Metode principperne, som er kendt for virksomhederne. DI sætter pris på, at Kommissionen med sit forslag i høj grad har lyttet til industriens ønsker, og er derfor overordnet positivt stemt overfor forslaget. Samtidig ses behov for at tilpasse forslaget, så det bliver mere klart, hvad, hvilke virksomheder skal, hvornår og hvordan. DI pointerer, at forslaget vil kræve meget af virksomhederne, der f.eks. som noget nyt, skal forholde sig til livcyklusperspektivet, og software som et selvstændigt produkt.

DI sætter endvidere pris på, at forslaget forholder sig til det kludetæppe af lovforslag, der regulerer produkters cybersikkerhed, og tillægger det stor betydning, at det samme produkt kun omfattes af et regelsæt ift. cybersikkerhed. Samtidig ses det, at den løsning, som forslaget opstiller, er kompliceret og sårbar i forhold til ændringer, der kan ske under forhandling af denne og anden lovgivning. DI opfordrer derfor regeringen til at have fokus på, at intentionen om én lovgivning opretholdes under forhandlingerne. DI er særligt glade for, at forslaget lægger op til, at den delegerede retsakt under radioudstyrsdirektivet kan trækkes tilbage, når forordningen finder anvendelse.

Landbrug & Fødevarer (L&F) bemærker, at forslaget har stor opmærksomhed i fødevareklyngen og agroindustrien. Man anser det overordnet for positivt at rydde op i kludetæppet af regler på cyberområdet og forhåbentligt dække nogle lovgivningshuller til anden lovgivning såsom maskindirektivet[20] og radioudstyrsdirektivet[21]. Yderligere fleksibilitet ift. imødekommelse af en mulig implementeringsfrist i 2026 efterlyses for at reducere industriens udgifter ikke mindst i brancher med mindre produktvolumen som fx agroindustrien.

Forsikring & Pension (F&P) glæder sig over ambitionen om at hæve niveauet af cybersikkerhed i EU via nye fælles cybersikkerhedsstandarder, der ses som et vigtigt skridt i den rigtige retning. F&P påpeger dog, at forsikringsbranchens brug af digitale produkter vil blive styret af DORA[22], og at sektoren derfor ikke bør være omfattet af forordningens krav. Af hensyn til de mange EU-lovgivningsinitiativer på området, mener F&P, at det er vigtigt, at der sikres en ensartethed i retsakterne, særligt ift. begrebsdefinitioner og anvendelsen af disse. F&P påpeger, at forsikringsbranchen helt konkret bidrager til sikkerheden i digitale produkter ved at tilbyde forsikringsdækning. Det er dog en forudsætning, at brugeren/virksomheden kan påvise, at vedkommende har sikret de digitale produkter. Det er desuden vigtigt, at brugeren har iværksat en række tiltag, så risiko for cyberangreb reduceres.

Finans Danmark (FIDA) ser positivt på ambitionerne i forslaget. FIDA ser et stigende behov for at udbrede kravene til beskyttelse af stadigt mere netværksforbundne miljøer mod cybersikkerhedshændelser, og særligt på de områder, der involverer hele forsyningskæder. Det anses som nødvendigt, at der etableres konkrete implementeringsforventninger for it-sikkerheden for de produkter – og indlejrede systemer – der introduceres på markedet af hardwarefabrikanter, softwareudviklere, distributører og importører (fra tredjelande). Ambitionen med forordningen, både politisk og økonomisk, bør ifølge FIDA være at realisere et "globalt benchmark" på dette område.

Forbrugerrådet Tænk (TÆNK) ser overordnet meget positivt på forslaget, der kan være med til at sikre, at produkter med digitale elementer, som forbrugere køber, har et højt niveau af sikkerhed. Dog ses der også problematiske aspekter af forslaget, herunder produkters levetid og risikoklassificeringen samt forbrugeres klageadgang. TÆNK mener, at disse aspekter bør søges ændret, så forbrugernes retsstilling sikres og forbrugertilliden til produkter med digitale elementer ikke risikerer at blive forringet.

---

[20] Forslag til forordning om maskinprodukter, 2021/0105(COD)
[21] Direktiv 2014/53/EU
[22] Digital Operational Resilience Act, 2020/0266(COD)

Specifikke bemærkninger

Anvendelsesområde
DE er betænkelige ved at omfatte så mange meget forskellige produkttyper, bl.a. af hensyn til de begrænsede erfaringer med CE-mærkning af software, og finder det ikke helt klart, hvad der er inkluderet – særligt ift. Software-as-a-Service (SaaS). Derfor mener DE, at det bør overvejes at begrænse forslagets anvendelsesområde til IoT-enheder i første omgang, eller som minimum gøre lovteksten mere klar ift. de forskellige typer af digitale produkter, der findes på markedet.

DI påpeger, at forslaget etablerer en ny kategori af produkter med digitale elementer, der ikke tidligere har været defineret, hvorfor det er vigtigt at forholde sig til, hvad definitionerne dækker over, og hvordan de spiller sammen. DI ser også, at anvendelsesområdet er meget bredt, men anerkender vigtigheden af at regulere software og produkter gennem hele deres livscyklus. Dette skal dog ifølge DI tilpasses Ny Metode bedst muligt. DI sætter pris på, at forslaget undtager software som tjenesteydelse, hvilket man mener ville have gjort det umuligt at udvikle de nødvendige underliggende harmoniserede standarder, indenfor rimelig tid. Samtidig er DI enige i Kommissionen vurdering af, at kravene i NIS2 tager højde for de største udfordringer, når det gælder tjenesteydelser.

Definitioner
F&P finder det væsentligt, at definitionerne af nøglebegreber er de samme på tværs af den europæiske lovgivning. F.eks. introduceres med AI forordningen begreber såsom "*developer*", "*deployer*", "*user*", "*operator*" og "*provider*", som også har betydning i relation til forslaget, hvorfor brugen af begreberne må strømlines på tværs af retsakterne for at undgå unødig kompleksitet og modsætninger i den samlede lovgivning.

DE mener, at det skal sikres, at der ikke er forskelle i definitionerne mellem de forskellige reguleringer, herunder de definitioner af "produkter", "software", "IoT" mv., der blandt andet findes i produktsikkerhedslovgivningen (NLF samt GPSR), produktansvarslovgivningen (den kommende revision af produktansvarsdirektivet) samt IPR-lovgivningen.

Økonomiske aktørers forpligtelser
TÆNK henviser til, at forslaget tidsbegrænser en fabrikants forpligtelserne til et produkts levetid eller i op til 5 år, afhængigt af hvad der er kortest. Det påpeges, at en lang række produkter med digitale elementer, som fx nyere vaskemaskiner, har en levetid på mere end 5 år. Man ser det som uhensigtsmæssigt og ude af trit med den grønne omstilling, at brugere risikere efter 5 år ikke længere at have et sikkert produkt. TÆNK foreslår, at

ordlyden ændres, så fabrikanter forpligtes til at sikre produkter (inkl. sikkerhedsopdateringer) i hele deres levetid og mindst 5 år – afhængigt af, hvad det længst. Endvidere mener man, at det skal sikres, at sikkerhedsopdateringerne er forståelige og brugervenlige, da målet med forslaget ellers ikke vil blive opnået i praksis.

Produktkrav

DE mener, at listen med krav til digitale produkter er for generisk formuleret (fx "*secure by default configuration*") og i høj grad åben for fortolkning. Man ser det for mere hensigtsmæssigt at formulere mere konkrete krav til forskellige produkttyper. Ligeledes bør kravet om sikringen i hele produktets *livscyklus* konkretiseres, da forskellige typer af digitale produkter har forskellig levetid, og krav til fx tilgængelighed af sikkerhedsopdateringer og support således afhænger af produkttypen. DE er også bekymrede for konsekvenserne af forslagets krav, særligt for SMV'er og startups, hvor det er vigtigt, at kunne udvikle og afprøve et produkt i tidligt stadie for se, om det er kommercielt bæredygtigt. Ekstra omkostninger i den indledende udvikling og eventuelle ventetider for at få produkter godkendt kan være en barriere for innovation og iværksætteri, og bør derfor adresseres i lovbehandlingen.

DI finder det positivt, at forslaget definerer et fælles minimumsniveau for produkters cybersikkerhed, der kan bygges oven på med speciallovgivning. Desuden er det positivt, at kravene bygger på og supplerer krav, der bliver gældende under den delegerede retsakt under radioudstyrsdirektivet, som vil gøre det lettere at implementere reglerne i virksomhederne. Ligeledes ses produktkravene som udgangspunkt relevante, dog med behov for præciseringer. Størst udfordringer ser DI's medlemmer umiddelbart ift. kravene i bilag I, del 1, pkt. 2 og 3e. De er positive over for "*dataminimering*" (pkt. 3e), men i tvivl om, hvad kravet betyder i praksis i forhold til, hvem der skal gøre hvad. Samtidig bør kravet sammentænkes med kravene til datadeling i dataforordningen. Når det gælder kravet om kun at levere produkter uden "*udnyttelige sårbarheder*" (pkt. 2) hæfter de sig ved, at det ikke er muligt i praksis, hvis man løbende skal beholde sine produkter på markedet. Det tager tid at udvikle de opdateringer, der skal til, når der f.eks. identificeres sårbarheder i software. For at vide om kravene fungerer i praksis er der behov for udvikling af "use cases" både generelt, og for software i særdeleshed.

DI bakker op om proceskrav ved håndtering af sårbarheder (bilag I, del 2), hvor der dog bør tages højde for de risici, der er forbundet med at informere om sårbarheder (hackerangreb), så f.eks. bør krav om information "*uden ophold*" modificeres. Offentliggørelse af hvordan sårbarheder er blevet håndteret anses desuden som en konkurrenceparameter, der kan blive kompromitteret. I relation til Ny Metode ser DI også behov for præcisering af,

hvordan livscykluskravene håndhæves, da det er nyt i en produktsammenhæng. Desuden kræver efterlevelse af kravene, at man holder sig orienteret om sårbarheder, hvorfor DI mener, at dette måske også burde være et krav. Også når det gælder krav om information og brugsvejledning (bilag II) er der brug for præciseringer og "use cases", ligesom der er behov for et eftersyn i forhold til Ny Metode-principperne. Samtidig bør det sikres, at "software bill of materials" beskyttes mod misbrug, og den bør som udgangspunkt sidestilles med teknisk dokumentation i anden produktlovgivning, og kun udleveres på foranledning af markedsovervågningsmyndigheden.

Endelig er DI enig i, at notifikationer kan være relevante, men er samtidig optaget af, at de bliver rimelige og udviklet på en sådan måde, at de også tager højde for de notifikationer, der skal foretages i henhold til NIS2. Det hænger sammen med, at mange af de samme produkter også reguleres på "enheds" niveau under NIS2. Som det ser ud i forslaget skal notifikationerne foretages til forskellige aktører med forskellige tidsfrister. DI stiller desuden spørgsmålstegn ved, om ENISA vil være den rette til at varetage opgaven vedrørende produkterne, når det ikke er tilfældet for "enhederne" under NIS2.

FIDA anfører, at der skal skabes gennemsigtighed for, at et digitalt produkt overholder et fastlagt cybersikkerhedsniveau. Dette vil stille krav til udformning af formelle/standardiserede produktblade for hvert digitalt produkt eller tjeneste. FIDA mener, at det som minimum bør beskrive de foranstaltninger, der skal være implementeret for at bidrage til et tilfredsstillende og sammenligneligt niveau af cyberrobusthed.

Standarder, certificering og produktkategorisering

DE mener, at Kommissionens mulighed for at anvende delegerede retsakter til at udvide listen i bilag III, skaber unødvendig usikkerhed for fabrikanter af digitale produkter, og at de omfattede produktkategorier derfor bør bestemmes endeligt i selve lovbehandlingen.

DI finder det positivt, at Kommissionen bakker op om brug af modul A (selvevaluering) ved overensstemmelsesvurdering, der vil sikre mere kapacitet hos 3. partscertificeringsudbydere til de virksomheder, der ikke har den fornødne modenhed til at foretage vurderingerne selv. Man har dog svært ved at gennemskue, hvorfor specifikke produkter er kategoriseret som kritiske, og de kriterier, der ligger bag. DI bemærker, at betingelserne i artikel 6 er meget forskelligartede og giver anledning til et stort manøvrerum for Kommissionen. DI så gerne, at betingelserne blev skærpet, og det blev tydeligere hvordan den risikobaserede tilgang er tænkt.

DI ser med bekymring på, at produktkategorierne først skal defineres et år efter, forordningen træder i kraft, og et år før den finder anvendelse. DI opfordrer til en proces, der minder om den, man har haft ved forhandling af maskinforordningen, hvor listerne med kritiske produkter som udgangspunkt er så korte som muligt, og løbende kan udvikles hvis det er nødvendigt ud fra mere restriktive krav. DI er fx uforstående overfor, hvorfor IoT-industriapplikationer altid er kritiske. Ofte har fabrikanten ikke et overblik over, hvor deres produkter ender, og det samme produkt kan have både privat og industriel anvendelse. DI stiller også spørgsmålstegn ved, at robotter betegnes som kritiske i kategori II. Endelig ses der behov for præciseringer, fx af at kategoriseringen kun relaterer sig til cybersikkerhedsrisici i forbindelse med overvågningsudstyr. Det samme gør sig gældende for produkter, der består af komponenter, der tilhører en højere kategori end slutproduktet.

DI er tillige bekymrede over de mulige konsekvenser af, at hhv. harmoniserede standarder, tekniske specifikationer og certificeringsordninger under ENISA, sidestilles. Dette kan underminere tilliden til det etablerede standardiseringssystem og medføre udvikling af tekniske specifikationer i ikke transparente, ikke inklusive, og ikke demokratiske processer, og risikerer at resultere i standarder, der ikke tager højde for international state-of-the art. DI finder derfor, at Kommissionens mulighed fro at udvikle tekniske specifikationer bør begrænses mest muligt, og der bør stilles proceskrav hertil, ligesom der bør tages stilling til, hvilke typer af forsinkelser i standardiseringssystemet, der kan begrunde udvikling af tekniske specifikationer. DI opfordrer regeringen til at lægge pres på Kommissionen i forhold til at udvikle principper for tekniske specifikationer, der ensrettes på tværs af lovområder, der tager ovenstående i betragtning. Parallelt hermed ser DI, at der bør arbejdes på at forbedre transparens og inklusion ved udvikling af certificeringsordninger under ENISA.
DI har også bekymringer i forhold til, om det er muligt, at nå at udvikle de nødvendige standarder i forhold til, hvornår loven finder anvendelse, og opfordrer til, at man allerede nu igangsætter arbejde, der forholder sig til hvordan et mandat, der sikrer hurtigst mulig udvikling af standarder, kunne skrues sammen.

FIDA fremfører, at der skal skabes de nødvendige standardiserede vurderingskriterier og effektiviteten af de implementerede sikkerhedsforanstaltninger. FIDA ser, at sådanne vurderinger skal fastlægges i forhold til den enkelte produktkategori.

TÆNK finder det uhensigtsmæssigt, at nogle af de produkter, der fremgår af bilag III, klasse II, som særligt kritiske, er gjort industrispecifikke – fx firewalls, routers, modems m.fl. Man henviser til, at mange cybersikkerhedsproblemer ved sådanne produkter også gør sig gældende ved privat

brug, hvorfor de også bør underkastes 3. partsevaluering af cybersikkerhedselementerne, når det bruges privat. Specifikt foreslår TÆNK, at ordet "*industrial*" slettes fra klasse I og II, og der i klasse II (15) tilføjes "*and smart home devices*".

FIDA påpeger, at en overvejende del af digitale forbrugerprodukter i dag fremstilles uden for EU. Således ser FIDA mulighed for at øge ambitionsniveauet og gøre forordningen mere virkningsfuld, ved at stille krav om, at alle leverandører, også leverandører fra tredjelande, som ikke kan dokumentere, at de opfylder EU's minimumskrav for den pågældende produktkategori, ikke kan få tilladelse til at sælge deres produkter i denne kategori i EU.

Tilsyn, håndhævelse, og sanktioner

DI finder det positivt, at forslaget lægger op til, at cybersikkerhed skal falde ind under markedsovervågningsforordningen. Samtidig hæfter DI sig ved de potentielt væsentligt højere bødestørrelser, og sætter spørgsmålstegn ved rimeligheden, særligt når det gælder krav, der ikke direkte relaterer sig til cybersikkerhed. Ydermere påpeger DI, at mange af produkterne er integreret i vigtige og væsentlige enheder under NIS2, så de også kan sanktioneres i den sammenhæng. Det bør sikres, at man ikke kan pålægges flere sanktioner for samme forseelse.

DI ser, at der, hvis intentionerne i forslaget skal kunne gennemføres i praksis, er behov for kapacitets-opbygning hos markedsovervågningsmyndighederne og de bemyndigede organer. DI opfordrer derfor de relevante myndigheder til at bidrage til arbejdet med udvikling af standarder under radioudstyrsdirektivet og stillingtagen til kommende mandat for standarder under dette lovforslag. Samtidig er det vigtigt at udvikle en model, hvor håndhævelse af NIS2 og produktlovgivningen spiller sammen, så de eksisterende ressourcer udnyttes bedst muligt, og der sikres størst mulig kvalitet i arbejdet.

TÆNK savner et krav om, at virksomheder, der bringer produkter med digitale elementer på markedet, skal forpligtes til at have effektive og fyldestgørende interne klagehåndteringsmekanismer. Forbrugere skal således sikres mulighed for at klage over et produkt, sideløbende med at markedsovervågningsmyndigheden fører tilsyn med produkterne, ligesom forbrugerne skal have adgang til at klage over den beslutning, som myndigheden har truffet. Sådanne klagesager skal tillige kunne efterprøves ved administrative organer og domstole.

9. Generelle forventninger til andre landes holdninger

Forslaget har alene været igennem første artikelgennemlæsning i Rådets horisontale arbejdsgruppe for cyber. Således er der indtil nu fortrinsvist

stillet tekniske spørgsmål til teksten. Samtlige lande har fortsat undersøgelsesforbehold og ikke givet officielle holdninger tilkende.

Forslaget er dog generelt blevet velmodtaget i Rådet, men der er også en række spørgsmål til bl.a. anvendelsesområdet, samspillet med anden lovgivning samt det mandat EU's cybersikkerhedsagentur ENISA tildeles med reguleringen.

Danmark har sammen med Nederlandene og Tyskland fremsendt et non-papir den 12. september (inden forslagets fremsættelse), med fokus på at sikre et bredt anvendelsesområde, og sammenhæng til anden lovgivning, herunder ved at bruge Ny Metode og sammenhængende standardisering på tværs af produktgrupper.

10. Regeringens generelle holdning

Regeringen ser overordnet positivt på forslaget om at skabe et minimumsniveau for cybersikkerhed i produkter med digitale elementer og software via horisontal EU-lovgivning. Regeringen er enig med Kommissionen i, at der i høj grad er brug for sådanne regler for at imødegå cybertruslen.

Regeringen hilser ligeledes det høje ambitionsniveau velkommen, om end man dog gerne så, at anvendelsesområdet blev klarere og endnu bredere. Således så regeringen gerne, at digitale processer og kommercielle tjenester var omfattet i forslaget, da sårbarheder i forhold til cybersikkerhed i højere og højere grad udnyttes gennem disse, men også for at forslaget kan omfavne udviklingen på området, og dermed bliver fremstidssikkert.

Regeringen synes, at reglerne bør finde en passende balance mellem et højt beskyttelsesniveau, den digitale udvikling samt omkostninger for erhvervslivet.

Regeringen vil arbejde for, at der stilles balancerede krav ud fra en risikobaseret tilgang, så kravene står mål med de ønskede effekter.

Regeringen finder det vigtigt, at centrale begreber i forslaget afklares. Der er behov for yderligere at præcisere afgrænsningen af produkter, der undtages for forordningens anvendelsesområde, herunder for så vidt angår motorkøretøjer samt offentlige produkter/tjenester, som indgår i, anvendes af eller eksisterer i konkurrence med produkter fra kommercielle aktører. Generelt skal afklaring også bidrage til at konkretisere de økonomiske konsekvenser. Ligeledes mener regeringen, at Kommissionens beføjelser til at udstede delegerede retsakter skal afgrænses.

Regeringen er tilfreds med, at forordningen er bygget op efter Ny Metode, idet der fastsættes væsentlige krav i forordningen, som skal udmøntes teknisk via harmoniserede standarder i samarbejde med industrien. Det er vigtigt, at Kommissionens bemyndigelse til at udstede tekniske specifikationer afgrænses til tilfælde, hvor der ikke er en standard. Det skal samtidigt være tydeligt, at det er en sidste udvej.

Generelt er det vigtigt for regeringen, at lovgivningen fastholder sin horisontale karakter, og at standarderne holdes generelle. De detaljerede sikkerhedskrav bør integreres i et mindre antal standarder på tværs af produkter, eller de samme krav bør som minimum gå igen på tværs af de produktspecifikke standarder. Desuden er det vigtigt, at evt. nye tekniske standarder udvikles i god tid, inden forordningen finder anvendelse.

Regeringen ønsker, at det gøres tydeligere i forordningen, hvad der ligger til grund for udvælgelsen af kritiske produkter. Regeringen ønsker samtidigt at få klargjort omfanget af Kommissionens bemyndigelser til at udarbejde, udbygge og opdatere denne liste og kriterierne herfor. Regeringen er skeptisk over for at den nærmere specificering af listen skal ske igennem fremtidige delegerede retsakter.

Regeringen mener, at der bør sikres sammenhæng og undgås unødvendige overlap mellem gældende og fremtidig regulering, herunder NIS2-direktivet, eIDAS-forordningen, forordningen om kunstig intelligens, maskinforordningen og forordning for det europæiske sundhedsdataområde (EHDS). Det skal samtidig være så klart som muligt,-hvilken lovgivning sikkerheden i et givent produkt eller tjeneste er reguleret under. Der skal samtidig ikke opstå huller eller overlap i beskyttelsen.

Regeringen finder det vigtigt, at forslaget ikke bliver en hindring for en sikker udbredelse af etisk og ansvarlig anvendelse af kunstig intelligens.

Det er også helt centralt for regeringen at bevare forslagets fleksibilitet i forhold til valg af sanktioner, således at medlemsstaterne ikke forpligtes til at indføre administrative bøder.

Endelig er regeringen forbeholden overfor at udvide ENISAs beføjelser, herunder særligt ENISA's kompetencer til tilstrækkeligt at håndtere og videreformidler indrapporteringer fra producenter sikkerhedsmæssigt forsvarligt og effektivt. Regeringen tager derudover også forbehold for Kommissionens kommende forslag til en cyberforsvarsmeddelelse for EU og dennes eventuelle sammenspil med nærværende forslag.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt for Folketingets Europaudvalg.