



## **NOTAT TIL FOLKETINGETS EUROPAUDVALG**

17. november 2022

### **Rådsmøde (transport, telekommunikation, energi) den 5.-6. december 2022**

#### **Indhold**

Europa-Kommissionens forslag til Europa-Parlamentet og Rådets forordning om harmoniserede regler for kunstig intelligens og ændring af visse af Unionens lovgivningsmæssige retsakter (kunstig intelligens forordningen) KOM (2021) 206..... 2

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om harmoniserede regler om fair adgang til og anvendelse af data (dataforordningen) KOM (2022) 68 ..... 39

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 ..... 71

Rådskonklusioner vedr. fremtidssikring af europæisk transport på indre vandveje (NAIADES III)..... 93

## **Europa-Kommissionens forslag til Europa-Parlamentet og Rådets forordning om harmoniserede regler for kunstig intelligens og ændring af visse af Unionens lovgivningsmæssige retsakter (kunstig intelligens forordningen) KOM (2021) 206**

*Notatet er en opdateret version af samlenotat af den 30. maj 2022. Ændringer er markeret med streg i venstre margin.*

### **1. Resumé**

*Formålet med dagsordenspunktet på rådsmødet er at opnå en generel indstilling for forordningsforslaget om harmoniserede regler for kunstig intelligens. Danmark kan bakke op om den generelle indstilling pga. udviklingen i forhandlingerne ang. bl.a. indsnævring af definitionen af kunstig intelligens og klarlægning af højrisikoklassificeringen.*

*Europa-Kommissionen har den 21. april 2021 fremsat et forslag til forordning om harmoniserede regler for kunstig intelligens og ændring af visse af Unionens lovgivningsmæssige retsakter (KOM (2021) 206). Forordningen er den første af sin slags til at fastlægge en juridisk ramme specifikt for kunstig intelligens.*

*Formålet er at sikre et velfungerende indre marked ved at etablere betingelser for udvikling og anvendelse af lovlig, sikker og pålidelig kunstig intelligens i EU. De fælles regler skal samtidig sikre, at kunstig intelligens, i EU respekterer eksisterende lovgivning, grundlæggende rettigheder samt EU's værdier. Samtidig skal reglerne bidrage til juridisk klarhed for at fremme investeringer og innovationsevnen.*

*Forordningen følger en risikobaseret tilgang, hvor graden af forpligtelser følger graden af risici, der er forbundet med den pågældende anvendelse af et kunstig intelligens-system. Forordningen opdeler kunstig intelligens i følgende risikokategorier: 1) Uacceptabel risiko, hvor der er direkte forbud af visse anvendelser, 2) højrisiko, hvor der er specifikke krav forbundet med visse anvendelser, og hvor der påkræves forudgående overensstemmelsesvurderinger samt efterfølgende markedsovervågning, 3) begrænset risiko, hvor der er gennemsigtighedsforpligtelser tilknyttet visse anvendelser af teknologien, samt 4) lav eller minimal risiko, hvor der ikke er specifikke krav, men i stedet er mulighed for at udarbejde frivillige adfærdskodeks til blandt andet at fremme den frivillige efterlevelse af kravene under højrisikokategorien.*

*Forvaltningen og håndhævelsen af forordningen skal hovedsageligt ske i medlemslandene. I forlængelse heraf skal medlemslandene indføre regler*

*om sanktioner ved overtrædelse af forordningen. Derudover nedsættes der et europæisk udvalg for kunstig intelligens, der blandt andet skal bidrage til et effektivt samarbejde på tværs af grænser og ensartet implementering. Forordningen indeholder foranstaltninger til at fremme innovation. Blandt andet fastsættes der en fælles ramme for implementering af reguleringsmæssige sandkasser.*

*Forslaget forventes at have lovgivningsmæssige og væsentlige erhvervsøkonomiske såvel som statsfinansielle konsekvenser. Regeringen er i gang med at undersøge omfanget af de erhvervsøkonomiske og statsfinansielle konsekvenser nærmere.*

*Regeringen støtter overordnet ambitionen om at skabe et velfungerende indre marked for etisk, ansvarlig og sikker kunstig intelligens. Regeringen anser kunstig intelligens som en af de afgørende teknologier til at understøtte EU's konkurrenceevne, velstand, grønne omstilling samt den offentlige forvaltning. Regeringen anerkender imidlertid, at anvendelsen af kunstig intelligens i visse situationer kan indebære en række alvorlige risici. Regeringen støtter, at risiciene forbundet ved kunstig intelligens adresseres i en europæisk lovgivningsramme.*

*Overordnet finder regeringen det vigtigt, at den europæiske lovgivningsramme følger en risikobaseret, teknologineutral og proportionel tilgang, hvor graden af forpligtelser følger graden af mulig skadevirkning. På den baggrund er det nødvendigt med en klar og operationel lovgivningsramme, der sikrer borgernes tillid og øger beskyttelsen i samfundet, uden at dette unødigt hæmmer innovationsevnen eller forringer konkurrenceevnen. Det er derfor centralt at finde den rette balance, hvor risici adresseres, samtidig med at teknologien kan udvikles og anvendes til gavn for samfundet samt understøtte fremtidens arbejdspladser. Regeringen finder det centralt, at centrale begreber i forslaget klarlægges og afgrænses, herunder definitionen af kunstig intelligens samt at der opstilles klare kriterier for, hvilke anvendelser der klassificeres som højrisiko kunstig intelligens. Desuden finder regeringen det centralt, at forordningen ligger inden for rammerne af eksisterende kompetencefordeling, herunder for så vidt angår national sikkerhed, og tager højde for eksisterende lovgivning, herunder GDPR og produktlovgivningen, hvor gevinsterne ved forslaget står mål med administrative og økonomiske omkostninger for virksomheder. Samtidig vil regeringen arbejde for et europæisk tilsyn til at håndtere sager af en vis størrelse eller grænseoverskridende karakter. Derudover fremhæver regeringen vigtigheden af udformningen af frivillige adfærdskodeks, der kan blive et konkurrenceparameter for danske og europæiske virksomheder og på etableringen af initiativer, der kan fremme innovationskraften inden for kunstig intelligens herunder effektive og fleksible rammer for regulatoriske sandkasser.*

| *Sagen forelægges til orientering.*

## 2. **Baggrund**

Europa-Kommissionen ('Kommissionen') har den 21. april 2021 fremlagt et forslag til forordningen om harmoniserede regler for kunstig intelligens og ændring af visse af Unionens lovgivningsmæssige retsakter (KOM (2021) 206). Forslaget er oversendt til Rådet i dansk sprogversion den 7. juni 2021.

Forslaget er en del af en kunstig intelligens pakke bestående af dette forslag til en forordning, revision af den koordinerede plan for kunstig intelligens samt forslag af revision af det eksisterende maskindirektiv.

Pakken kommer som opfølgning på Kommissionens hvidbog om kunstig intelligens, der blev præsenteret den 19. februar 2019.<sup>1</sup> Baggrunden for hvidbogen var Kommissionsformand von der Leyens annoncering af, at der i løbet af de første 100 dage af Kommissionens mandatperiode skulle fastlægges en europæisk tilgang til kunstig intelligens, herunder dens konsekvenser for mennesker og etik.

Som opfølgning på hvidbogen vedtog det Europæiske Råd konklusioner i oktober 2020, hvori der blev lagt vægt på, at EU bør være en global leder inden for udviklingen af sikker, pålidelig og etisk kunstig intelligens. Samtidig opfordrede det Europæiske Råd til, at Kommissionen fremlagde en klar, objektiv definition af højrisiko systemer.

Forud for lanceringen af hvidbogen underskrev 24 medlemslande en ministererklæring vedrørende samarbejde om kunstig intelligens i forbindelse med Digital Day tilbage i 2018<sup>2</sup>, hvorpå Kommissionen som opfølgning præsenterede en strategi for kunstig intelligens den 25. april 2018<sup>3</sup>. Denne fokuserede både på socioøkonomiske aspekter samt en forøgelse af investeringer i forskning, innovation og kapabiliteter inden for kunstig intelligens. Som led i arbejdet etablerede Kommissionen en højniveauekspertgruppe for kunstig intelligens, der i april 2019 præsenterede sine etiske retningslinjer for pålidelig kunstig intelligens.

---

<sup>1</sup> Kommissionens hvidbog om kunstig intelligens: "En europæisk tilgang til ekspertise og tillid" (KOM (2020) 65) fra den 19. februar 2020

<sup>2</sup> <https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence>

<sup>3</sup> Kommissionens meddelelse "Kunstig intelligens for Europa" (KOM (2018) 237) fra den 25. april 2018

Disse omfattede menneskelige aktiviteter og tilsyn udført af mennesker; teknologisk robusthed og sikkerhed; privatlivets fred og datastyring; gennemsigtighed, mangfoldighed, ikkediskrimination og retfærdighed; social og miljømæssig velfærd; samt ansvarlighed. I tillæg hertil offentliggjorde Kommissionen den 8. april 2019 meddelelsen ”Opbygning af tillid til menneskecentreret kunstig intelligens” (KOM (2019) 168), der havde til formål at iværksætte en pilotfase med afprøvning af den praktiske anvendelse af højniveauekspertgruppens etiske retningslinjer. Dette førte til en revision af retningslinjerne på baggrund af modtagen feedback samt udformningen af en konkret evalueringsliste for pålidelig kunstig intelligens.

### **3. Formål og indhold**

Formålet med dagsordenspunktet på rådsmødet er at opnå en generel indstilling for forordningsforslaget. Danmark kan bakke op om den generelle indstilling pga. udviklingen i forhandlingerne angående bl.a. indsnævring af definitionen af kunstig intelligens og klarlægning af højrisikoklassificeringen.

Forordningens overordnede formål er at sikre et velfungerende indre marked ved at etablere betingelserne for udvikling og anvendelse af lovlig, sikker og pålidelig kunstig intelligens i EU.

Dette skal ske gennem fælles regler, der skal sikre, at kunstig intelligens, der bringes i omsætning og anvendes i EU, er sikker og respekterer eksisterende lovgivning, grundlæggende rettigheder samt EU's værdier. Samtidig skal reglerne også være med til at sikre juridisk klarhed for at fremme investeringer og innovationsevnen samt muliggøre effektiv håndhævelse.

#### Afsnit I: Anvendelsesområde og definitioner (artikel 1-4)

Forordningen indfører harmoniserede regler for omsætning, ibrugtagning og anvendelse af kunstig intelligens-systemer i EU.

Reglerne følger en risikobaseret tilgang, hvor graden af forpligtelser følger graden af de risici, der er forbundet med den pågældende anvendelse af kunstig intelligens. Forordningen opdeler kunstig intelligens i følgende risikokategorier: Uacceptabel risiko, højrisiko, begrænset risiko samt lav eller minimal risiko.

På den baggrund fastsætter forordningen regler for:

- Forbud mod anvendelser af kunstig intelligens, der udgør en uacceptabel risiko.
- Specifikke krav for anvendelser af kunstig intelligens, der udgør en høj risiko.

- Gennemsigtighedsforpligtelser for anvendelsen af kunstig intelligenssystemer, der udgør en begrænset risiko. Omfattede systemer af gennemsigtighedsreglerne er beregnet til at interagere med personer, følelsesgenkendelsessystemer og biometriske kategoriseringssystemer, samt systemer, der anvendes til at generere eller manipulere billede-, lyd- eller videoindhold.
- Regler om markedsovervågning – og tilsyn.

Forordningen definerer kunstig intelligens som software, der er udviklet ved hjælp af en eller flere teknikker eller tilgange, eksempelvis maskinlæring eller statistiske metoder, og der ud fra et sæt menneskeligt definerede mål kan generere output såsom indhold, forudsigelser, anbefalinger eller beslutninger, der påvirker de miljøer, som de interagerer med.

For at fremtidssikre definitionen i forhold til fremtidig teknologisk og markedsrettet udvikling har Kommissionen specificeret de førnævnte teknikker og tilgange, der kan anvendes til at udvikle kunstig intelligens, i et bilag til forordningen. Bilaget oplister en række konkrete kunstig intelligens-teknikker, som forordningen omfatter. Det gælder maskinlæring, logiske og vidensbaserede tilgange samt statistiske metoder. Forslaget giver derudover Kommissionen beføjelser til at ændre bilaget via delegerede retsakter.

De harmoniserede regler finder ikke anvendelse på kunstig intelligens, der er udviklet eller udelukkende anvendes til militære formål, eller i forbindelse med offentlige myndigheder i tredjelande eller internationale organisationers brug af kunstig intelligens, hvis denne brug sker inden for rammerne af en aftale om retshåndhævelse og retligt samarbejde med EU eller med en eller flere medlemslande.

#### Afsnit II: Forbudt praksis med hensyn til kunstig intelligens (artikel 5)

Visse anvendelser af kunstig intelligens medfører uacceptable risici for samfundet og individers rettigheder, da de anses for at være i strid med EU's værdier, for eksempelvis ved at krænke grundlæggende rettigheder.

Forordningen fastlægger, at følgende former for anvendelse af kunstig intelligens skal være forbudt:

- anvendelse af subliminale teknikker, dvs. teknikker der formidler et budskab skjult, der rækker ud over den menneskelige bevidsthed og har til hensigt i en væsentlig grad at ændre personens adfærd på en måde, der forårsager eller sandsynligvis vil forårsage fysiske eller psykisk skade.
- udnytte sårbarheder hos en specifik gruppe på baggrund af deres alder eller handicap ved i en væsentlig grad at ændre adfærden hos en person tilhørende denne gruppe på en måde, der forårsager eller sandsynligvis vil forårsage fysiske eller psykisk skade.

- offentlige myndigheders - eller private virksomheders på vegne af offentlige myndigheder - evaluering eller klassificering af troværdigheden af personer baseret på deres sociale adfærd, personlige egenskaber eller personlighedstræk, hvor den sociale bedømmelse vil lede til en skadelig eller ugunstig behandling.
- anvendelse af systemer til biometrisk fjernidentifikation i realtid i det offentlige rum med henblik på retshåndhævelse.

Sidstnævnte kan dog anvendes til visse strengt nødvendige formål såsom ved målrettet eftersøgning af specifikke potentielle ofre for kriminalitet, herunder børn, samt forebyggelse af terrorangreb. Forordningen fastlægger en udtømmende liste over de tilfælde, hvor biometrisk fjernidentifikation i realtid kan anvendes i det offentlige rum. Anvendelsen kræver desuden en forudgående tilladelse udstedt af en judiciel myndighed eller en uafhængighed administrativ myndighed på baggrund af indført national lovgivning. Det står således medlemslandene frit for, om de vil give mulighed for denne anvendelse, og om de vil tillade alle tilfælde på den udtømmende liste eller kun et udsnit heraf.

Grundet retsforbeholdet er Danmark ikke underlagt reglerne i artikel 5 vedrørende systemer til anvendelse for biometrisk fjernidentifikation i realtid.

### Afsnittet III: Højrisiko kunstig intelligens-systemer (artikel 6-51)

#### *Kapitel 1: Klassificering af højrisiko kunstig intelligens-systemer*

Kapitel 1 klassificerer den anvendelse af kunstig intelligens, der anses for at udgøre en høj risiko for samfundet og individers grundlæggende rettigheder. Forordningen identificerer to hovedkategorier for anvendelse af kunstig intelligens, der kan anses for at være højrisiko kunstig intelligens.

Den ene kategori omfatter kunstig intelligens, der er beregnet til at blive anvendt som en sikkerhedskomponent i et produkt eller i sig selv er et produkt omfattet af harmoniseret EU-lovgivning anført i bilag 2, og der er forpligtet til at gennemgå en tredjepartsoverensstemmelsesvurdering. Bilaget omfatter retsakter baseret på den nye lovgivningsmæssige ramme, "New Legislative Framework" (NLF), der blandt andet omfatter maskiner, legetøj, elevatorer, radioudstyr samt medicinsk udstyr. Derudover omfatter bilaget også retsakter, der ikke er baseret på NLF, men derimod den gamle metode, såsom landbrugskøretøjer, skibsudstyr, jernbanesystemet, civil luftfart og biler. Disse retsakter omfattes også af højrisiko kategorien, men underlægges dog ikke direkte kravene for højrisiko. Dette skyldes, at de pågældende retsakter, der er baseret på den gamle metode, ikke indeholder mulighed for, at eksisterende overensstemmelsesprocedurer deri kan omfatte yderligere krav. Det vil enten kræve, at de pågældende retsakter genforhandles og tilpasses NLF, eller at

kravene indføres via fremtidige delegerede eller gennemførelsesretsakter under disse retsakter. Kommissionen lægger op til, at tilpasningen i den kommende tid sker via sidstnævnte.

Den anden kategori er selvstændige kunstig intelligens systemer – uafhængige af et produkt – hvor Kommissionen vurderer, at systemers formål udgør en høj risiko for menneskers sundhed og sikkerhed eller grundlæggende rettigheder.

Den anden kategori er selvstændige kunstig intelligens systemer – uafhængige af et produkt – hvor Kommissionen vurderer, at systemers formål udgør en høj risiko for menneskers sundhed og sikkerhed eller grundlæggende rettigheder. I vurderingen er der blandt andet taget højde for alvorligheden af den mulige skade samt sandsynligheden for, at den mulige skade vil udspille sig. Kommissionen har oplistet disse systemer i bilag 3, der omfatter otte overordnede områder med dertilhørende specificerede anvendelser:

1. Biometrisk identifikation og kategorisering af fysiske personer
  - Systemer beregnet til biometrisk fjernidentifikation i realtid af personer.
2. Forvaltning og drift af kritisk infrastruktur
  - Systemer beregnet som sikkerhedskomponenter i forvaltning og drift af blandt andet forsyning af vand, gas, varme og elektricitet.
3. Uddannelse og erhvervsuddannelse
  - Systemer beregnet til at fastslå personers adgang til eller fordeling på uddannelsesinstitutioner, at evaluere studerende eller at vurdere deltagere i test, der normalt kræves for at få adgang til uddannelsesinstitutioner.
4. Beskæftigelse, forvaltning af arbejdstagere og adgang til selvstændig beskæftigelse
  - Systemer beregnet til rekruttering eller udvælgelse af kandidater eller beregnet til at træffe beslutninger om forfremmelse og afskedigelse, opgavefordeling samt til overvågning og evaluering af personers præstation og adfærd i arbejdsrelaterede kontraktforhold.
5. Adgang til og benyttelse af væsentlige private tjenester og offentlige tjenester og fordele
  - Systemer beregnet til at blive anvendt af eller på vegne af offentlige myndigheder til at vurdere personers berettigelse til offentlige sociale ydelser og tjenester samt at tildele, reducere, annullere eller tilbagekalde sådanne ydelser og tjenester.



- Systemer beregnet til at foretage kreditvurderinger af personer eller at fastslå deres kreditværdighed, med undtagelse af systemer der tages i brug af mindre udbydere til eget brug.
  - Systemer beregnet til at sende eller at prioritere i udsendelsen af beredskabstjenester i nødsituationer, herunder brandslukning og lægehjælp.
6. Retshåndhævelse
- Systemer beregnet til at blive anvendt af retshåndhævende myndigheder med henblik på at foretage individuelle risikovurderinger af personer for at vurdere risikoen for lovovertrædelser, at anvende som polygrafer eller lignende værktøjer til at påvise en persons følelsesmæssige tilstand, at finde deep fakes, at vurdere pålideligheden af bevismateriale, at forudsige strafbare handlinger baseret på profilering, at profilere samt at anvende til kriminalitetsanalyse vedrørende personer.
7. Migrationsstyring, asylforvaltning og grænsekontrol
- Systemer beregnet til at blive anvendt af kompetente offentlige myndigheder med henblik på at anvende som polygrafer eller lignende værktøjer til at påvise en persons følelsesmæssige tilstand samt at vurdere en risiko, herunder en sikkerhedsrisiko, en risiko for irregulær indvandring eller en sundhedsrisiko som udgøres af en person, der har til hensigt at komme ind eller er indrejst i et medlemsland.
  - Systemer beregnet til offentlige myndigheder til at kontrollere ægtheden af rejsedokumenter.
  - Systemer beregnet til at hjælpe offentlige myndigheder med behandlingen af ansøgninger om asyl, visum og opholdstilladelse og tilhørende klager.
8. Retspleje og demokratiske processer
- Systemer beregnet til at hjælpe retlige myndigheder med blandt andet at undersøge og fortolke fakta og lovgivning.

Forslaget giver Kommissionen beføjelser til at ændre bilag 3 via en delegeret retsakt, hvor Kommissionen kan tilføje anvendelser af kunstig intelligens, der falder under et af de otte områder, og der udgør en risiko for sundhed, sikkerhed eller de grundlæggende rettigheder. I vurderingen heraf skal Kommissionen tage højde for en række kriterier, herunder det potentielle omfang af den mulige skade, hvorvidt mennesker er afhængige af systemets resultat, samt hvor nemt det er at omgøre resultatet af systemet.

Selvom et system klassificeres som højrisiko i forordningen, betyder det ikke, at anvendelsen af systemet er lovlig under andre EU-retsakter eller national lovgivning. De eksisterende krav i den sammenhæng vil således stadig finde anvendelse.

## *Kapitel 2: Kravene for højrisikosystemer*

Systemer, der er kategoriseret som et højrisikosystem, pålægges en række forpligtelser. Det omfatter etableringen af et risikostyringssystem, der blandt andet skal identificere risici tilknyttet systemet samt indføre passende risikostyringsforanstaltninger til at adressere de pågældende risici.

Ud over risikostyringssystemet skal højrisiko kunstig intelligens desuden efterleve krav inden for:

- *data og datastyring*: Såfremt systemer involverer træning af modeller med data, skal de pågældende datasæt efterleve en række kvalitetskriterier, herunder blandt andet for passende datastyring- og dataforvaltningspraksis samt at datasæt skal være relevante, repræsentative, fejlfri og fuldstændige.
- *teknisk dokumentation*: Der skal udarbejdes teknisk dokumentation, der skal demonstrere efterlevelse af højrisiko kravene samt give nationale kompetente myndigheder og bemyndigede organer den nødvendige information til at vurdere overholdelsen af kravene. Bilag 4 indeholder de elementer, som den tekniske dokumentation som minimum skal omfatte. Det omfatter blandt andet en detaljeret beskrivelse af systemets elementer og processen for udviklingen, oplysninger om systemets funktion, overvågning og kontrol af systemet, en kopi af EU-overensstemmelseserklæringen samt en detaljeret beskrivelse af proceduren, der er på plads for at evaluere systemets ydeevne, efter det er kommet på markedet. Kommissionen får beføjelser til at ændre bilag 4 gennem delegerede retsakter.
- *registrering*: Systemer skal udformes og udvikles, således at der foretages automatisk registrering af systemets handlinger, dvs. logfunktioner, når det er i drift. Dette skal blandt andet muliggøre overvågning af driften af systemet samt sikre en passende grad af sporbarhed gennem hele systemets livscyklus.
- *gennemsigtighed og formidling af oplysninger til brugere*: Systemer skal udformes og udvikles, således at det sikres, at driften heraf er tilstrækkelig gennemsigtig til, at brugeren kan fortolke systemets output og anvende det korrekt. Samtidig skal systemet ledsages af en brugsanvisning i et passende digitalt format eller på anden vis, der blandt andet skal omfatte udbyderens kontaktoplysninger samt oplysninger om systemets egenskaber, kapaciteter, begrænsninger, foranstaltninger til menneskeligt tilsyn og forventede levetid.
- *menneskeligt tilsyn*: Systemer skal udformes og udvikles, således at de effektivt kan overvåges af personer i den periode, hvor systemet

anvendes. Dette skal enten sikres ved, at menneskeligt tilsyn indbygges direkte i systemet eller ved at menneskeligt tilsyn implementeres af brugeren. Det skal muliggøre, at de personer, der har ansvar for det menneskelige tilsyn, blandt andet er i stand til at forstå systemets kapaciteter og begrænsninger, at være opmærksom på den mulige tendens til automatisk at stole på systemet eller at gribe ind i driften af systemet og afbryde, hvis nødvendigt.

- *nøjagtighed, robusthed og cybersikkerhed*: Systemer skal udformes og udvikles, således at de i lyset af deres tilsigtede formål opnår et passende niveau af nøjagtighed, robusthed og cybersikkerhed. Nøjagtighedsniveauet skal fremgå af den medfølgende brugsanvisning. Robustheden kan opnås gennem tekniske løsninger såsom backupplaner. Cybersikkerhed skal sikre, at systemet er modstandsdygtigt med hensyn til at afværge en uautoriseret tredjeparts forsøg på at udnytte systemets sårbarheder. Dette kan omfatte tekniske løsninger, der blandt andet omfatter tiltag til at forhindre eller kontrollere for angreb.

Det er tanken med de ovenstående principbaserede krav, at den konkrete tekniske løsning enten kan leveres via harmoniserede standarder, fælles specifikationer eller udvikles på baggrund af udbydernes tekniske eller videnskabelig viden.

### *Kapitel 3: Forpligtelser for udbydere og brugere af højrisiko systemer og andre parter*

Kapitlet fastlægger forpligtelser for de forskellige aktører afhængig af deres placering i værdikæden:

- *udbydere* pålægges blandt andet at sikre overensstemmelse med højrisiko kravene, at etablere et kvalitetsstyringssystem, at udarbejde den tekniske dokumentation, at samarbejde med den kompetente myndighed, at gennemgå den relevante overensstemmelsesvurdering samt at CE-mærke systemet.
- *importører og distributører* pålægges blandt andet at sikre, at den relevante overensstemmelsesvurdering er udført af udbyderen, at systemet er forsynet med CE-mærkning samt ledsaget af påkrævet dokumentation og brugsanvisning.
- *brugere* pålægges blandt andet at sikre, at anvendelsen af systemet sker i overensstemmelse med den medfølgende brugsanvisning, at overvåge driften af systemet med henblik på mulige risici samt at underrette udbydere eller distributører om alvorlige hændelser eller funktionsfejl.

Såfremt en distributør, importør, bruger eller anden part under eget navn eller varemærke bringer et højrisiko kunstig intelligens-system i omsætning eller tager det i brug, eller såfremt de ændrer den påtænkte anvendelse eller foretager en væsentlig ændring af systemet, får de status som en udbyder og *bliver* deraf underlagt disse forpligtelser.

#### *Kapitel 4-5: Proceduren for overensstemmelsesvurdering*

Forordningen fastlægger, at efterlevelsen af højrisiko kravene skal kontrolleres via forudgående overensstemmelsesvurderinger. Dog formodes systemet at være i overensstemmelse med kravene, såfremt der er anvendt harmoniserede standarder eller fælles specifikationer, hvoraf sidstnævnt er vedtaget af Kommissionen via gennemførelsesretsakter.

De pågældende procedurer for overensstemmelsesvurderinger er forskellige, afhængigt af hvorvidt der er tale om kunstig intelligens, der er selvstændige systemer (punkt 2-8 i bilag 3), biometrisk identifikation og kategorisering af personer (punkt 1 i bilag 3) eller indlejret i et produkt (bilag 2).

Ved de selvstændige systemer omfattet af punkt 2-8 i bilag 3 skal overensstemmelsesvurderingen basere sig på intern kontrol, der ikke kræver inddragelsen af en tredjepart, dvs. et bemyndiget organ. Proceduren herfor er fastlagt i bilag 6 og påkræver blandt andet, at udbyderen kontrollerer, at det etablerede kvalitetstyringssystem er i overensstemmelse med kravene; at udbyderen undersøger oplysninger i den tekniske dokumentation for at vurdere, om systemet er i overensstemmelse med de relevante højrisiko krav; samt at udbyderen kontrollerer, at systemet og dets overvågning efter omsætning er i overensstemmelse med den tekniske dokumentation. Derudover skal udbydere af selvstændige systemer også registrere systemet i en offentlig tilgængelig EU-database, der etableres i forbindelse med forordningen samt varetages og vedligeholdes af Kommissionen.

Ved biometrisk identifikation og kategorisering af personer omfattet af punkt 1 i bilag 3 kan udbydere basere overensstemmelsesvurderingen på intern kontrol eller gå via overensstemmelsesvurdering gennem tredjepartskontrol, der blandt andet skal kontrollere kvalitetsstyringssystemet samt den tekniske dokumentation. Proceduren for tredjepartsoverensstemmelsesvurdering er fastlagt i bilag 7. Intern kontrol er dog kun muligt, såfremt udbyderen har anvendt harmoniserede standarder eller fælles specifikationer.

Forslaget giver Kommissionen beføjelser til at ændre bilag 6 og 7 via delegerede retsakter.

Ved de indlejrede systemer i produkter, der er omfattet af den harmoniserede EU-lovgivning baseret på "NLF" i bilag 2, skal den eksisterende overensstemmelsesvurdering under den pågældende sektorretsakt gøre sig gældende,

hvor der også tages højde for højrisiko kravene samt den tekniske dokumentation herom. Såfremt sektorretsakternes overensstemmelsesvurderinger giver mulighed for anvendelsen af harmoniserede standarder eller fælles specifikationer, der dækker kravene, kan udbyderne fravælge en tredjepartsoverensstemmelsesvurdering.

Såfremt der foretages en væsentlig ændring af systemet, kræver det, at systemet gennemgår en ny overensstemmelsesvurdering. Væsentlige ændringer omfatter imidlertid ikke ændringer, der er fastlagt på forhånd ved den indledende overensstemmelsesvurdering samt indgår i den tekniske dokumentation.

Udbyderne er pålagt at opbevare dokumentation, herunder den tekniske dokumentation, dokumenter i forbindelse med overensstemmelsesvurderingen samt EU-overensstemmelseserklæringen i en periode på 10 år til rådighed for de nationale kompetente myndigheder.

I tilfælde af ekstraordinære situationer i forhold til beskyttelse af offentlig sikkerhed, menneskers liv og sundhed, miljø eller centrale industrielle samt infrastrukturmæssige aktiver kan markedsovervågningsmyndighederne tillade, at specifikke højrisiko systemer bringes i omsætning eller tages i brug uden en overensstemmelsesvurdering, såfremt tilladelsen gælder for en begrænset periode, mens de nødvendige overensstemmelsesvurderinger gennemføres, og såfremt myndigheden konkluderer, at højrisiko kravene overholdes. Dette skal underrettes til både Kommissionen og de øvrige medlemslande, der får mulighed for at gøre indsigelse.

#### Afsnit IV: Gennemsigtighedsforpligtelser for visse systemer (artikel 52)

For visse anvendelser af kunstig intelligens pålægges **der** gennemsigtighedsforpligtelser:

- Ved systemer, der er beregnet til at interagere med personer, skal personer informeres om denne interaktion, medmindre dette er indlysende ud fra omstændighederne og anvendelsessammenhængen.
- Ved systemer, der er beregnet til at genkende følelser eller biometrisk kategorisering, skal personer informeres om deres eksponering for sådanne systemer.
- Ved systemer, der er beregnet til at generere eller manipulere billede-, lyd- eller videoindhold, der i væsentlig grad ligner blandt andet faktiske personer eller genstande, og der fejlagtigt vil fremstå ægte, eksempelvis deep fakes, skal der informeres om, at indholdet er genereret på kunstig vis eller er manipuleret.

Kravene er dog undtaget i forbindelse med systemer, der er tilladt ved lov med henblik på retshåndhævelse. Ved sidstnævnte anvendelse er kravet der-

udover heller ikke gældende, hvis anvendelsen er nødvendig for at udøve retten til ytringsfrihed eller retten til kunst og videnskab, der er sikret ved Den Europæiske Unions charter om grundlæggende rettigheder.

#### Afsnit V: Foranstaltninger til støtte for innovation (artikel 53-55)

Forordningen fastsætter fælles regler for oprettelsen af reguleringsmæssige sandkasser inden for kunstig intelligens samt samarbejde mellem relevante myndigheder. Sandkasserne kan etableres af et eller flere medlemslandes kompetente myndigheder samt den Europæiske Tilsynsførende for Databeskyttelse. Formålet er at fremme innovationen inden for kunstig intelligens ved at etablere et kontrolleret miljø blandt andet med henblik på at lette udviklingen og validering af systemer i et begrænset tidsrum, inden de bringes i omsætning eller tages i brug, accelerere markedsadgang samt at sikre overholdelse af forordningen og anden relevant lovgivning.

Medlemslandene forpligtes desuden til at indføre foranstaltninger for mindre udbydere og brugere, blandt andet skal medlemslandene prioritere disse aktører samt nystartede virksomheders adgang til de reguleringsmæssige sandkasser samt organisere informationsaktiviteter.

#### Afsnit VI, VII og VIII: Forvaltning og gennemførelse (artikel 56-68)

Medlemslande spiller en nøglerolle i forvaltningen og håndhævelsen af forordningen. Hvert medlemsland skal i den forbindelse udpege en eller flere nationale kompetente myndigheder, hvoraf en af myndighederne skal fungere som ansvarlig national tilsynsmyndighed og dermed det officielle kontaktpunkt over for andre medlemslande og Kommissionen.

Et europæisk udvalg for kunstig intelligens skal desuden nedsættes for at assistere Kommissionen i forvaltningen af forordningen. Formålet med udvalget er at bidrage til et effektivt samarbejde mellem de nationale tilsynsmyndigheder og Kommissionen, at koordinere og bidrage til vejledning og analyse samt at assistere i sikringen af en ensartet anvendelse af forordningen. Udvalget skal bestå af repræsentanter fra de nationale tilsynsmyndigheder samt den Europæiske Tilsynsførende for Databeskyttelse.

Udbydere af højrisiko systemer er pålagt at etablere et overvågningssystem og -plan, der efter omsætningen af højrisiko systemet på markedet blandt andet skal sørge for en løbende evaluering af overholdelsen af højrisiko kravene. De nærmere detaljer herfor vil blive fastlagt af Kommissionen via en gennemførelsesretsakt.

I tilfælde af alvorlige hændelser eller funktionsfejl såsom en persons død, alvorlig skade eller afbrydelse af driften af kritisk infrastruktur eller overtrædelse af grundlæggende rettigheder er udbydere af højrisiko systemer pålagt at informere den relevante markedsovervågningsmyndighed herom.

Markedsovervågningen og kontrol af kunstig intelligens-systemer skal ske på baggrund af markedsovervågningsforordningen, der skal finde anvendelse på kunstig intelligens-forordningens udbydere, importører, distributører og brugere på tilsvarende måde, som markedsovervågningen i dag finder anvendelse på økonomiske operatører af produkter. Procedurene i markedsovervågningsforordningen suppleres blandt andet med regler om adgang til data og dokumentation samt procedurer for meddelelse af og kontrol med nationale indgreb over for kunstig intelligens-systemer. Herudover skal kompetencedelingen imellem markedsovervågningsmyndighederne hovedsageligt følge den kompetencedeling, der findes i dag.

#### Afsnit IX: Adfærdskodeks (artikel 69)

Forordningen fastlægger en ramme for udformningen af adfærdskodeks, der har til formål at tilskynde udbydere uden for højrisikokategorien til frivilligt at anvende højrisiko kravene. Sådanne adfærdskodeks kan også tilskynde den frivillige anvendelse af yderligere krav, eksempelvis inden for bæredygtighed eller mangfoldighed i udviklingsholdet.

#### Afsnit X, XI og XII: Afsluttende bestemmelser (artikel 70-85)

Afsnit X fastlægger forpligtelser vedrørende fortroligheden af information og data samt fastlægger regler for udveksling af oplysninger, der er indhentet i forbindelse med gennemførelsen af forordningen.

Samtidig indeholder afsnittet også foranstaltninger til at sikre en effektiv gennemførelse af forordningen gennem sanktioner for overtrædelse af bestemmelserne, der er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. Medlemslandene pålægges, at indfører regler om sanktioner, herunder administrative bøder, hvor der blandt andet skal tages højde for mindre udbydere og nystartede virksomheder. Medlemslande skal meddele Kommissionen om disse regler. I stil med GDPR tages der dog højde for medlemslandenes forskellige retssystemer, hvor det fastlægges, at administrative bøder kan anvendes på en sådan måde, at bøderne pålægges af kompetente nationale domstole.

I tilfælde af manglende overholdelse vedrørende forbud i artikel 5 eller ved manglende overholdelse af højrisiko kravene vedrørende data og datastyring i artikel 10 kan der pålægges bøder på op til 30 mio. euro eller op til 6 procent af den samlede globale omsætning i det foregående regnskabsår. I tilfælde af manglende overholdelse af andre bestemmelser i forordningen kan der pålægges bøder op til 20 mio. euro eller op til 4 procent af den samlede globale omsætning i det foregående regnskabsår. I tilfælde af afgivelse af ukorrekte, ufuldstændige eller vildledende oplysninger til nationale kompetente myndigheder eller bemyndigede organer kan der pålægges bøder op til 10 mio.

euro eller op til 2 procent af den samlede globale omsætning i det foregående regnskabsår.

Afsnit XI indeholder regler for udøvelse og delegering af beføjelser til Kommissionen, herunder for brugen af delegerede og gennemførelsesretsakter. Forslaget bemyndiger Kommissionen til, hvor det er relevant, at vedtage gennemførelsesretsakter for at sikre ensartet anvendelse af forordningen eller delegerede retsakter til opdatering eller supplerende af bilag 1 til 7, herunder til definitionen af kunstig intelligens samt listen over selvstændige højrisiko systemer.

Afsnit XII indeholder blandt andet en forpligtelse for Kommissionen om årligt at vurdere behovet for en opdatering af bilag 3 og til regelmæssigt at udarbejde rapporter om evalueringen og gennemgangen af forordningen.

Samtidig fastlægges det i afsnittet, at forordningen kun finder anvendelse på højrisikosystemer, der allerede er bragt i omsætning eller taget i brug, hvis disse systemer undergår betydelige ændringer i forhold til deres design eller tilsigtede formål efter anvendelsesdatoen.

Forordningen vil træde i kraft 20 dage efter offentliggørelse i Den Europæiske Unions Tidende og finde anvendelse to år efter ikrafttrædelsesdatoen. Dog skal overensstemmelsesvurderingerne, forvaltningen samt reglerne for sanktioner være operationelle inden forordningens anvendelse. Derfor lægges der op til en tidligere anvendelsesdato for de disse områder, henholdsvis tre måneder for overensstemmelsesvurderinger og forvaltningsstrukturen samt 12 måneder for sanktionsreglerne efter forordningens ikrafttrædelsesdato.

#### **4. Europa-Parlamentets udtalelser**

I Europa-Parlamentet blev det 1. december 2021 besluttet at Udvalget om det Indre Marked og Forbrugerbeskyttelse (IMCO) og Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender (LIBE) har fælles kompetence på sagen. Derudover er industri, forsknings-, og energi-, udvalget (ITRE), retsudvalget (JURI), og kultur og uddannelses- udvalget (CULT) associerede udvalg.

IMCO og LIBE offentliggjorde deres fælles udkast den. 21. april og en endelig plenarafstemning forventes i november 2022. I IMCO er italienske S&D medlem Brando Benifei udnævnt som ordfører, mens det i LIBE er rumænske RENEW-medlem Dragos Tudorache.

IMCO og LIBE støtter op om den risikobaserede tilgang mens det understreges, at ingen kunstig intelligens skal ekskluderes fra forordningen ex-



ante, hverken fra definitionen af kunstig intelligens eller ved at lave undtagelser for visse typer af systemer. Det fremhæves, at forordningen i højere grad skal strømlines med GDPR, samt at interessenter og civilsamfundsorganisationer i højere grad skal inddrages ift. at opdatere listen over højrisikosystemer, standardiseringsprocessen samt udvalgets og sandkassernes aktiviteter.

I rapporten tilføjes ”predictive policing” til listen over forbudte anvendelser, ligesom det foreslås at tilføje en række yderligere brugsscenarier til listen over højrisikosystemer. Derudover identificeres yderligere deepfakes og redaktionelt indhold skrevet af kunstig intelligens som systemer, der bør underlægges både gennemsigtighedskrav og højrisiko overensstemmelsesprocedurerne.

Rapporten indeholder et nyt kapitel 3a om håndhævelse på EU-niveau. Der lægges op til en ny håndhævelsesmekanisme til Kommissionen, som bl.a. kan udløses hvis det vurderes, at et system vil føre til en såkaldt ”omfattende brud”, der omfatter tre eller flere medlemslande. Mekanismen bygger på modellen fra Digital Services Act. Samtidig lægges op til, at udvalget for kunstig intelligens skal spille en større rolle, fx i at vejlede Kommissionen og nationale tilsynsmyndigheder og udgøre et forum for voldgift af tvister mellem en eller flere medlemslande. Endelig foreslås et nyt kapitel om retsmidler for både fysiske og juridiske personer, herunder ift. retten til at klage.

I Europa-Parlamentets Retsudvalg offentliggjorde ordføreren Axel Voss fra EPP sin rapport i marts og en lang række ændringsforslag blev offentliggjort i starten af april. Voss har lagt op til at indsnævre definitionen betydeligt og anlægge en mere tydelig risikobaseret tilgang. Ændringsforslagene går dog i mange retninger, og det er derfor for tidligt at konkludere, hvordan retsudvalgets endelige rapport vil falde ud.

Europa-Parlamentet forventes at nå til enighed om en holdning i starten af 2023.

## 5. Nærhedsprincippet

Kommissionen vurderer, at regulering på EU-niveau er nødvendig henset til karakteren af kunstig intelligens, der ofte er afhængig af store og varierede datasæt, og der kan være integreret i ethvert produkt eller enhver tjeneste til fri cirkulation i det indre marked.

Uden regulering på EU-niveau vurderer Kommissionen, at der er risiko for, at medlemslande vedtager egne regler for kunstig intelligens, der potentielt

kan divergere eller være modstridende. Dette vil hæmme den frie bevægelighed af produkter og tjenester med kunstig intelligens-systemer samt bremse markedsoptagelsen af kunstig intelligens i EU, herunder grundet juridiske usikkerhed og barrierer. Derudover vurderer Kommissionen, at dette vil lede til ineffektiv beskyttelse af sikkerheden og af de grundlæggende rettigheder samt EU's værdier i de forskellige medlemslande. Af disse grunde ser Kommissionen derfor, at EU-regulering er nødvendig for at opnå formålet om at fremme et indre marked for lovlige, sikre og pålidelige kunstig intelligens-systemer.

Regeringen er enig med Kommissionen i, at regulering af området bør ske på EU-niveau, da ensartet regulering er nødvendig for realiseringen af det digitale indre marked. Derfor vurderer regeringen på det foreliggende grundlag, at nærhedsprincippet er overholdt.

## **6. Gældende dansk ret**

Der findes på nuværende tidspunkt ikke en specifik juridisk ramme for kunstig intelligens hverken på europæisk eller nationalt plan.

Udviklingen og anvendelsen af kunstig intelligens er dog underlagt eksisterende lovgivning, der ikke nødvendigvis indeholder specifikke krav til kunstig intelligens, men alligevel fastsætter regler om eksempelvis beskyttelse af grundlæggende rettigheder, herunder blandt andet ligestilling, forbrugerbeskyttelse og databeskyttelse, samt inden for områderne såsom asyl, migration, retligt samarbejde, finansielle tjenester samt produktsikkerhed. Disse har direkte indvirkning på udviklingen og anvendelsen af kunstig intelligens.

## **7. Konsekvenser**

### *Lovgivningsmæssige konsekvenser*

Forslaget vil indebære lovgivningsmæssige konsekvenser. Blandt andet vil forslaget supplere visse eksisterende sektorretsakter inden for produkt- samt finansområdet, hvor disse retsakter skal tage højde for højrisikokraverne i forbindelse med overensstemmelsesvurderinger eller risikostyringsprocedurer. Såfremt disse sektorretsakter er implementeret i dansk lovgivning, kan det potentielt kræve lovændringer i Danmark.

Samtidig vil forslaget kræve, at Danmark indfører regler for sanktioner.

### *Økonomiske konsekvenser*

### *Statsfinansielle konsekvenser*

Det forventes, at forslaget vil medføre statsfinansielle konsekvenser, idet udpegning eller etablering af en national tilsynsmyndighed, der er ansvarlig for implementeringen af forordningen, vil kræve ressourcer. Tilsynsfunktionen kan bygge på eksisterende strukturer, men vil kræve tilstrækkelig teknologisk ekspertise og ressourcer. Kommissionen vurderer, at ressourcebehovet afhængig af den eksisterende struktur i hvert medlemsland kan udgøre 1 til 25 fuldtidsansatte. Derudover vil det kræve ressourcer i forhold til etableringen af det europæiske udvalg for kunstig intelligens, hvor hvert medlemsland skal udpege en repræsentant. Der vil ligeledes opstå en forøgelse af resourceforbruget hos den eller de myndigheder, der udpeges til kompetente myndigheder, idet forordningen medfører en øget sagsmængde eller en udvidet opgaveportefølje, herunder i forhold til den kontinuerlige evaluering af forordningen, der er indbygget i forslaget.

Ligeledes forventes forslaget at medføre administrative byrder for offentlige myndigheder til efterlevelse af de krav, der påkræves i forbindelse med højrisiko kunstig intelligens, herunder proces- og dokumentationskrav samt krav om menneskeligt tilsyn. Samtidig kan kravene medføre statsfinansielle konsekvenser for den højrisiko kunstig intelligens, der udvikles og anvendes af offentlige myndigheder i forbindelse med kravet i den politiske aftale om digitaliseringsklar lovgivning.

Regeringen er fortsat i gang med at evaluere de statsfinansielle omkostninger forbundet med udvidelsen af tilsyn hos de eksisterende myndigheder som foreslået af Kommissionen.

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 positive samfundsøkonomiske konsekvenser, såfremt de harmoniserede regler er med til at styrke tilliden samt skabe juridisk klarhed i det indre marked for kunstig intelligens og deraf resultere i øget optag samt forbedrede skaleringsmuligheder. Det vurderes, at det potentielt kan have en positiv effekt på samfundsøkonomien i form af øget produktivitet og konkurrenceevne.

#### *Erhvervsøkonomiske konsekvenser*

Forslaget forventes at medføre væsentlige administrative byrder for de omfattede virksomheder, herunder særligt i forbindelse med efterlevelsen af de krav, der påkræves i forbindelse med højrisiko kunstig intelligens. Byrderne kan dog ikke kvantificeres nærmere på nuværende tidspunkt, da kravenes endelige udformning og udmøntning endnu ikke er kendt.

Da forslaget krav forventes at omfatte danske virksomheder, vurderes de samlede administrative byrder at kunne have et betydeligt omfang, idet lovgivning dækker et komplekst område, hvor anvendelsen potentielt kan findes på tværs af alle sektorer. Konsekvenser for danske virksomheder vil både omfatte udviklingen samt anvendelsen af de omfattede systemer, herunder ligeledes proces- og dokumentationskrav. Eksempelvis kan kravet om menneskeligt tilsyn samt efterlevelse af kravene i hele systemets livscyklus medføre omkostninger i forbindelse med opkvalificering af medarbejdere samt årlige lønudgifter forbundet med tilsynet.

Herudover forventes forslaget gennemsigthedsforpligtelser ved visse systemer med begrænset risiko samt den frivillige vedtagelse af adfærdskodeks at medføre administrative byrder. Forbud mod visse systemer kan derudover medføre øvrige efterlevelseseffekter, idet forbud udgør en produktionsbegrænsning for virksomheder. Det er dog uvist, hvorvidt der er danske virksomheder, der vil være omfattet af de konkrete forbud.

#### Andre konsekvenser og beskyttelsesniveauet

En vedtagelse af forslaget forventes at kunne forbedre beskyttelsesniveauet for borgere, forbrugere og samfundet som helhed som følge af, at forslaget har til hensigt at skabe et mere ansvarligt indre marked for kunstig intelligens. Dette ved at stille krav til udviklingen og anvendelsen af den del af teknologien, der kan have negativ eller direkte skadelig indvirkning på sikkerhed, gældende lov samt grundlæggende rettigheder, samt ved at stille krav om gennemsigthed ved visse anvendelser.

## **8. Høring**

Forslaget har været sendt i EU-specialudvalget for konkurrenceevne, vækst og forbrugerspørgsmål med frist for bemærkninger den 5. maj 2021. Der er indkommet høringssvar fra Dansk Erhverv, Dansk Industri, Dansk Standard, Finans Danmark, Finansforbundet, Forbrugerrådet Tænk, Forsikring & Pension, Ingeniørforeningen IDA, IT-Branchen og Kommunernes Landsforening.

### **Generelle bemærkninger**

**Dansk Industri (DI)** ser Kommissionens forslag som en mulighed for, at medlemslandene skal være de bedste i verden til at bruge data og kunstig intelligens på en ansvarlig måde. Der er behov for at regulere området, hvilket virksomhederne også har efterspurgt, men det skal ske med den rette balance. På den ene side skal anvendelsen af kunstig intelligens føre til beslutninger, resultater og anbefalinger, som man kan stole på. På den anden side skal man huske, at anvendelsen af kunstig intelligens kan være en

afgørende faktor i løsningen af samfundsudfordringer som den grønne omstilling og skabe ny vækst, og at man ikke må stille urealistiske krav og administrative byrder, der hæmmer innovationen og rammer bredere end tiltænkt.

**Dansk Standard** fremhæver, at den kommende lovgivning kan få global effekt. Høje standarder kan være en effektiv måde at opnå indflydelse globalt og kan fremme den europæiske konkurrenceevne. Virksomheder, som vil sælge deres produkter på det attraktive europæiske marked, må udvikle produkter som overholder europæisk lovgivning. De høje europæiske standarder og produktkrav kan dermed migrere til andre dele af verden.

**Finans Danmark** hilser Kommissionens udspil velkomment. Finans Danmark ser store muligheder i brugen af kunstig intelligens, da det giver mulighed for, at Europa kan øge velstanden for borgerne og sætte skub i væksten for virksomhederne. Det er vigtigt, at der etableres en sammenhængende og robust regulering af kunstig intelligens. Det vil på den ene side tilvejebringe gode rammer for at udvikle og udbrede kunstig intelligens, og på den anden side sikre at borgere og forbrugere trygt kan anvende de løsninger, der anvender kunstig intelligens.

**Finansforbundet** er positivt indstillet over for regulering på området, hvor der bør reguleres med udgangspunkt i europæiske værdier og beskyttelse af mennesker. Virksomheder må redegøre for beslutninger som træffes algoritmisk og stå til ansvar for fejlagtige beslutninger. Teknologierne må og skal anvendes konstruktivt og ikke til øget overvågning. Derfor skal regler og kodekser tilsige, hvad kunstig intelligens må bruges til, og navnlig hvad den ikke må bruges til. Transparens i anvendelsen af ethvert kunstig intelligens-værktøj er ligeledes af stor vigtighed.

**Finansforbundet** mener, at virksomheder bør følge et forklaringsprincip og redegøre for de beslutninger, der træffes af algoritmer. Ansvar ligger entydigt hos ledelsen, hvis der træffes fejlagtige beslutninger ud fra algoritmens beregninger. Virksomheden bør opstille klare retningslinjer og grænser for værktøjerne, ligesom virksomheder skal udvikle, implementere og følge et handlingsorienteret og praksisnært dataetisk kodeks.

**Forbrugerrådet Tænk** støtter Kommissionens forslag, idet det er nødvendigt med regler, der sikrer en dataetisk tilgang til udvikling og brug af kunstig intelligens i hele EU. Kunstig intelligens indgår allerede i kommercielle produkter og tjenester målrettet forbrugere, ligesom kunstig intelligens er taget i anvendelse i den offentlige sektor. Udviklingen forventes at gå stærkt og derfor haster det med at få et regelsæt på plads, så en dataetisk tilgang til at udvikle og anvende teknologien harmoniseres på tværs af EU.

**Ingeniørforeningen IDA (IDA)** er positive over for EU's tilgang til regulering af kunstig intelligens, når formålet blandt andet er at skabe en europæisk vej – et alternativ til den amerikanske ”data for profit” og den kinesiske ”data for control”. Kunstig intelligens er en ny og relativ umoden teknologi, der udvikler sig hurtigt. Der er flere steder i verden sat store summer af til forskning og udvikling med forskellige formål, der ikke nødvendigvis er i overensstemmelse med danske eller europæiske værdier. Det er derfor vigtigt, at myndighederne er med til at sætte demokratisk fastsatte rammer for, hvad man vil med denne teknologi, hvad den skal bruges til, og hvad man ikke ønsker, at den skal bruges til.

**IDA** fremhæver, at kunstig intelligens og den enkelte borgers retssikkerhed skal gå hånd i hånd. Datakvaliteten skal ligeledes være i orden. De fejl, der lægges ind i kunstig intelligens, går igen i outputtet og i langt større skala, end man er vant til. Derudover finder kunstig intelligens mønstre i eksisterende data og gentager disse. Det vil sige, at hvis ikke man er opmærksom, kommer man til at forstærke de u hensigtsmæssigheder og problemer, som man allerede har i dag. IDA mener, at formålet med en regulering må være at understøtte tillid til brug af data, så flere data kan komme ud at arbejde.

**IT-Branchen** mener, at det er positivt, at EU går forrest og skaber en ramme for regulering af kunstig intelligens som modspil til tilgangen fra USA og Kina. Helt overordnet bliver det afgørende, at reguleringen ikke afskrækker brugen af kunstig intelligens. For kunstig intelligens rummer store muligheder for at gøre samfundet endnu bedre. Danske virksomheder efterspørger klare og ensartede regler inden for kunstig intelligens, som gælder på tværs af landegrænser og som skaber lige konkurrencevilkår.

**IT-Branchen** ser, at det bliver helt centralt, hvordan resten af verden tager imod reguleringen, så virksomhederne i EU ikke skal leve op til forskellige regler i forskellige verdensdele. Det vil ikke kun svække virksomheders konkurrenceevne, men det vil være en stopklods for innovation og udvikling til det globale marked. I værste fald risikerer EU at blive valgt fra som et attraktivt sted for nye startups. En forsigtig og præventiv tilgang til regulering kan have en stor effekt på innovationshøjden i EU. Helt generelt mener IT-Branchen, at regulering som udgangspunkt bør være teknologineutral, og at etisk problematiske anvendelser af datadrevne løsninger ikke kan afgrænses til kunstig intelligens.

**Kommunernes Landsforening (KL)** mener, at det er relevant med en EU-indsats til regulering af anvendelse af kunstig intelligens, og at den skal sikre borgernes rettigheder og tillid til den offentlige sektor. Reguleringen skal tage højde for medlemslandenes forskelligheder samt det forhold, at diskussionerne om dataetik og kunstig intelligens er forskellige steder på tværs af EU. KL mener, at der i den offentlige sektor er behov for klare

juridiske rammer og brugbare redskaber samt hjælp til at forstå og fortolke, hvordan man må arbejde med kunstig intelligens. Det er afgørende, at gennemsigthed sikrer, at borgere kan have tillid til og kan gennemskue, at myndigheder anvender kunstig intelligens ansvarligt.

**KL** finder, at kunstig intelligens skal anvendes, hvor det kan effektivisere og forbedre den kommunale administration og sagsbehandling, men finder samtidig også, at det er afgørende, at beslutninger, der regulerer væsentlige forhold for borgere, ikke alene kan træffes på baggrund af behandlinger foretaget med kunstig intelligens. **KL** fremhæver ligeledes arbejdet med signaturprojekter vedrørende anvendelse af kunstig intelligens på en række kommunale fagområder. En kommende forordning og en efterfølgende dansk implementering bør blandt andet tage afsæt i de konkrete kommunale erfaringer og behov fra signaturprojekterne.

### **Specifikke bemærkninger**

#### *Forslagets anvendelsesområde og definitioner*

**Dansk Erhverv (DE)** bemærker, at en stor del af de problemer, som forordningen er sat i verden for at løse, allerede er eller burde være dækket under anden regulering. Bedre håndhævelse af de eksisterende regler er en genvej til at mitigere nogle af de risici, der søges at adressere. Heri ligger også, at der er nogle handlinger, hvor lovligheden ikke bør afgøres af, om det er en maskine, der udfører dem, eller et menneske.

**DE** mener, at forslaget bruger en uklar og uhensigtsmæssig definition på kunstig intelligens, og der bør skelnes yderligere mellem, hvordan kunstig intelligens anvendes. Bilag 1 inkluderer ganske almindelige statistiske værktøjer og metoder til sandsynlighedsberegning. Med så bred en definition er der et stort antal databehandlingsværktøjer, der risikerer at falde ind under lovgivningen, som ret beset intet har at gøre med kunstig intelligens. Samtidig nævnes "AI systems that continue to 'learn' after being placed in the market" som en særskilt kategori. Det understreger behovet for en klarere forståelse af, hvad kunstig intelligens dækker over, da netop evnen til at imitere menneskelig læring og optimering i forhold til opgaveløsning er en del appellen ved at bruge kunstig intelligens.

**DE** bemærker, at der i forslaget skelnes til formålet og konteksten for anvendelse af kunstig intelligens, men at der med fordel også bør skelnes mellem algoritmer, der er designet til at kunne træffe beslutninger, samt de mange andre måder som kunstig intelligens anvendes på.

**DE** støtter desuden, at kunstig intelligens-systemer, der allerede er bragt til markedet forud for forordningens ikrafttræden, ikke omfattes, såfremt der ikke sker væsentlige ændringer i systemernes design eller formål.

**DI** bakker op om en risikobaseret tilgang til regulering af kunstig intelligens. DI fremhæver, at med forslaget definition af kunstig intelligens, der inkluderer brug af statistiske metoder, samt med definitionen af højrisikoanvendelse i produkter vil forordningen komme til at ramme mange allerede etablerede digitale løsninger, hvor krav om involvering af tredjepartskontrol vil være urimelig dyr og unødvendig, når det gælder produkter. DI bemærker i den forbindelse, at de eksisterende krav allerede er omkostningskrævende, og de ekstra krav risikerer derved at bremse innovatonslysten. En løsning kunne være at indskrænke definitionen ved at udelade de statistiske metoder. Alternativt kan det undtages i maskinproduktforordningen og tilsvarende reguleringer.

**Finans Danmark** anbefaler en risikobaseret tilgang med flere risikoniveauer. En risikobaseret tilgang med kun to niveauer vil sandsynligvis reducere anvendelsen af kunstig intelligens. Finans Danmark ser, at der med fordel kan søges inspiration i, hvorledes den finansielle regulering fungerer i forhold til fintech, hvor man arbejder med en regulatorisk perimenter. Sådan en tilgang vil både sikre forbrugerbeskyttelsen samt understøtte innovation og udvikling.

**Finans Danmark** finder, at forslaget ikke sonder tydeligt mellem kunstig intelligens, der anvendes til at støtte menneskelige beslutninger, og den kunstige intelligens, der fungerer autonomt. En risikobaseret tilgang bør afstedkomme lettere regulatoriske krav til kunstige intelligenser, der kun bruges til at hjælpe mennesker med at træffe beslutninger, hvorimod autonome kunstige intelligenser skal reguleres mere indgående. Samtidig er det vigtigt at sikre lige vilkår for alle brancher og geografier.

**Finansforbundet** mener, at den valgte tilgang med horisontal lovgivning og proportional, risikobaseret tilgang til brugen af kunstig intelligens, herunder med angivelse af ikke tilladt kunstig intelligens-benyttelse, som går imod EU's værdier, virker fornuftig.

**Forsikring & Pension** mener, at det er positivt, at Kommissionen lægger op til, at reguleringen bliver risikobaseret og proportional, så der alene fokuseres på højrisiko og forbudte applikationer, og at almindelige robot-automatiseringsprocesser ikke rammes af unødvendige skrappe krav. Definitionen af kunstig intelligens og anvendelsesområdet for reguleringen ser ud til at blive indskrænket. Det er positivt, fordi en bred definition af begrebet kunstig intelligens vil ramme en lang række almindelige automatiseringsprocesser, der ikke udgør nogen risiko for forbrugerne. Forsikring & Pension fremhæver, at bilag 1 referer til en række teknikker, der karakteriseres som kunstig intelligens. Der kan dog stadig være juridisk uklarhed om, hvorvidt et system er omfattet eller ej, hvilket bør klarlægges.



**KL** mener, at en risikobaseret tilgang i sig selv er fornuftig, men at der er behov for en udfoldning og dialog om, hvilke kriterier der skal lægges til grund for en bestemt risikovurdering, og at der skal være mulighed for at kategorierne kan nuanceres af de enkelte lande. Der vil i konkrete tilfælde være stor forskel på, hvilke formål som løsningen skal bidrage til, og der er derfor behov for en nuanceret tilgang, der indeholder en relativt fintmasket risikovurdering til det enkelte projekt. Placeringen i risikogruppen og dertilhørende forpligtelser skal tage højde for en given løsnings kombination af formål, teknologi og output. **KL** mener, at det på nuværende tidspunkt er vanskeligt at vurdere konsekvenserne af forordningen, og at der er derfor behov for dybere præciseringen af konkrete reguleringstiltag.

#### Forbudt praksis med hensyn til kunstig intelligens

**DE** mener, at nogle af de problemer, som forslaget skal løse, allerede er klart ulovlige. Som eksempel på kunstig intelligens, der udnytter udsatte grupper, har Kommissionen præsenteret, at dette kan være en dukke, der med en integreret stemmeassistent, opfordrer børn til at udføre farlige handlinger. Uanset om denne stemmeassistent har en kunstig intelligens-komponent eller blot er en optagelse, der afspilles ved faste intervaller, har **DE** en klar formodning om, at dette allerede er dækket af eksisterende lovgivning – og at det ellers under alle omstændigheder burde være det. Det er med til at understrege, at Kommissionen enten er i færd med at regulere områder, som allerede er dækket under anden lovgivning, eller at Kommissionen er uklar på, hvad formålet med forordningen er. Derfor mener **DE**, at der med fordel kan arbejdes på at skabe større klarhed om forordningens intention og formål.

**DE** er til dels enige i, at der kan være brug af kunstig intelligens, som strider mod vores europæiske værdier og rettigheder, men i artikel 5 forbydes anvendelse af kunstig intelligens i for brede træk, således at det kan forhindre, at teknologiens potentiale bruges til gode formål.

**Forbrugerrådet Tænk** mener, at selvom kunstig intelligens kan skabe en positiv forandring i samfundet, kan teknologien også gøre skade på det enkelte individ. Det sker, hvis de algoritmer, der i fremtiden kommer til at træffe beslutninger og afgørelser, diskriminerer og dermed ikke udvikles på betryggende vis, eller hvis den data, der anvendes til analyserne, ikke er forsvarligt sikret. Forbrugerrådet Tænk støtter derfor, at forslaget lægger op til at forbyde visse former for brug af kunstig intelligens, ligesom forslaget henviser til, at charteret for menneskerettigheder og databeskyttelseslovgivningen/GDPR skal overholdes.

#### Højrisiko kunstig intelligens-systemer

**DE** bemærker, at en række produkter, hvor højrisiko kunstig intelligens indgår som komponent, blandt andet køretøjer, kun er omfattet af forordningens artikel 84 vedrørende evaluering og gennemgang. Dette bør udvides til at gælde alle eksisterende produktdirektiver mv., da den nuværende opdeling, hvor nogle produktkategorier både reguleres af sektorspecifik regulering og denne forordning, giver anledning til regulatorisk overlap, uigennemsigtighed og usikkerhed for virksomhederne.

**DE** bemærker, at datasæt til træning, validering og test af kunstig intelligens-systemer pålægges krav om at være fri for fejl. **DE** støtter intentionen om høj datakvalitet, som er fri for bias og er repræsentativ, men med de meget store datasæt, der kræves for at kunne træne algoritmer, vil det være tidskrævende og ressourcetungt at skulle sikre, at der ikke er en eneste fejl i datasættet. Dette vil medføre betydelige administrative byrder for virksomheder og kan reducere innovation og afprøvning af nye løsninger.

**DE** fremhæver, at der stilles krav om, at teknisk dokumentation bør være opdateret. Her vil det være hensigtsmæssigt at have klare rammer for, hvor ofte materialet skal opdateres for at leve op til dette krav. Derudover vil det være hensigtsmæssigt med flere templates og/eller eksempler. Det gælder både systemer til kvalitetstjek, men kan også udvides til at omfatte eksempelvis teknisk dokumentation mv.

**DE** fremhæver, at det vil være vanskeligt for udviklere, leverandører og forhandlere at sikre fuld forståelse for kapacitet og begrænsninger ved et givent kunstig intelligens-system hos den person, der har ansvar for menneskeligt tilsyn. En del af dette ansvar bør pålægges brugerne, ligesom det understreger behovet for investeringer i uddannelse, kompetence- og vidensløft i befolkningen, efterhånden som flere medarbejdsgrupper skal bruge forskellige former for kunstig intelligens.

**DE** anser det for fornuftigt, at der stilles krav til modstandsdygtigheden i højrisiko kunstig intelligens-systemer, men der vil altid være en mulighed for, at der opstår fejl eller lignende, når systemet interagerer med mennesker. Det er ikke muligt at lave systemer, som er fuldstændigt sikrede mod fejl 40-hændelser, og derfor er investeringer i uddannelse vigtig for at reducere denne type risiko.

**DE** mener desuden, at der er uklarhed, i forhold til hvornår et højrisiko kunstig intelligens-system skal revurderes.

**DI** mener, at der er behov for afklaring af definitionen af højrisikoanvendelse i produkter. Det er uklart, om det alene er kunstig intelligens designet til at indgå i sikkerhedskomponenter, der er omfattet, eller om det også gælder andre anvendelser, der kræver tredjepartskontrol. Ifølge NLF skal

lovgiver vælge de moduler til overensstemmelsesvurdering, som er relevante i forhold til størrelsen af risikoen. Derfor synes det logisk at kræve tredjepartskontrol ved højrisikooanvendelse. DI finder dog, at forslaget definerer risiko omvendt, hvor en anvendelse af kunstig intelligens bliver betragtet som højrisiko, hvis sektorlovgivningen stiller krav om tredjepartskontrol. Det kan gælde produktkategorier, men det kan også opstå ved manglende harmoniserede standarder. De nuværende problemer med at harmonisere europæiske standarder kan få afgørende indflydelse på, hvilke anvendelser af kunstig intelligens der karakteriseres som højrisikooanvendelse. Løses problemet ikke, vil det medføre unødigt store omkostninger.

**DI** fremhæver, at forslagens massive bødestørrelser stiller ekstra høje krav til, at det skal være tale om tydelige kriterier, klarhed over hvorvidt virksomhederne indfrier kravene, og at reguleringen ikke rammer bredere end tiltænkt. I forhold til selve kravene ved højrisikooanvendelse af kunstig intelligens bør der være mere fokus på den ønskede effekt end at stille specifikke krav til at opnå den ønskede effekt. DI finder det afgørende for reguleringens succes og europæiske virksomhedernes konkurrenceevne, at der arbejdes videre med forslaget på disse områder for at skabe mere klarhed. Det er vigtigt, at reguleringen ikke rammer skævt, for bredt eller bliver u håndterbar for virksomhederne, når den rammer virkeligheden.

**Finans Danmark** mener, at der kan forventes et løbende behov for at re-vurdere, hvilken kunstig intelligens der er højrisiko, da teknologien er under udvikling. Hvis ikke der etableres løbende justeringer, vil regulering sandsynligvis over tid komme til at ramme skævt i forhold til formålet om beskyttelse og innovation.

**Forbrugerrådet Tænk** mener, at definitionen af højrisiko kunstig intelligens ikke må være for snæver. Hvis begrebet fortolkes snævert, vil en masse kunstig intelligens-løsninger, som forbrugerne omgiver sig med hver eneste dag, falde uden for reglerne, og forbrugerbeskyttelsen vil alene skulle sikres gennem frivillige retningslinjer. Forbrugerrådet Tænk mener, at højrisiko kunstig intelligens også bør omfatte andre mulige skader eller ulemper hos forbrugeren såsom økonomisk tab eller økonomisk diskrimination samt købs- og fastholdelsesmanipulation. Forordningens krav om fysisk og psykisk skadevirkning bør derfor udvides.

**Forsikring & Pension** finder det positivt, at Kommissionen er gået bort fra at definere særlige sektorer som højrisikosektorer med høj regulering af al anvendelse af kunstig intelligens inden for den pågældende sektor til følge. Det giver bedre mening at fokusere på en risikobaseret tilgang til den konkrete anvendelse af kunstig intelligens og alene fokusere på at sætte rammer omkring højrisikooanvendelse for at sikre borgernes rettigheder,

hvor der er en reel risiko. Forsikring & Pension opfordrer til, at man fra dansk side bakker op om dette fremadrettet.

**IT-Branchen** byder opdelingen i risikokategorier velkommen, da det er med til at skabe klarhed. Samtidig bliver det afgørende, at listen over højrisiko kunstig intelligens med tiden ikke vokser sig lang og uoverskuelig. Man skal være helt skarpe på, at det kun er løsninger, hvor det er betydelig risiko for skade, ender med at falde i kategorien højrisiko kunstig intelligens. IT-Branchen mener, at der skal foreligge et klart mandat og kriterier, før listen kan udvides med nye områder - og først efter dialog med eksperter og virksomheder med branchekendskab.

*Overensstemmelsesvurdering af højrisiko kunstig intelligens, herunder udarbejdelse af standarder og fælles specifikationer*

**DE** bemærker, at der vil være behov for fælles standarder og specifikationer, der i dag ikke eksisterer, for at udføre overensstemmelsesvurderinger. Forslaget giver Kommissionen opgaven med at implementere disse. DE mener, det vil være bedre, hvis denne opgave blev løst i de regulatoriske sandkasser, da det vil være en ny tilgang til regulering af teknologi. Det vil samtidig give en mere permanent og veldefineret rolle til sandkasserne.

**DI** ser, at når det gælder de standarder, der skal gøre det muligt at opnå formodning om overensstemmelse med forslagets krav, vil Kommissionen udvikle mandater til brug for det europæiske standardiseringssystem. Samtidig vil forordningen finde anvendelse 30 måneder efter, at den er trådt i kraft. DI sætter spørgsmålstejn ved, om det er realistisk, at de nødvendige standarder er tilgængelige på det tidspunkt, samt om disse standarder også skal harmoniseres under sektorreguleringen eller alene under forordning om kunstig intelligens. Forslaget lægger op til, at overensstemmelsen med kravene skal foretages i forbindelse med udarbejdelse af overensstemmelsesvurderingen i sektorlovgivningen. Der er derfor behov for en nærmere analyse af, hvordan samspillet mellem denne forordning og den sektorspecifikke lovgivning skal fungere i praksis.

**DI og Dansk Standard** fremhæver, at der i forslaget lægges op til, at Kommissionen selv kan udvikle tekniske specifikationer, hvis standarder til brug for publicering ikke udvikles tilstrækkeligt hurtigt. Reelt betyder det, at Kommissionen får beføjelser til at udvikle detailregulering, som det ellers med NLF er formålet at undgå. Beføjelsen bør skrives ud af forslaget. Alternativt bør der stilles samme krav til udvikling af de tekniske specifikationer som i standardiseringsforordningen.

**Dansk Standard** finder det positivt, at Kommissionen lægger op til, at højrisiko kunstig intelligens håndteres med NLF-tilgangen og brug af CE-

mærkning med henholdsvis egne erklæringer og tredjepartserklæringer. Denne tilgang bør fastholdes.

**Dansk Standard** finder det positivt, at harmoniserede standarder er tiltænkt en vigtig rolle i forhold til at hjælpe virksomhederne med at overholde den nye lovgivning. Samtidig er det vigtigt, at myndigheder, som senere skal varetage markedsovervågning på området, har forståelse for det tekniske indhold i standarderne. Ligeledes kan det være en fordel, at de bemyndigede organer, som skal udføre tredjepartsvurderinger, får grundigt kendskab til de standarder, som de skal anvende.

**IT-Branchen** mener, at det kommer til at kræve betydelige administrative omkostninger for virksomhederne at skulle dokumentere og teste, at de lever op til reglerne inden for højrisikoområderne. Det bliver derfor afgørende, at danske og europæiske virksomheder kan forstå og agere ud fra lovgivningen, og at virksomhederne i videst muligt omfang ikke skal indsende samme dokumentation til flere instanser. Det kræver, at EU får skabt en fleksibel lovgivningsramme uden unødigt bureaukrati. Der kan med fordel fra national side oprettes støttefunktioner til at guide særligt de små og mellemstore virksomheder (SMV'erne).

**KL** finder det væsentligt, at ny regulering ikke påfører myndigheder bureaukrati i forhold til at implementere de kommende regler. Særligt kan der være opmærksomhed på at holde eventuelle dokumentationskrav på et minimum. Derudover fremhæver KL, at det bør anerkendes, at reguleringen introduceres på et område, hvor der allerede sker anvendelse af teknologien. Myndighederne, herunder kommunerne, bør således sikres en tilstrækkelig frist og fleksibilitet til at forholde sig til reguleringen, så man ikke sanktioneres for positive frontrunner indsats. Samtidig er det centralt, at kommunernes erfaringer med konkrete løsninger indarbejdes i standardiseringsarbejdet, således at de danske myndigheders erfaringer og den danske forvaltningstradition bliver repræsenteret i arbejdet.

#### Eksisterende lovgivning og NLF

**DI** støtter, at kravene vedrørende højrisikoanvendelsen i produkter bygger på principperne bag NLF. Visse steder bryder forslaget med NLF såsom Kommissionens mulighed for at udarbejde tekniske specifikationer samt kravet om, at udbyder skal monitorere regelefterlevelse af systemet gennem hele dets livscyklus. Sidstnævnte åbner desuden en række spørgsmål om deling af data, der kan påvirke fortrolighed og intellektuelle ejendomsrettigheder. DI opfordrer til, at man fra dansk side anmoder Kommissionen om at redegøre for uoverensstemmelser med NLF-grundlaget. DI mener, at man kun bør ændre på de grundlæggende principper bag NLF, hvis det er absolut nødvendigt, og DI savner argumenter, der begrundet denne gennemgribende ændring. Desuden vil Kommissionen som led i evaluering af

NLF undersøge, hvordan brug af nye teknologier påvirker NLF, hvorfor introduktion af ændringer i dette forslag forekommer præmaturligt.

**DI** fremhæver, at mange EU-initiativer påvirker produkter. Hvis regellevelse skal sikres på sigt, er det vigtigt at forholde sig til, hvordan de forskellige lovgivninger spiller sammen, så resultatet bliver en lovgivningsmæssig ramme, der fungerer for virksomhederne.

**Dansk Standard** fremhæver, at Kommissionens tilgang, der bygger på NLF og udarbejdelsen af standarder, er en væsentlig lettere metode for virksomhederne at efterleve samt vil være med til at skabe en agil regulering, da der løbende kan justeres via tekniske standarder. Det kan i den forbindelse være vigtigt at fastholde krav om rimelige overgangsordninger, således at virksomheder kan nå at omstille sig til nye krav.

**Dansk Standard** ser desuden positivt på, at for kunstig intelligens-komponenter, der allerede er en del af regulerede produkter med tredje-partsvurdering, bygges der videre på NLF-modellen med CE-mærkning. Der vil dog være udgifter forbundet med udvidelsen af tredjepartsvurderingerne. Samtidig bør det overvejes, hvad samspillet mellem lovgivninger kommer til at indebære, også i relation harmoniserede standarder.

#### Krav om forbrugerrettigheder

**Forbrugerrådet Tænk** savner, at der i regelsættet indgår forbrugerrettigheder, som forbrugerne kan gøre brug af, når de agerer med virksomheder og myndigheder, der anvender kunstig intelligens. Forslaget henvender sig i nuværende udformning først og fremmest til virksomhederne med rammer og krav, hvorimod forbrugerbeskyttelse som et grundelement og de rettigheder, der medfølger i den forbindelse, helt er udeladt. En forbruger bør eksempelvis kunne klage direkte til virksomheden, såfremt den er uenig i en algoritmisk afgørelse, ligesom muligheden for et menneskeligt tilsyn/revurdering bør sikres. Uanset at GDPR indeholder en bestemmelse om kunstig intelligens, bør en tilsvarende regel adresseres direkte i dette forslag.

#### Gennemsiglighedsforpligtelser for visse systemer

**Forbrugerrådet Tænk** mener, at der bør indgå et krav om, at kunstig intelligens-systemer rettet mod forbrugere skal deklareres.

**Forsikring & Pension** fremhæver, at der fastsættes krav om, at systemer, der skal interagere med mennesker, er designet på en måde, så det er tydeligt for personen, at det er et kunstig intelligens-system, der interageres med. I det omfang det måtte omfatte chatbots, henstilles det, at kravet ikke bliver unødvendigt bebyrdende.

### Foranstaltninger til støtte for innovation

**DE** støtter ideen om regulatoriske sandkasser for at give bedre vilkår for innovation. DE mener dog, at dette bør følges af medfinansiering fra EU-budgettet og andre incitamenter, så det sikres, at der på tværs af medlemsstaterne etableres et tilstrækkeligt antal sandkasser. Derudover ser DE positivt på forslagene om at understøtte SMV'erne. Dog bør der fastsættes en grænse, så de mindste virksomheder og iværksættere fritages helt for at betale gebyrer og lignende i forbindelse med forordningens krav.

### Forvaltning og gennemførelse

**Dansk Standard** mener, at det er vigtigt, at der indføres rimelige overgangsperioder, da der er lagt op til en ambitiøs lovgivning, der stiller store krav til virksomheder og myndigheders kompetencer og viden på området.

**Finans Danmark** støtter, at kommende tilsyn af den finansielle sektor vil skulle foretages af de reguleringsmyndigheder, som i dag har tilsynsforpligtelsen for de finansielle virksomheder. Hertil vil det være hensigtsmæssigt, hvis det for dette specifikke sektortilsyn blev muligt at anvende en mere risikobaseret tilgang, og at de finansielle tilsynsmyndigheder i højere grad kan fravige den firkantede højrisiko og lavrisiko tilgang.

**Finansforbundet** mener, at det i denne sammenhæng kan være på sin plads med en forordning, så der sikres en helt ensartet tilgang i EU til dette vigtige og komplicerede område. Det må dog sikres, at medlemsstaterne ikke hindres i at udvikle nationale tiltag for at understøtte forordningens regelsæt og intentioner. Finansforbundet fremhæver desuden, at meget kunstig intelligens-software, som anvendes af virksomheder i Danmark og andre europæiske lande, er udviklet uden for EU. Det sætter ekstra fokus på krav om overholdelse af danske og europæiske værdier i implementeringen.

**Forbrugerrådet Tænk** bemærker, at foruden klageadgang, er tilsyn og håndhævelse en afgørende forudsætning for reglernes effekt. Det er derfor vigtigt, at tilstrækkelige myndighedsressourcer og tidseffektiv behandling af forbrugerklager ikke mindst over for globale teknologivirksomheder sikres bedre, end tilfældet er i dag efter databeskyttelsesreglerne/GDPR.

**IT-Branchen** noterer, at implementeringen af forslaget er henlagt til medlemslandene. Det bliver afgørende, at der kommer ensartede nationale afgørelser i alle medlemslande, og at der ikke skabes smuthuller og gråzoner ud fra nationale hensyn. IT-Branchen stiller spørgsmål ved, om medlemslandene er gearret til denne nye opgave, og hvilke(n) instans(er) der skal varetage opgaven. Det kommer til at kræve stor ekspertise i medlemslandene at varetage denne opgave, blandt andet da anvendelsesområderne udvikler sig over tid. Dette gør den administrative opgave med den fortløbende kontrol og regulering ekstremt tung. IT-Branchen er bekymret for,

om alle medlemslandene har de nødvendige kompetencer, og om den uklare nationale implementering kan skabe øget usikkerhed for virksomheder på det europæiske marked.

**KL** mener, at en god og effektiv implementering kræver viden og støtte. Det er vigtigt, at forordningen skaber klarhed over, hvilke regler og fortolkninger der gælder. Med erfaring fra tidligere forordninger anbefales det, at der bliver krav om støtte til myndigheder i form af hurtig hjælp til afklaring af eventuelle spørgsmål, der følger af forordningen. På samme måde er det centralt, at leverandører af løsninger forpligtes til at sikre overholdelse af reglerne i de løsninger, som de udbyder. Dermed vil de formentlig have samme behov for grundig regelindføring og -afklaring.

**KL** mener, at der er brug for vejledning og konkrete værktøjer til at understøtte reguleringen, og at disse skal være på plads inden reglerne træder i kraft, så virksomheder og myndigheder kan sikre overensstemmelse med lovgivningen uden overimplementering eller unødigt bureaukratisk dokumentation. Der bør afsættes finansiering til arbejdet med disse aktiviteter.

#### Etablering af det europæiske udvalg for kunstig intelligens

**DE** mener, at relevante interessenter skal inddrages i møderne i det europæiske udvalg for kunstig intelligens.

**DI** mener, at udvalget ikke alene skal følge implementeringen af den nye regulering for at sikre en gnidningsfri implementering, men også tage ansvaret på sig for at sikre, at implementeringen af reguleringen understøtter EU's ambitioner om at tage ny teknologi i brug til innovation, vækst og for at skabe et bedre samfund. At skabe en god balance mellem at tage ny teknologi i brug og at beskytte samfundet mod en u hensigtsmæssig udvikling bør være en formel og prioriteret opgave for det foreslåede europæiske udvalg for kunstig intelligens.

#### Sanktioner

**DE** mener, at bødestørrelsen for brud på artikel 5 vedrørende forbudte anvendelser virker unødvendigt højt. Det lægger to procentpoint oveni rammen fra GDPR og kan være en medvirkende faktor til, at virksomheder helt fravælger at udvikle og levere kunstig intelligens til skade for europæisk vækst og innovation.

**Forsikring & Pension** noterer, at forslaget anvender et bøderegime, der kendes fra konkurrenceretten og GDPR. Der stilles dog spørgsmålstejn ved proportionaliteten i det foreslåede bødeniveau, der umiddelbart virker voldsomt højt.



**KL** mener, at det er vanskeligt at vurdere, hvilke sanktioner der vil blive gennemført, såfremt forpligtelserne ikke overholdes. Som ved GDPR er KL meget kritisk over for eventuelle økonomiske sanktioner til offentlige myndigheder.

#### Adfærdskodeks

**DE** bakker generelt op om initiativer båret af frivillighed, der kan bruges til at promovere en ansvarlig tilgang til digitalisering, herunder kunstig intelligens. Her bør Danmark søge at integrere eksisterende indsatser, eksempelvis den danske mærkningsordning D-mærket, og eventuelt bruge forordningen som en løftestang for at udbrede mærket til resten af EU.

**DI** fremhæver, at reguleringen ikke kommer til at finde anvendelse på en lang række anvendelser af kunstig intelligens, men derfor skal virksomheder ikke lade være med at tage ansvar. DI ser, at den danske mærkningsordning D-mærket vil være et godt eksempel på et adfærdskodeks for kunstig intelligens, der ikke er kategoriseret som højrisiko. DI opfordrer til, at der fra dansk side arbejdes for, at D-mærket anerkendes som et adfærdskodeks for anvendelse af kunstig intelligens, der ikke reguleres som højrisiko.

**Finans Danmark** mener, at den skarpe binære sondring mellem høj risiko og lav risiko sammenholdt med adgangen til frivilligt at underlægge sig højrisikoregulering sandsynligvis vil risikere ikke at have den ønskede virkning. Finans Danmarks vurderer, at en mere differentieret og risikobaseret tilgang til reguleringen i højere grad vil styrke virksomhedernes interesse for frivilligt at efterleve kravene i den nye regulering.

**Finansforbundet** støtter udvikling af adfærdskodekser som et vigtigt supplement til forordningens regler og intentioner. Det er samtidig vigtigt, at tilsynsmyndigheder mv. sættes i stand til at anvende disse kodekser proaktivt, uden at området udvikler sig i omfang og kompleksitet på samme måde som eksempelvis GDPR. Det er vigtigt, at tiltagene kan være effektivt retningsgivende og eksempelvis facilitere transparente rapporteringer.

#### Delegerede retsakter

**DE** bemærker, at forslaget i vid udstrækning åbner for brug af delegerede retsakter, hvilket øger usikkerheden for de virksomheder, som lovgivningen rammer. DE er generelt af den holdning, at delegerede retsakter bør anvendes mindst muligt.

**DI** bemærker, at forordningen lægger op til, at de nærmere krav til monitoreringen af regelefterlevelsen skal ske i form af en delegeret retsakt. DI har brug for mere tid til at tage stilling til, om dette er den mest hensigtsmæssige løsning, skulle kravet blive fastholdt.

## 9. Generelle forventninger til andre landes holdninger

I Rådet færdiggjorde man under det slovenske formandskab i andet halvår af 2021 den første artikelgennemgang af forslaget. Det slovenske formandskab fremlagde en fremskridtsrapport på telerådsmødet den 3. december 2021, som identificerede en række elementer, der krævede yderligere drøftelse, herunder højrisikokrav, aktørforpligtelser, håndhævelse samt samspil med eksisterende lovgivning.

Det franske formandskab satte ambitiøst fra start i første halvår af 2022 og afsluttede den anden artikelgennemgang, og fremsatte en fremskridtsrapport på telerådsmødet den 3. juni 2022.

Det tjekkiske formandskab har arbejdet målrettet og effektivt efter at opnå en generel indstilling til telerådsmødet i december 2022. Der er udarbejdet en balanceret kompromistekst, og det er forventningen, at alle medlemslande vil kunne støtte den generelle indstilling på telerådsmødet den 6. december 2022. Fra dansk side kan den generelle indstilling støttes, da danske prioriteter såsom indsnævring af definitionen og klarlægning af højrisikoklassificeringen er blevet efterkommet. Det samme gælder ift. fleksibilitet til at indrette regulatoriske sandkasser og medlemsstaternes innovationsstøttende tiltag.

## 10. Regeringens generelle holdning

Regeringen mener, at digitaliseringen skal tjene samfundets interesser ved, at digitalisering bidrager til at adressere samfundets udfordringer, mens etisk, ansvarlig og sikker digitalisering går hånd i hånd med digital vækst. På den baggrund støtter regeringen ambitionen om at skabe et velfungerende indre marked for etisk, ansvarlig og sikker kunstig intelligens.

Regeringen arbejder for, at den digitale økonomi i Europa generelt kendetegnes ved et højt niveau af tillid og tryghed samt en stærk digital konkurrenceevne baseret på innovationsfremmende og teknologineutrale rammevilkår, hvor gevinsterne ved regulering står mål med administrative og økonomiske omkostninger for virksomhederne.

Regeringen anser kunstig intelligens som en af de afgørende teknologier til at understøtte EU's konkurrenceevne, velstand, grønne omstilling samt den offentlige forvaltning. Regeringen anerkender imidlertid, at anvendelsen af kunstig intelligens kan indebære en række risici, der kan underminere en etisk, ansvarlig og sikker anvendelse af kunstig intelligens.

Regeringen støtter, at risiciene ved kunstig intelligens adresseres i en europæisk lovgivningsramme. Regeringen finder det centralt, at der med forslaget opnås en ansvarlig og etisk anvendelse af kunstig intelligens-løsninger og dataene bag disse.

Regeringen finder det vigtigt, at den europæiske lovgivningsramme følger en risikobaseret, teknologineutral og proportionel tilgang, hvor graden af forpligtelser følger graden af mulig skadevirkning. På den baggrund finder regeringen det vigtigt at opnå en klar, principbaseret og operationel lovgivningsramme, der sikrer borgernes og forbrugernes tillid og øger beskyttelsen i samfundet, uden at dette unødigt hæmmer innovationsevnen eller forringer konkurrenceevnen. Regeringen finder det derfor vigtigt, at der findes den rette balance, hvor risici adresseres, samtidig med at teknologien kan udvikles og anvendes til gavn for vores samfund samt understøtte fremtidens arbejdspladser og offentlige forvaltning. Regeringen finder det vigtigt, at der stilles krav til datakvaliteten i udvikling af højrisiko kunstig intelligens-systemer.

I den henseende finder regeringen det centralt, at forordningen ligger inden for rammerne af eksisterende kompetencefordeling, herunder for så vidt angår national sikkerhed

Regeringen finder det centralt, at forordningen ligger inden for rammerne af eksisterende lovgivning, herunder GDPR og produktlovgivningen. Det bemærkes, at de eksisterende regler i GDPR tilvejebringer en beskyttelse af personoplysninger. Borgere og forbrugere (registrerede) vil således efter de eksisterende databeskyttelsesregler kunne klage til Datatilsynet over en behandling af deres personoplysninger. Herudover vil borgere og forbrugere (registrerede) kunne tilbagetrække sit samtykke i de tilfælde, hvor samtykke udgør grundlaget for databehandling. Regeringen finder det vigtigt, at der sikres klarhed i forhold til samspillet mellem AI-forordningens bestemmelser om personoplysninger og de generelle regler i GDPR, og at dobbeltregulering så vidt muligt undgås.

Regeringen finder det vigtigt, at der anlægges en principbaseret tilgang, der efterlader et vist manøvrerum til den specifikke tekniske løsning, samt at der bl.a. gives mulighed for anvendelsen af harmoniserede standarder (f.eks. ift. forpligtelser om data og datahåndtering, hvor standardisering giver mulighed for kvalitetssikring). Hertil finder regeringen det vigtigt, at der stilles krav til datakvaliteten i udvikling af højrisiko kunstig intelligens-systemer. En principbaseret tilgang forudsætter dog udarbejdelse af vejledning på europæisk plan samt udarbejdelse af standarder, inden forordningen finder anvendelse, hvilket regeringen finder vigtigt.

Regeringen finder det centralt, at centrale begreber i forslaget klarlægges og afgrænses, herunder definitionen af kunstig intelligens samt kategoriseringen af højrisiko kunstig intelligens. Det er vigtigt, at definitionen af kunstig intelligens er klar og kun omfatter det, der reelt udgør kunstig intelligens.

Kategorien af højrisiko kunstig intelligens bør klart afgrænses til anvendelser, der reelt kan medføre betydelig og svært genoprettelig skade. En potentiel, fremtidig udbygning af højrisikokategorien skal ske på grundlag af en konkret risikovurdering samt klare og forudsigelige kriterier. I den henseende finder regeringen det vigtigt, at højrisikoanvendelserne afgrænses til de anvendelser, der kan være ugunstige for de påvirkede aktører, herunder borgere og forbrugere, og arbejder for, at efterlevelseseomkostninger står mål med gevinsterne ved regulering.

Regeringen bakker op om forbud af specifikke anvendelser af kunstig intelligens, hvor anvendelsen kan resultere i alvorlig, uoprettelig skade for individer eller samfundet eller er uforenelig med gældende lovgivning eller rettigheder, samt hvor dette ikke kan adresseres på anden vis.

I forlængelse heraf mener regeringen, at retshåndhævende myndigheders brug af biometrisk fjernidentificering i realtid på offentlige steder i visse situationer, kan retfærdiggøres. Det må dog hverken resultere i generel overvågning eller undergravning af grundlæggende rettigheder såvel som eksisterende lovgivning. Det bemærkes dog, at forordningens regler om retshåndhævende myndigheders brug af biometrisk fjernidentifikation i realtid på offentligt tilgængelige steder er omfattet af retsforbeholdet, og Danmark er således ikke bundet heraf.

Regeringen støtter forudgående overensstemmelsesvurderinger til at sikre efterlevelse af højrisikokravene. I den forbindelse ser regeringen positivt på Kommissionens forslag, der blandt andet tager højde for eksisterende lovgivning og kombinerer forskellige procedurer, herunder både intern og tredjepartskontrol. Regeringen arbejder imidlertid for, at efterlevelseseomkostninger, herunder de administrative omkostninger, står mål med gevinsterne ved reguleringen. Samtidig er det vigtigt, at der sikres effektive efterlevelsese procedurer, herunder tilstrækkelig kapacitet samt kompetencer til at certificere den omfattede kunstig intelligens effektivt.

Regeringen støtter enkle gennemsigtighedsforpligtelser for visse anvendelser af kunstig intelligens. Målet om gennemsigtighed skal dog give merværdi, og regeringen finder det vigtigt, at de omfattede anvendelser af kunstig intelligens klarlægges, og at gennemsigtighedsforpligtelserne er pro-

portionelle og ikke skaber modsatrettede hensyn i forhold til grundlæggende rettigheder, da kunstig intelligens kan anvendes til at redigere indhold som led i udøvelsen af informations- og ytringsfrihed.

Da det overordnede mål er at styrke etisk, ansvarlig og sikker kunstig intelligens, støtter regeringen udformningen af frivillige adfærdskodeks, der kan blive et konkurrenceparameter for danske og europæiske virksomheder. Regeringen arbejder for, at der bør være forskel på højrisiko kravene og kravene i adfærdskodeks, da al kunstig intelligens ellers de facto vil være underlagt de skærpede højrisikokrav. Frivillige adfærdskodeks kan være et indledende skridt mod en europæisk frivillig mærkningsordning for kunstig intelligens, som regeringen fortsat vil arbejde for.

Regeringen finder det vigtigt, at forvaltningen og håndhævelsen foregår nationalt, hvor der bygges på eksisterende, nationale strukturer, der sikrer en effektiv databeskyttelse og forbrugerbeskyttelse. I den henseende arbejder regeringen for, at medlemslandene bevarer retten til at fastlægge den nationale organisering. Regeringen finder det vigtigt, at forslaget ikke pålægger medlemslandene unødige statsfinansielle omkostninger, og at gevinsterne ved forslaget står mål med de administrative omkostninger. Derudover vil regeringen fremhæve behovet for et europæisk tilsyn til at håndtere sager af en vis størrelse eller grænseoverskridende karakter.

I forlængelse heraf bakker regeringen op om etablering af et europæisk udvalg for kunstig intelligens, der skal sikre effektiv og ensartet håndhævelse af de nye regler på tværs af grænserne.

Regeringen mener, at effektiv håndhævelse er vigtigt, hvis målet om at udvikle og anvende etisk, ansvarlig og sikker kunstig intelligens skal nås. Regeringen støtter derfor indførelsen af effektive og passende sanktioner, herunder bøder. I samme ombæring finder regeringen det vigtigt, at det nuværende hensyn til medlemslandenes forskellige juridiske systemer bevares.

Som udgangspunkt er regeringen skeptisk over for Kommissionens forslag om delegerede retsakter. I den forbindelse arbejder regeringen for, at anvendelsesområdet for potentielle, følgende retsakter med betydning for lovgivningsmæssige og økonomiske konsekvenser klart afgrænses.

Regeringen støtter initiativer, der kan fremme innovationskraften inden for kunstig intelligens, herunder etableringen af effektive og fleksible rammer for regulatoriske sandkasser. Disse kan blandt andet understøtte de små og mellemstore virksomheders efterlevelse af kravene og deraf bidrage til at understøtte udviklingen af kunstig intelligens.

## **11. Tidligere forelæggelse for Folketingets Europaudvalg**

Forslaget blev forelagt Folketingets Europaudvalg til forhandlingsoplæg den 3. juni 2022.

Forslaget har desuden været forelagt Folketingets Europaudvalg til orientering den 23. september 2021 i forbindelse med forelæggelsen af konkurrenceevnerådsmødet, den 25. november 2021 i forbindelse med forelæggelsen af telekommunikationsrådsmødet d. 2. december og den 19. maj i forbindelse med telekommunikationsrådsmøderne, samt til skriftlig orientering den 1. oktober 2021 i forbindelse med det uformelle telekommunikationsrådsmøde d. 14. oktober 2021. Der blev oversendt grund- og nærhedsnotat den 28. juni 2021.

## **EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om harmoniserede regler om fair adgang til og anvendelse af data (dataforordningen) KOM (2022) 68**

*Revideret udgave af Grund- og Nærhedsnotatet oversendt d. 11. april 2022  
Ændringer markeret med streg i venstre side.*

### **1. Resumé**

Formålet med dagsordenspunktet på rådsmødet er at drøfte fremskridtsrapporten for dataforordningen for at få en politisk pejling på forslaget, hvilket man fra dansk side kan støtte.

Europa-Kommissionen ('Kommissionen') præsenterede den 23. februar 2022 "The Data Act" (dataforordningen). Forordningen lanceres som den anden retsakt på baggrund af Kommissionens datastrategi, der blev fremsat i februar 2020.

Forslaget har til formål at fremme adgangen til og anvendelsen af data, samt at sikre retfærdighed i fordelingen af den værdi, der hidrører fra data, herunder adressere techgiganters datamonopol. Forslagets hovedelementer er (1) regler der skal gøre data, der er genereret ved brug af et produkt eller en relateret tjeneste ('Internet of Things-produkter og tjenester'), tilgængelige for brugeren; (2) horisontale rammer for dataindehavere, hvor disse er retligt forpligtede til at stille data til rådighed; (3) horisontale rammer, der skal beskytte mikrovirksomheder og SMV'er mod urimelige aftalevilkår i forbindelse med datadeling; (4) en harmoniseret ramme for offentlig myndigheders eller for EU's institutioners, agenturers og organers adgang til og anvendelse af virksomhedsdata, ved tilfælde af ekstraordinært behov; (5) krav, der skal give brugere af databehandlingstjenester mulighed for at skifte udbyder; (6) tiltag til beskyttelse mod tredjeparters ulovlige adgang til ikke-persondata i EU.

Regeringen støtter ambitionen om at øge adgangen til og anvendelsen af data og sikre en mere retfærdig fordeling af data, herunder adressere techgiganters datamonopol. Regeringen anser adgangen til og anvendelsen af data som et væsentligt fundament for udviklingen af digitale teknologier og tjenester, der kan fremme vækst og innovation, og som derigennem kan bidrage til genopretningen af økonomien og til at løse klimaudfordringen. Regeringen mener, at digitaliseringen skal tjene samfundets interesser ved, at digitalisering bidrager til at adressere samfundets udfordringer, mens etisk, ansvarlig og sikker digitalisering går hånd i hånd med digital vækst.

Regeringen finder det vigtigt, at forordningens initiativer understøtter en effektiv, ansvarlig og sikker adgang til og anvendelse af data, som skaber reel værdi for borgere og virksomheder. Regeringen mener, at virksomheders datadeling og -anvendelse skal fremmes gennem etablering af klare, forståelige og horisontale rammer for datadeling, samt gennem øget interoperabilitet mellem tjenester og decentraliseret dataudveksling.

Regeringen finder det essentielt, at offentlige myndigheders ret til at tilgå virksomhedsdata til samfundsmæssige formål skal afgrænses på baggrund af en klar definition af, hvad der udgør en offentlig nødsituation. Endvidere mener regeringen, at offentlige myndigheders adgang til virksomhedsdata på tværs grænser skal gå igennem de nationale myndigheder i etableringslandet.

Regeringen ser positivt på etablering af horisontale rammer til at beskytte mikrovirksomheder og SMV'er mod urimelige aftalevilkår i forbindelse med datadeling, samt på at brugere af Internet of Things-produkter og -tjenester får adgangsret til data. Regeringen støtter desuden hensigten om at fremme en effektiv flytning af data mellem cloudtjenester, og at de tekniske udfordringer søges håndteret gennem fælles standarder og formater.

Regeringen finder, at dataøkonomien er grænseoverskridende af natur, hvorfor tiltag til at fremme den europæiske dataøkonomi skal fungere i den globale økonomi og respektere internationale samarbejdspartnere og handelsaftaler.

Regeringen vurderer, at der vil være lovgivningsmæssige og økonomiske konsekvenser.

| Sagen forelægges til orientering.

## 2. **Baggrund**

Kommissionen har den 23. februar 2022 fremsendt forslag om dataforordningen (KOM (2022) 68). Forslaget er oversendt til Rådet den 21. marts 2022 i dansk sprogversion. Forslaget er fremsat med hjemmel i TEUF artikel 114. Forslaget skal vedtages af Rådet og Europa-Parlamentet efter den almindelige lovgivningsprocedure, jf. traktatens artikel 294. Rådet træffer afgørelse med kvalificeret flertal.

Baggrunden for forslaget er den digitale pakke, som Kommissionen fremsatte i februar 2020, herunder særligt ”En europæisk strategi for data” (jf. grund- og nærhedsnotat oversendt til FEU d. 27. marts 2020). Kommissionens datastrategi beskriver retningen, formålet med og processen for initiativer for data i perioden 2020-2025. Heraf fremgår det, at Kommissionen vil understøtte et



indre marked for data gennem fælles regler for dataadgang og dataanvendelse og undersøge, under hvilke omstændigheder, virksomheder, offentlige myndigheder og borgere kan og bør dele data. Strategien lægger op til investeringer i fælles europæiske dataområder og sammenslutning af cloudinfrastrukturer, som skal nedbryde juridiske og tekniske barrierer for datadeling, samt understøtte sikker datadeling i EU.

Datastyringsforordningen blev fremsat som den første retsakt med afsæt i datastrategien, og har til formål at øge tilgængeligheden af data ved dels at styrke tilliden til datadelingstjenester og dels at indføre nye datadelingsmekanismer på tværs af EU. Rådet, Kommissionen og Europa-Parlamentet nåede til enighed om forordningen den 30. november 2021.

Kommissionen har den 15. november fremsat forslag om en retsakt om digitale markeder, der har til formål at sikre åbne og retfærdige digitale markeder i de tilfælde, hvor digitale platforme fungerer som såkaldte "gatekeepers". Med gatekeepers forstås platforme, som i høj grad påvirker rammer og regler for både forbrugervalg og konkurrencen på de dele af markedet, hvor platformene er kontrollerende. Rådet og Europa-Parlamentet nåede til enighed om forordningen den 24. marts 2022.

Dataforordningen er den anden retsakt, som er blevet fremsat med afsæt i Kommissionens datastrategi.

### **3. Formål og indhold**

Der ventes på rådsmødet en drøftelse af formandskabets fremskridtsrapport med henblik på at få politisk pejling på forslaget.

Dataforordningens formål er at fremme adgangen til og anvendelsen af data, samt at sikre retfærdighed i fordelingen af den værdi, der hidrører fra data. Forordningen skal give bedre adgang til data for forbrugere og virksomheder, adressere techgiganters datamonopol, samt sikre at offentlige myndigheder og EU's institutioner, agenturer og organer kan anvende virksomhedsdata i tilfælde af et ekstraordinært behov.

Derudover skal forslaget facilitere et lettere skift mellem databehandlingstjenester, såsom cloud og edgetjenester, og indføre sikkerhedsbeskyttelsesforanstaltninger mod ulovlig dataadgang ved opbevaring af ikke-persondata hos databehandlingstjenester. Endelig skal forordningen facilitere udarbejdelse af interoperabilitetsstandarder for, at data kan genanvendes på tværs af sektorer.

#### Kap. 1: Anvendelsesområde og definitioner

Forslagets kapitel 1 indeholder generelle bestemmelser, herunder om forordningens genstandsfelt og anvendelsesområde. Forordningen skal finde anvendelse på:

- a) producenter af produkter og leverandører af relaterede tjenester, som markedsføres i EU og brugerne af sådanne produkter og tjenester
- b) dataindehavere, der stiller data til rådighed for datamodtagere i EU
- c) datamodtagere i EU, som dataene stilles til rådighed for
- d) offentlige myndigheder og EU's institutioner, agenturer og organer
- e) udbydere af databehandlingstjenester, der tilbyder databehandling i EU.

Forslaget berører ikke forordning (EU) 2016/679 (persondataforordningen) og direktiv 2002/58/EF (e-databeskyttelsesdirektivet), men bestemmelser i denne forordning supplerer retten til dataportabilitet i henhold til artikel 20 i persondataforordningen. Forslaget berører ikke EU-retsakter, nationale retsakter og internationalt samarbejde om udveksling af, adgang til og anvendelse af data med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger.

## Kap. 2: Datadeling mellem virksomheder og forbrugere og mellem virksomheder

Kapitlet giver forbrugere og virksomheder ret til at få adgang til og anvende data, der genereres af de produkter eller relaterede tjenester, de ejer, lejer eller leaser.

Kommissionen foreslår at forpligte producenter og leverandører af Internet of Things-genstande (IoT-genstande) til at udforme produkter og relaterede tjenester på en måde, der som standard gør data let tilgængelige for brugeren. Hvor brugerens direkte adgang til data ikke er mulig, skal dataindehavere stille data gratis til rådighed på baggrund af en simpel anmodning.

Dertil indføres gennemsigtighedsforpligtelser, hvormed brugeren, inden der indgås en aftale, skal oplyses om, bl.a. hvordan data kan tilgås, hvorvidt producenten eller andre vil bruge data, samt mulighederne for klageadgang.

Dataindehaveres ret til at anvende ikke-persondata, som genereres ved brug af et produkt eller relateret tjeneste, begrænses, idet en sådan anvendelse skal ske på grundlag af en kontrakt med brugeren.

Derudover foreslår Kommissionen, at brugere skal have ret til at dele IoT-genereret data med tredjeparter, hvormed dataindehaveren forpligtes til at stille data gratis til rådighed til tredjeparter på brugerens anmodning. Hensigten er, at forbrugere og erhvervsbrugere, der anvender IoT-produkter, skal kunne drage fordel af andre reparations- og vedligeholdelsestjenester end producentens, samt få mulighed for at få analyseret og behandlet deres data.

Der lægges herudover op til at kravene til producenter af IoT-produkter og dataindehavere af IoT-data er omfattet af forordningen, hvis de udbyder tjenester i EU eller stiller data til rådighed i EU. Samtidig lægges der op til, at det vil være nationale myndigheder, der håndhæver hele forordningen. Som udgangspunkt udpeges/etableres en kompetent myndighed for dataforordningen, der skal håndhæve stort set hele forslaget inkl. krav til dataindehavere overfor danske forbrugere eller virksomheder (enkelte aspekter af kapitlet fsva. persondata skal dog håndhæves af datatilsynet).

Der indføres en undtagelse om, at virksomheder, der er blevet udpeget som gatekeepere i henhold til forslaget om en retsakt om digitale markeder, ikke må være tredjepart i henhold til dataforordningen. Gatekeepers må dermed ikke modtage IoT-genereret data fra en bruger, eller anmode eller kommercielt tilskynde brugere til at give adgang til sådanne data. Berettigede tredjeparter må endvidere ikke stille data til rådighed for gatekeepers.

Hverken brugere eller tredjeparter må anvende data til at udvikle et produkt, der konkurrerer med det produkt, som data stammer fra. Endvidere skal der træffes de nødvendige foranstaltninger for at beskytte forretningshemmeligheder.

Der indføres derudover en række begrænsninger for tredjeparter angående deres anvendelse af data og samarbejde med brugeren.

Endelig foreslår Kommissionen, at forpligtelser i kapitel 2 ikke skal finde anvendelse for data genereret ved brug af produkter eller relaterede tjenester, der fremstilles eller leveres af virksomheder, der betragtes som mikrovirksomheder eller små virksomheder som defineret i artikel 2 i bilaget til henstilling 2003/361/EF (Kommissionens henstilling om definitionen af mikrovirksomheder, små og mellemstore virksomheder).

### Kap. 3: Forpligtelser for dataindehavere, der er retligt forpligtede til at stille data til rådighed

Kapitlet fastlægger horisontale rammer for dataindehavere, hvor disse er retligt forpligtede til at stille data til rådighed i henhold til fremtidig lovgivning, samt i henhold til kapitel 2 i forordningen.

Der opstilles en række betingelser for dataindehavere, hvor de på baggrund af en retlig forpligtelse skal stille data til rådighed:

- (a) data skal stilles til rådighed på fair, rimelige og ikke diskriminerende vilkår og på en gennemsigtig måde
- (b) vilkår for at stille data til rådighed skal aftales mellem dataindehaver og datamodtager

- (c) dataindehaver må ikke diskriminere mellem sammenlignelige kategorier af datamodtagere. Dataindehaver har bevisbyrden, såfremt denne anklages for at diskriminere
- (d) en dataindehaver må ikke stille data til rådighed med eneret for en datamodtager
- (e) dataholdere og datamodtagere kan ikke kræves at skulle give yderligere information end, hvad er strengt nødvendigt for at bekræfte overholdelse af de aftalte kontraktlige vilkår
- (f) medmindre andet angives i EU-lov, kan en forpligtelse om at stille data til rådighed til en datamodtager ikke medføre en forpligtelse til at videregive forretningshemmeligheder.

Kommissionen foreslår at dataindehavere, der er retligt forpligtede til at stille data til rådighed, kan kræve godtgørelse derfor. I den forbindelse skal enhver godtgørelse, der aftales mellem dataindehaver og datamodtager være rimelig, og dataindehaveren skal derfor oplyse datamodtageren grundlaget for beregningen af godtgørelsen. Når datamodtageren er en mikrovirksomhed eller en SMV, må den aftalte godtgørelse ikke overstige de omkostninger, der er direkte forbundet med at stille data til rådighed for datamodtageren. Endelig er bestemmelserne ikke til hinder for, at der i fremtidig lovgivning fastsættes lavere kompensationsmuligheder eller indføres krav, der ekskluderer dataholders mulighed for at kræve godtgørelse.

Medlemsstaterne skal ifølge forslaget certificere et tvistbilægningsorgan, der kan bilægge tvister mellem dataindehaver og datamodtager angående fastsættelsen af fair, rimelige og ikke-diskriminerende vilkår for dataadgang. Tvistbilæggelsesorganets afgørelser skal kun være bindende for parterne, hvis de udtrykkeligt har samtykket til den bindende karakter forud for mæglingen.

Endelig indføres bestemmelser, der giver dataholder mulighed for at anvende tekniske beskyttelsesforanstaltninger til at forebygge uautoriseret adgang til data og for at sikre overholdelse af forordningens øvrige bestemmelser.

#### Kap. 4: urimelige vilkår vedrørende dataadgang og -anvendelse mellem virksomheder

Kapitlet indfører horisontale rammer, der skal beskytte mikrovirksomheder og SMV'er mod urimelige aftalevilkår i forbindelse med datadeling. Formålet er at forebygge situationer, hvor en part udnytter et skævt magtbalanceforhold, når der indgås kontrakter om dataadgang og -anvendelse.

Det foreslås, at kontraktlige vilkår indgået om adgangen til og brugen af data ikke skal være bindende for mikrovirksomheder og SMV'er, hvis disse vilkår

er urimelige, og hvis de er ensidigt påtvunget af den anden part. Hvis det urimelige aftalevilkår kan adskilles fra de øvrige aftalevilkår, forbliver disse øvrige vilkår bindende.

Reglerne for urimelige vilkår skal kun gælde de elementer af en kontrakt, som er relateret til at stille data til rådighed. Andre dele af samme kontrakt vil ikke være underlagt reglerne i forordningen. Derudover finder reglerne ikke anvendelse for aftalevilkår om den pris, der skal betales.

Kap. 5: Tilrådighedsstillelse af data for offentlige myndigheder og unionens institutioner, agenturer eller organer på grundlag af et ekstraordinært behov  
Kapitlet vedrører fastlæggelsen af en harmoniseret ramme for offentlig myndigheders eller for EU's institutioners, agenturers og organers (herefter 'offentlige myndigheder') adgang til og anvendelse af virksomhedsdata, ved tilfælde af et ekstraordinært behov.

Kapitlet finder ikke anvendelse for virksomheder, der betragtes som mikrovirksomheder eller små virksomheder.

Kommissionen foreslår, at dataindehavere efter anmodning skal stille data til rådighed for en offentlig myndighed, hos hvilken der foreligger et ekstraordinært behov for at anvende de ønskede data.

Et ekstraordinært behov for data anses for at foreligge under følgende omstændigheder:

- (a) de data, der anmodes om, er nødvendige for at reagere på en offentlig nødsituation
- (b) dataanmodningen er begrænset i tid og omfang og er nødvendig for at forebygge eller bidrage til genopretningen efter en offentlig nødsituation
- (c) manglen på tilgængelige data forhindrer den offentlige myndighed i at udføre en specifik opgave i offentlighedens interesse, som udtrykkeligt er fastsat ved lov, og hvor
  - (1) den offentlige myndighed ikke har været i stand til at indhente sådanne data på alternative måder, og vedtagelsen af nye lovgivningsmæssige foranstaltninger ikke kan sikre rettidig tilgængelighed, eller
  - (2) indhentningen af data i væsentlig grad mindsker den administrative byrde for dataindehaveren eller andre virksomheder.

Der foreslås rammer for offentlige myndigheders anmodninger om at få data stillet til rådighed, der bl.a. stiller krav til at påvise det ekstraordinære behov, og til at præcisere hvilke data og hvordan de skal stilles til rådighed, samt at

anmodninger skal stå i et rimeligt formål til behovet. Anmodninger skal så vidt muligt vedrøre ikke-persondata.

Hvis en af EU's institutioner eller en offentlig myndighed i et medlemsland vil anmode om data fra en dataindehaver etableret i en anden medlemsstat, skal denne først underrette den kompetente myndighed for dataforordningen i den pågældende medlemsstat og tage højde for den kompetente myndigheds rådgivning om behov for samarbejde med nationale myndigheder med henblik på at mindske den administrative byrde for dataindehaveren.

Der stilles krav til de offentlige myndigheders anvendelse af data, herunder, at anvendelse skal være forenelig med formålet for anmodningen, og at data skal destrueres efterfølgende. Data kan deles med enkeltpersoner eller organisationer med henblik på at udføre videnskabelig forskning eller analyse, der er forenelig med det angivne formål, samt udarbejdelse af officielle statistikker.

Der foreslås rammer for dataindehaverens efterlevelse af anmodninger og mulighed for at afslå eller anmode om ændringer til anmodningen om tilrådighedsstillelse.

Dataindehavere har ikke krav på at få godtgørelse for data, der stilles til rådighed for at reagere på en offentlig nødsituation. Dataindehavere kan kræve godtgørelse for at efterkomme anmodninger om data baseret på de øvrige kategorier af ekstraordinært behov. Godtgørelsen kan ikke overstige de omkostninger, der er afholdt for at efterkomme anmodningen plus en rimelig margin, og dataindehaver skal fremlægge oplysninger om beregningen deraf.

I forslaget anføres, at dataforordningens bestemmelser om at stille data til rådighed for offentlige myndigheder ikke berører de forpligtelser om at stille data til rådighed for offentlige myndigheder, der er fastsat i anden europæisk eller national lovgivning.

Offentlige myndigheders rettigheder i kapitel 5 må endvidere ikke udøves med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af strafferetlige eller administrative overtrædelser eller fuldbyrdelse af strafferetlige sanktioner eller told- og skatteforvaltning.

#### Kap. 6: Skift mellem databehandlingstjenester

Kapitlet introducerer minimumskrav for databehandlingstjenester, såsom cloud- og edgetjenester med henblik på at give brugere af tjenesterne mulighed for at skifte udbyder.

Kommissionen foreslår, at udbydere af databehandlingstjenester skal fjerne handelsmæssige, tekniske, kontraktmæssige og organisatoriske hindringer for, at deres brugere effektivt kan skifte fra én udbyder til en anden. Det indebærer, at brugere skal kunne flytte alle deres data og digitale aktiver, samt afslutte deres kontrakt med 30 dages varsel.

Udbyderene forpligtes til at tilbyde al den bistand og støtte, der er nødvendig for et vellykket skifte. Derved skal brugere efter et skift kunne opretholde et minimum af funktionalitet, når de anvender den nye tjeneste, hvis den nye udbyder dækker den samme tjenestetype som den forrige. Hvor der er tale om skifte mellem forskellige tjenestetyper eller det af andre årsager ikke er teknisk muligt at opretholde et minimum af funktionalitet, skal udbyderne løse opgaven bedst muligt, bl.a. ved at anvende værktøjer og standarder for interoperabilitet, der ventes indført på baggrund af forordningen. Hvis disse værktøjer endnu ikke findes, skal udbyderen på kundens anmodning eksportere alle kundens data i et struktureret og maskinlæsbart format.

Hvor overgangsperioden på 30 dage ikke er teknisk gennemførlig, skal udbyderen angive en alternativ overgangsperiode, der ikke må overstige seks måneder.

Der lægges op til, at gebyrer for at skifte af udbyder gradvis fjernes over en treårig periode. Forslaget giver Kommissionen beføjelse til at vedtage delegerede retsakter for at indføre en overvågningsmekanisme, hvorigennem Kommissionen kan føre tilsyn med tilbagetrækningen af gebyrer.

#### Kap. 7: Beskyttelse af andre data end personoplysninger i internationale sammenhænge

Kapitlet indfører tiltag til beskyttelse mod tredjeparters ulovlige adgang til andre data end personoplysninger i EU gennem databehandlingstjenester, der udbydes på det indre marked.

Det foreslås, at udbydere af databehandlingstjenester skal træffe alle rimelige tekniske, retlige og organisatoriske foranstaltninger for at forhindre statslig adgang til ikke-persondata, hvor sådan adgang er i strid med lovgivningen.

Derved kan en forespørgsel om adgang til ikke-persondata på baggrund af en afgørelse afsagt af en domstol, ret eller administrativ myndighed i et tredjeland kun anerkendes og håndhæves, hvis den bygger på en international aftale mellem tredjelandet og EU eller den relevante medlemsstat. Hvor der ikke foreligger en sådan aftale, må databehandlingstjenesten kun efterleve anmodningen hvis:

- (a) tredjelandets system kræver, at afgørelsen begrundes, er af specifik karakter, og at den skal stå i et rimeligt forhold til formålet,

- (b) adressatens indsigelse kan prøves ved en kompetent domstol eller ret, og
- (c) den kompetente domstol har beføjelse til at tage behørigt hensyn til retlige interesser hos den, der stiller data til rådighed.

Adressaten for afgørelsen får mulighed for at anmode om en udtalelse fra relevante kompetente myndigheder for at fastslå, om ovenstående betingelser er opfyldt. Derudover foreslås det, at Kommissionen skal udarbejde retningslinjer for sådanne vurderinger.

Når udbyderen af en databehandlingstjeneste lovligt kan efterkomme et tredjeland's forespørgsel om dataadgang, skal udbyderen levere så lidt data som muligt.

Der indføres et gennemsigtighedskrav, idet udbydere af databehandlingstjenester skal underrette dataindehaveren om anmodningen, inden denne imødekommes.

Forslaget berører hverken retsgrundlaget for anmodninger om adgang til data, som EU-borgere eller -virksomheder er i besiddelse af, eller EU's ramme for databeskyttelse og beskyttelse af privatlivets fred.

### Kapitel 8: Interoperabilitet

Kapitlet indfører krav, der skal opfyldes for at fremme interoperabilitet for dataområder og databehandlingstjenester, samt rammer for anvendelse af intelligente kontrakter om datadeling.

#### *Dataområder*

Forslaget introducerer en række overordnede krav til operatører af dataområder med henblik på at fremme interoperabilitet for data, datadelingsmekanismer og datadelingstjenester. Kravene kan være generiske eller vedrøre specifikke sektorer. Kravene skal specificeres yderligere, hvilket foreslås gjort gennem en række tiltag, herunder:

- (a) tillægges Kommissionen beføjelser til at vedtage delegerede retsakter
- (b) gives Kommissionen bemyndigelse til at anmode europæiske standardiseringsorganisationer om at udarbejde udkast til harmoniserede standarder
- (c) tillægges Kommissionen beføjelser til at vedtage fælles specifikationer ved hjælp af gennemførselsretsakter, hvis der ikke findes harmoniserede standarder eller Kommissionen finder, at de harmoniserede standarder ikke er tilstrækkelige.

Endelig tillægges Kommissionen beføjelse til at vedtage retningslinjer, der fastsætter specifikationer for interoperabilitet for driften af fælles europæiske dataområder.



*Databehandlingstjenester*

Forslaget indeholder krav til, hvad åbne interoperabilitetsspecifikationer og europæiske standarder for interoperabilitet mellem databehandlingstjenester skal opnå, og hvad de skal omhandle med henblik på at understøtte forpligtelserne, der indføres i forordningens kapitel 6.

Det foreslås at Kommissionen skal kunne anmode europæiske standardiseringsorganisationer om at udarbejde udkast til harmoniserede standarder for specifikke tjenestetyper, der udbydes af databehandlingstjenester.

*Intelligente kontrakter*

Det foreslås, at der sættes en ramme for anvendelsen af intelligente kontrakter til aftaler om datadeling. Det gøres ved at stille krav til leverandøren af en applikation, der anvender intelligente kontrakter eller den person, hvis erhverv, forretning eller profession omfatter indførelse af intelligente kontrakter for andre (herefter 'leverandør af intelligente kontrakter').

Det foreslås, at Kommissionen skal kunne anmode europæiske standardiseringsorganisationer om at udarbejde udkast til harmoniserede standarder, der opfylder de væsentlige krav for leverandører af intelligente kontrakter.

Kommissionen tillægges beføjelser til at vedtage fælles specifikationer ved hjælp af gennemførelsesretsakter, hvis der ikke findes harmoniserede standarder eller hvis Kommissionen finder, at de harmoniserede standarder er utilstrækkelige.

Kapitel 9: Gennemførelse og håndhævelse

Kapitel 9 fastsætter gennemførelses- og håndhævelsesrammen med de kompetente myndigheder i hver medlemsstat, herunder en klagemekanisme og sanktioner.

*Kompetente myndigheder*

Ifølge forslaget skal hver medlemsstat udpege én eller flere kompetente myndigheder, som har ansvaret for anvendelsen og håndhævelsen af denne forordning. Medlemsstaterne kan oprette en eller flere nye myndigheder eller forlade sig på eksisterende myndigheder. Den kompetente myndighed skal udover at føre tilsyn og håndhæve forordningens tiltag, bl.a. informere om forordningen, behandle klager, samarbejde med kompetente myndigheder i andre medlemsstater og overvåge den teknologiske udvikling på området.

De uafhængige tilsynsmyndigheder, der er ansvarlige for at føre tilsyn med anvendelsen af persondataforordningen, bliver ansvarlige for at overvåge anvendelsen af denne forordning for så vidt angår beskyttelsen af personoplysninger.

Hvis en medlemsstat udpeger mere end én kompetent myndighed, skal der udpeges en koordinerende kompetent myndighed, og de kompetente myndigheder skal samarbejde med hinanden, samt med den tilsynsmyndighed, der er ansvarlig for at overvåge anvendelsen af persondataforordningen.

#### *Klageadgang*

Fysiske og juridiske personer får ret til at indgive klage til den relevante kompetente myndighed i den medlemsstat, hvor vedkommende har sit sædvanlige opholdssted, arbejdssted eller forretningssted, hvis personen mener, at vedkommendes rettigheder i henhold til forordningen er blevet krænket.

#### *Sanktioner*

Medlemsstaterne skal fastsætte regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af forordningen. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelserne og have afskrækkende virkning.

Eksisterende myndigheder, der har ansvaret for persondataforordningen og forordning (EU) 2018/1725 (forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer) får mulighed for at sanktionere i forhold til udvalgte forpligtelser.

#### *Model for aftalevilkår*

Det foreslås, at Kommissionen udvikler og anbefaler brugen af en ikkebindende model for aftalevilkår for dataadgang og -anvendelse for at bistå parterne med at udarbejde og forhandle kontrakter med afbalancerede kontraktlige rettigheder og forpligtelser.

#### Kapitel 10: Sui generis-retten i henhold til direktiv 1996/9/EF

Kapitlet reviderer direktiv 96/9/EF (Databasedirektivet). Det foreslås, at *sui generis*-retten i databasedirektivets artikel 7 ikke skal finde anvendelse for databaser, der lagrer data genereret af brugere af forbundne enheder eller tjenester. *Sui generis*-retten tilsiger, at en databases fremstiller har ret til at forbyde udtræk og genanvendelse deraf fra databasen. Databasedirektivets *sui-generis*-ret vil dermed ikke hindre brugernes effektive udøvelse af deres ret jf. kapitel 3 til at få adgang til og anvende IoT-genereret data.

#### **4. Europa-Parlamentets udtalelser**

I Europa-Parlamentet blev det 31. marts 2022 besluttet, at industri, forsknings-, og energi-, udvalget (ITRE) har kompetence på sagen. Derudover er Udvalget om det Indre Marked og Forbrugerbeskyttelse (IMCO), Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender (LIBE), og

Retsudvalget (JURI) associerede udvalg. I ITRE er det spanske EPP-medlem, Pilar del Castillo, udnævnt som ordfører.

Udvalgene er blevet enige om en ansvarsfordeling, hvor IMCO har kompetence for krav til databehandlingstjenester, JURI har kompetence på de aspekter, der angår beskyttelse af forretningshemmeligheder, LIBE har kompetence på beskyttelse af persondata og fundamentale rettigheder, mens ITRE har det overordnede ansvar for forslaget. Udvalgene er ved at behandle de første udkast og en endelig plenarafstemning forventes i marts 2023.

## 5. Nærhedsprincippet

Kommissionen vurderer, at forslaget er i overensstemmelse med nærhedsprincippet. Det er Kommissionens opfattelse, at den grænseoverskridende karakter af anvendelsen af data ikke kan behandles effektivt på nationalt niveau, og at fragmentering som følge af forskelle i nationale regler bør undgås, da det vil føre til manglende gennemsigtighed, manglende retssikkerhed og uønsket forumshopping. Kommissionen vurderer endvidere, at der er behov for en ensartet ramme i hele EU forsvarende aftalevilkår for datadeling mellem virksomheder, forpligtelser for producenter af IoT-produkter og for cloudcomputing-tjenester, samt datadeling mellem virksomheder og myndigheder. Samtidig argumenterer Kommissionen for, at forslaget vil bidrage til realiseringen af et indre marked for data, der kan give datadrevne virksomheder lige vilkår og fremme innovation og konkurrence.

Regeringen vurderer samlet set, at forslaget er i overensstemmelse med nærhedsprincippet.

## 6. Gældende dansk ret

Ophavsretslovens §71 vil skulle revideres for at tage højde for forordningens forslag om at revidere databasedirektivets artikel 7 på baggrund af forordningen.

## 7. Konsekvenser

### Lovgivningsmæssige konsekvenser

Det følger af forordningens artikel 35, stk. 1, at artikel 7 i databasedirektivet ikke finder anvendelse for databaser, der lagrer data genereret af brugere af forbundne enheder eller tjenester. Dermed skal ophavsretsloven revideres på baggrund af forordningen.

Der kan være love fra andre ministerområder, som endnu ikke er blevet identificeret, der vil blive påvirket af forordningen.

Bestemmelserne i forslaget har klare snitflader til eksisterende og kommende retsakter og derfor bør omfanget af sammenhæng til anden EU-regulering undersøges nærmere.

### Økonomiske konsekvenser

#### *Statsfinansielle konsekvenser*

Det forventes, at forslaget vil medføre statsfinansielle konsekvenser, idet udpegning eller etablering af en national myndighed, der er ansvarlig for implementeringen af forordningen, vil kræve ressourcer. Der vil ligeledes være øgede udgifter forbundet med håndhævelsen af forordningen hos den eller de myndigheder, der udpeges til kompetente myndigheder, idet forordningen forventes at medføre en øget sagsmængde og en udvidet opgaveportefølje, herunder i forhold til tilsynsfunktion, rådgivende opgaver, behandling af klager og sanktionering.

Afledte nationale udgifter som følge af EU-retsakter afholdes inden for de berørte ministeriers eksisterende bevillingsramme, jf. budgetvejledningens bestemmelser herom. Såfremt det viser sig, at det ikke er muligt at holde udgifterne inden for eksisterende bevillinger, vil håndteringen af udgifterne skulle afklares særskilt.

#### *Samfundsøkonomiske konsekvenser*

Forslaget vurderes at kunne få positive samfundsøkonomiske konsekvenser, såfremt reglerne er med til at understøtte udviklingen af et indre marked for data, der fremmer adgangen til og anvendelsen af data og medfører øget datadreven innovation.

Omvendt kan forslaget have negative samfundsøkonomiske konsekvenser, såfremt de nye krav og forpligtelser for erhverv skaber en u hensigtsmæssig incitamentstruktur, fx at forslaget modsat hensigten fjerner incitamenterne for at indsamle og lagre data, eller hvis forpligtelserne til portabilitet mellem databehandlingstjenester fx medfører krav om høj opstartsbetaling eller umuliggør flytning af organisationers komplekse cloudløsninger, resulterende i mindre optag af cloudløsninger.

#### *Erhvervsøkonomiske konsekvenser*

Forslaget forventes at medføre administrative byrder for de omfattede virksomheder. Forpligtelserne forbundet med at stille IoT-data til rådighed ventes at medføre løbende omkostninger for producenter og leverandører af IoT-genstande, samt omstillingsomkostninger til opsætning af tekniske in-

frastrukturer og ændring af skriftlige aftaler, herunder kontrakter. Derudover forventes administrative byrder forbundet med, at virksomhederne kan påkræves at dele data med offentlige myndigheder i EU, særligt da virksomhederne ikke vil kunne kræve godtgørelse i tilfælde hvor myndighederne skal bruge data til at reagere på en nødsituation. Udgifter hermed vil bl.a. afhænge af, hvor bredt en ”offentlig nødsituation” fortolkes. Der forventes endvidere udgifter for databehandlingstjenester relateret til efterlevelse af interoperabilitetskrav og beskyttende foranstaltninger mod ulovlig og uautoriseret dataadgang. Endvidere kan der være byrder på baggrund af tilsyn med de omfattede virksomheder, hvilket må antages at indebære dokumentationsforpligtelser. Endelig kan den konkrete udmøntning af krav og standarder indeholdt i delegerede- og gennemførselsretsakter medføre administrative byrder.

Samtidig kan forslaget føre til en lettelse af byrder relateret til større aftalemæssig retfærdighed ved datadeling mellem virksomheder, strømlining af offentlige myndigheders adgang til virksomhedsdata, og lettere skifte af databehandlingstjenester. Særligt mikrovirksomheder og SMV’er ventes at drage fordel af forslaget, idet de vurderes at få bedre aftalevilkår, bedre adgang til IoT-data til lavere omkostninger, og idet de samtidig er undtaget flere af forpligtelserne i forordningen. Derudover kan brugerens adgangsret til IoT-data og ret til at overføre data til tredjeparter være med til at forebygge fremkomsten af nye typer af techgiganter, der sidder inde med datamonopol. Endelig kan forslaget fremme et konkurrencepræget udbud af eftersalgsservice for virksomhedsbrugere og fremme virksomheders data-baserede innovation, ligesom udelukkelsen af gatekeepers kan stille det øvrige erhvervsliv bedre i konkurrencen overfor techgiganterne.

#### Andre konsekvenser og beskyttelsesniveauet

En vedtagelse af forslaget skønnes ikke at berøre beskyttelsesniveauet i Danmark.

Ud over de økonomiske konsekvenser, kan forslaget medføre afledte positive effekter for samfundet, da øget datadeling mellem virksomheder og mellem virksomheder og offentlige myndigheder kan bidrage til at løse samfundets problemer, herunder fx klimaudfordringen. Derudover fremmes forbrugerforhold, idet forbrugere får en ret til at anvende data, de genererer ved brug af en IoT-genstand, samt større valgfrihed af databehandlingstjenester. Endelig kan virksomheders datadeling med myndigheder bidrage til at reagere på offentlige nødsituationer.

## **8. Høring**

Forslaget har været sendt i høring i EU-specialudvalget for konkurrence, vækst og forbrugerspørgsmål med frist for bemærkninger den 31. marts 2022. Der er indkommet høringssvar fra Dansk Erhverv, Dansk Industri, Danske Rederier, Finans Danmark, Finansforbundet, Forbrugerrådet TÆNK, Ingeniørforeningen, IT-Branchen, samt Kommunernes Landsforening.

## Generelle bemærkninger

**Dansk Erhverv (DE)** bakker op om tiltag, der understøtter den europæiske dataøkonomi og gør det nemmere at dele og bruge data både i den private og den offentlige sektor. Forslagets intention om at styrke datadeling mellem virksomheder og henholdsvis forbrugere, andre virksomheder og offentlige myndigheder, samt intentionen om at gøre det nemmere for virksomheder at skifte mellem udbydere af cloudtjenester anses som udmærket. DE finder dog ikke, at de valgte policy-redskaber er hensigtsmæssige, hvorfor DE mener, at forslaget med fordel kan gentænkes på flere afgørende områder. DE mener, at deling af data bør ske på frivillig basis. DE har mange eksempler på, hvordan der indenfor branchefællesskaber eller fagområder etableres samarbejde om at dele data, ligesom data deles mellem virksomheder i værdikæden inden for en række sektorer. Derfor bør forslaget afholde sig fra at indføre lovkrav om datadeling, og bør i stedet se på muligheder for at etablere incitamentsstrukturer for datadeling og udbredelse af bedste praksis fra datadelingsfællesskaber, der fungerer godt. DE bakker op om, at forslaget ikke påvirker databeskyttelsesforordningen, som skal respekteres i forbindelse med deling af data. Anonymisering eller udskillelse af personhenførbare data fra ikke-personhenførbare data kan i mange tilfælde pålægge erhvervslivet væsentlige byrder og omkostninger, eftersom mange erhvervsdrivendes behandling af data sker til opfyldelse af kundeformål, hvor det netop er vigtigt, at data kan knyttes til en konkret kunde eller bruger. DE kan derfor ikke støtte eventuelle krav om, at erhvervslivet skal kunne udskille eller opdele personhenførbare data fra ikke-personhenførbare data, som led i at data skal stilles til rådighed for andre erhvervsdrivende eller offentlige myndigheder.

**DE** mener, at forslaget med dets bestemmelser om tilrådighedsstillesle af data for offentlige myndigheder forsøger at komme et problem til livs, der efter DE's overbevisning ikke er et reelt problem. Bl.a. under Covid-19 pandemien har samarbejdet mellem den offentlige og private sektor vist sit værd. Virksomhederne har i den forbindelse indgået aktivt og delt data på forespørgsel fra myndighederne, hvilket efter DE's overbevisning er forløbet forbilledligt. DE undres over, at Kommissionen ønsker at bruge ressourcer på at etablere et helt nyt bureaukratisk rammeværktøj for datadeling i krisesituationer, når erfaringerne fortæller, at en sådan datadeling løber af stablen uden problemer, når der er behov derfor.

**Dansk Industri (DI)** bakker op om, at man med forslaget få tydeligere regler for adgang til data og datadeling. Det kan være med til at skabe rammerne for en egentlig databaseret økonomi i EU. Det vil afhjælpe en række situationer, hvor købere af et givet produkt er begrænset i deres handlemuligheder, fordi de ikke har adgang til de data, produktet genererer. DI bemærker dog, at "data" som her reguleres, dækker over mange forskellige typer data, herunder blandede datasæt, hvoraf persondata allerede er omfattet af persondataloven. Der kan derfor være behov for at præcisere forslaget i forhold til, hvilke typer data, der er tale om, så reglerne tilpasses forholdene i den enkelte sektor. DI bemærker, at det ikke fremgår tydeligt på alle fronter, hvordan forslaget spiller sammen med anden lovgivning på området, herunder generel konkurrenceret, datastyringsforordningen, samt Kommissionens forslag til retsakt om digitale markeder, retsakt om digitale tjenester, forordningsforslag om harmoniserede regler for kunstig intelligens, forordningsforslag om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager, samt forordningsforslag vedrørende respekt for privatlivets fred og beskyttelse af persondata ved elektronisk kommunikation, NIS2 og den kommende regelbog for cloudtjenester, samt forhandlinger med USA om Privacy Shield og Cloud Act. Det gælder fx i forhold til virtuelle assistenter. DI mener derudover, at det er uklart, hvad der forventes af virksomheder, der betragtes som databehandlere under persondataforordningen.

**Danske Rederier** bemærker, at dansk skibsfart er blandt verdens mest avancerede og allerede i dag benytter sig af data fx i forbindelse med avancerede operationssystemer. Danske Rederier mener, at en regulering på området er vigtig for skibsfarten, der netop nu er i gang med en transformation til digitale og forbundne skibe bl.a. gennem brugen af datadrevne IoT-teknologier. Skibsfarten har som global industri brug for globale rammer for deling og brug af data, hvorfor det er vigtigt, at forslaget ikke fører til konkurrenceforvridning mellem EU og non-EU skibe. Danske Rederier er i færd med at undersøge forslagets betydning og sammenhæng med anden regulering og ser frem til at bidrage med mere detaljerede bemærkninger.

**Finans Danmark (FIDA)** mener, at en stærk europæisk dataøkonomi kan give nye muligheder for borgere og virksomheder og styrke innovation og vækst i samfundet. FIDA er derfor glade for, at der på EU-niveau med forslaget bliver bedre adgang til deling af data. For at realisere dette, mener FIDA dog, at det er nødvendigt at opfylde to væsentlige forudsætninger: 1) datadelingen skal udvides til at omfatte flere sektorer, herunder for at sikre, at datadeling sker på tværs af sektorer og 2) brugeren skal sættes i centrum, og der skal kun ske deling af persondata efter brugerens udtrykkelige tilsagn. FIDA mener, at forslaget kun lægger op til en øget datadeling for IoT-produkter og relaterede tjenester, hvorfor forslaget må forventes at få en forholdsvis begrænset effekt på datadelingen på tværs af sektorer. For ikke unødigt at sinke

udviklingen af europæisk dataøkonomi, er der behov for, at forslaget bredes ud til at omfatte flere sektorer data.

**Finansforbundet** mener, at det er afgørende, at datadeling i og på tværs af sektorer sker under rimelige, ensartede og ikke-diskriminerende forhold. Datastrømme bør i fremtiden ikke kun ensrettes en type virksomhed til en anden, men bør kunne flyde begge veje. Finansforbundet mener, det er et paradoks, at fx pengeinstitutter med højeste datasikkerhedsniveauer skal dele data uden samtidig at sættes i stand til at modtage data fra fx datadrevne SMV'ere. Forslaget bør bidrage til at adressere den ulige konkurrence, der er skabt med PSD2. Finansforbundet mener, at de finansielle områder i forvejen er højt reguleret og bemærker, at forslaget på det finansielle område kan medføre øget lovgivning og administrative byrder, der hindrer det tilsigtede potentiale. Finansforbundet bemærker, at det er omkostningsfuldt at skabe forsvarlige rammer for at kunne dele data sikkert, og der er derfor behov for, at der sikres en forretningsmodel, der både skaber incitament for at dele data sikkert, men også for at sikre, at den delte data er af høj kvalitet.

**Forbrugerrådet TÆNK** mener, at forslaget kan være med til at forbedre forbrugeres retstilling på det digitale marked og øge konkurrencen blandt virksomheder. Hvor databeskyttelsesloven skal sikre forbrugernes indsigt i og kontrol med egne data, kan forslaget især understøtte rettigheden om dataportabilitet, som fremgår af databeskyttelseslovens artikel 20, men som indtil videre har haft en begrænset anvendelse i praksis.

**Ingeniørforeningen (IDA)** er overordnet meget positive overfor forslaget. IDA mener, at forslaget vil gøre det lettere for forbrugerne at få adgang til og overføre data fra de digitale produkter og tjenester, som er blevet en del af de fleste danskeres hverdag. Det er vigtigt for både tillid til digitalisering generelt og lyst og nysgerrighed overfor nye digitale produkter og tjenester, at forbrugere sikres adgang til egne data og den bedst mulige handlekraft i forhold til at håndtere egne data. Det handler om at sikre størst muligt overblik over og rettighed til egne data. IDA mener, at det er positivt, at der med forslaget sikres bedre innovation og et nødvendigt og længe ønsket brud med de helt store techvirksomheders reelle monopol på data. Det giver en mere fair platform for nye innovative og fx dataetiske startups, der har som mål at tilbyde forbrugerne alternative digitale muligheder, og et stigende ønske blandt danskerne om at få mere kontrol over egne data. IDA er positiv overfor forslaget om at forhindre store gatekeeper virksomheder i at få kommerciel fordel af den adgang til datadeling, som gives til virksomheder, offentlige myndigheder og forbrugere. Dette er en forudsætning for at nå målet om at styrke konkurrencen. IDA finder imidlertid, at det er nødvendigt, at lovgivningen sikrer, at der er en grundlæggende beskyttelse af forbrugeren, så det bliver et kollektivt fremfor et individuelt ansvar at beskytte privatlivets fred og grundretighederne i persondataforordningen. IDA mener endvidere, at det er positivt,



at forbrugerne får klageadgang og reglerne er bødesanktioneret, idet det dog bemærkes, at der kun opnås den ønskede effekt, hvis der sikres en effektiv håndhævelse af lovgivningen.

**IT-Branchen** er overordnet positiv over for de politiske mål om at tilskynde en højere grad af datadeling. Forslaget kan være med til at indfri de markante gevinster, der ligger i den europæiske dataøkonomi, og danske virksomheder kan få en hjemlig markedsplads på storskala-niveau, når der tales data og kunstig intelligens. Offentlige instanser ligger ligeledes inde med store data-mængder, der med fordel kan fordeles på tværs af EU til gavn for innovation og vækst. I forhold til de private virksomheder mener IT-Branchen, at dette mål bedre kan realiseres ved hjælp af frivillige, markedsstyrede løsninger, baseret på internationale anerkendte standarder og normer, samt klare retningslinjer og incitamenter til øget datadeling. At indføre strenge obligatoriske krav til produktdesigns i en dataøkonomi, der på flere markeder fortsat er i sin tidlige udvikling, kan markant skade Europas digitale udvikling.

**Kommunernes Landsforening (KL)** bemærker, at forslagens ambition er en større grad af datadeling, der samtidigt skal være i overensstemmelse med persondataforordningen, hvilket anses som helt essentielt. Datadrevet innovation forventes at give store fordele for bl.a. borgerne i form af bedre og smartere løsninger og produkter, der tager udgangspunkt bl.a. i individets rettigheder, således at borgernes tillid opretholdes. KL bakker overordnet set op om hensynet bag forordningen bl.a. pga. et stigende behov for klarhed i forhold til dataadgang, således at udviklingen ikke primært drives af tech-virksomheder, men i højere grad af hensyn til det offentliges rolle og opgaver, samt hensyn til borgerne. Det er i den forbindelse som udgangspunkt positivt, at forslaget ser ud til at lette skift af cloudleverandører, samt at der lægges op til en regulering af udleveringsanmodninger fra tredjelande. Overordnet set hæfter KL sig dog ved, at forslaget er uklart i forhold til roller og konsekvenser for offentlige myndigheder, herunder kommunerne og de data, som kommunerne behandler. Særligt er det uklart, om offentlige myndigheder kan og i givet fald i hvilket omfang de vil være omfattet af begreberne "udbydere af databehandlingstjenester" og "dataindehaver". Dette er centralt for forståelsen for forslagens anvendelsesområde og for KL's konkrete spørgsmål til denne. I den udstrækning, at de mulige konsekvenser for offentlige myndigheder ikke er hensigten, bør det fremgå mere eksplicit af definitioner, afgrænsninger med videre. I det tilfælde at hensigten fx er at påvirke relationen i forhold til data mellem myndighed og borger, bør dette beskrives tydeligere, således, at KL og øvrige har mulighed for at forholde sig konkret til forslagens konsekvenser.

## **Specifikke bemærkninger**

### Anvendelsesområde og definitioner

**DE** mener, at forslaget med fordel kan blive meget tydeligere afgrænset, og at det nuværende anvendelsesområde ikke har en klar logik eller tydelig begrundelse forsvarende hvilke produkter og tjenester, der omfattes i forhold til krav om brugeradgang til IoT-data.

**F&P** bemærker, at der er flere steder i forslaget anvendes begreber fra andre EU-retsakter, uden at der direkte henvises til disse, ligesom flere begreber ikke defineres i forslaget. F&P mener, at det, henset til risikoen for høje bøder for manglende overholdelse, er væsentligt, at der ikke er tvivl om definitionerne, samt rækkevidden af de enkelte bestemmelser.

**IT-Branchen** mener, at anvendelsesområdet er for bredt, og at flere af definitionerne er uklare og giver anledning til en vis grad af usikkerhed om hvornår og i hvilke situationer, bestemmelserne finder anvendelse. Det vil medføre utilsigtede konsekvenser, der ikke er i overensstemmelse med forslagets formål. I forhold til anvendelsesområdet undtages tjenester, der i langt de fleste tilfælde har og kan tilbyde mange af de samme funktioner, som de omfattede tjenester tilbyder., hvilket virker uklart og arbitrært. IT-Branchen mener, at udviklingen af værktøjer for dataadgang vil komme til at kræve en komplet omstrukturering af produkter, hvorfor det kun bør finde anvendelse ved data, hvor producenten eller udbyderen af en tjeneste har mulighed for at få adgang til eller identificere data. I forhold til definitioner fremhæver IT-Branchen, at det er uklart, hvad der menes med ”funktionel ækvivalens” i sammenhæng med bestemmelser om skift af databehandlingstjeneste. Denne bør blive fortolket snævert for at sikre, at resultatet ikke er en udjævning eller kommercialisering af de databehandlingstjenester, der udbydes. IT-Branchen fremhæver også definitionen af ”relateret tjeneste” i forhold til IoT-produkter, idet begrebet kan tolkes meget bredt og dermed inkludere databehandlingstjenester, da de fleste enheder vil være cloud-baseret. Der kan stilles spørgsmålstegn ved, om relaterede tjenester blot bør fjernes fra forslagets anvendelsesområde.

#### Datadeling mellem virksomheder og forbrugere og mellem virksomheder

**DI** er forstående overfor, at der foreslås en meget klar og tydelig ret til egne data. DI er enige i, at det er nødvendigt for dataøkonomien med klare regler for, hvornår man ejer data og ikke mindst har adgang til data. Det sikrer, at databrugere kan anvende data, og at der for alvor kan skabes en dataøkonomi baseret på data fra de produkter, de anvender. DI mener dog ikke, at der skal være tale om en universal og uindskrænket ret, eller at data nødvendigvis skal kunne tilgås gratis. Hvis adgangsretten til data skal fremme formålet om en dataøkonomi, er det vigtigt, at den begrænses på en række væsentlige punkter, samt at der arbejdes på at skabe de rette incitamentter for at dele data.

**DI** mener for det første, at retten til data ikke må følges op af en begrænsning på prisen for data, da det i praksis vil betyde, at omkostningen i stedet lægges på det produkt, man vil sælge. Hermed begrænses dataholders valg af forretningsmodel. De dataholdere, der hellere vil sælge produkter med underskud i forventning om indtægter på et eftermarked, herunder salg af data, bliver begrænset, hvilket særligt gælder når databrunder kan videreformidle data til dataholderens konkurrenter. Imod forslaget om en datadrevet økonomi, begrænses incitament til at udvikle produkter, der genererer data, idet data skal stilles til rådighed uden kompensation. DI vurderer derfor, at forslaget risikerer at hæmme den digitale innovation i EU. DI foreslår, at virksomhederne skal have lov at kræve kompensation for at stille data til rådighed for brugerne, hvilket som minimum skal dække over omkostningerne ved at stille data til rådighed. For det andet, mener DI, at reglerne til beskyttelse af forretningshemmeligheder bør udbygges for at bevare virksomhedernes incitament til at innovere, herunder er det u hensigtsmæssigt, at beskyttelsen af forretningshemmeligheder er forskellig, alt efter om data leveres til brugeren eller tredjepart. Forslaget bør indføre mere robust beskyttelse eller helt undtage forretningshemmeligheder med reference til direktivet om forretningshemmeligheder. For det tredje, mener DI, at det bør præciseres, at virksomheder kun er forpligtet til at stille rådata til rådighed, hvormed det må være op til den enkelte bruger at bearbejde data. Det bør dertil tydeliggøres, at der kun er tale om de data, som i dag opsamles fra produktet, fremfor alle data, som potentielt kan genereres. DI støtter en ret til adgang til de data, brugeren genererer med de ovenfor anførte begrænsninger. Endvidere bemærker DI, at forslaget om at tredjeparter ikke må anvende modtaget IoT-data til at udvikle et konkurrerende produkt, vil være svært at håndhæve i praksis og vil kunne give anledning til mange tvister.

**F&P** mener, at det skal være mere tydeligt, hvilke rettigheder dataindehaveren har i forhold til forretningshemmeligheder. Det kunne være ønskeligt, hvis dataindehaveren havde en vis indflydelse på og kan begrænse hvem de deler deres forretningshemmeligheder med og i hvilket omfang. F&P mener, at det skal sikres og kontrolleres, at IoT-data ikke misbruges til fremstilling af konkurrerende produkter. Derudover skal det afklares, hvad det betyder for eksisterende nationale løsninger, at det anføres, at medlemsstaterne ikke må vedtage eller stille yderligere krav i forhold til adgangsretten for IoT-data.

**F&P** bemærker, at flere af bestemmelserne har et indhold, der minder om rettigheder efter persondataforordningen. I nogle tilfælde tilføjer forslaget et ekstra lag til de eksisterende rettigheder fra persondataforordningen, som fx er tilfældet med retten til dataportabilitet. F&P mener, at opfyldelsen af rettighederne efter persondataforordningen er tidskrævende, hvorfor det bekymrer, at introduktionen af yderligere og lignende forpligtelser kan blive administrativt meget tungt for dataindehaverne. Hertil kommer, at adgangen til

IoT-data også i nogle situationer skal stilles til rådighed for tredjeparter, hvilket kan give udfordringer i forhold til samtidig at skulle efterleve persondataforordningen. Kravet om, at data skal stilles til rådighed på en let og sikker måde og hvor hensigtsmæssigt direkte, finder også anvendelse for persondata, hvilket betyder, at persondataforordningen også skal efterleves ved produktets udformning eller levering af tjenesten. Det vil formodentlig kunne medføre større krav til de tekniske løsninger og dermed øget ressourceforbrug. Da de fleste løsninger leveres i forskellige samarbejdsmodeller med store teknologileverandører, er effektiv adgang til data vigtigt, hvis formålet med reglerne skal opnås. Ellers er risikoen, at brugerne får rettighederne om dataadgang, men ikke kan udnytte data selv. Endvidere er der udfordringer relateret til at få dokumenteret samtykket fra brugeren, hvor tredjeparter indhenter data fra dataindehaveren, idet dette ikke specificeres i forslaget. Det er derudover uklart, hvordan det skal sikres, at data ikke anvendes af tredjeparten til egne formål.

**FIDA** bemærker, at bankerne i dag allerede deler betalingsdata med tredjeparter i henhold til betalingstjenestedirektivet (PSD2). FIDA mener, at forslaget risikerer at uddybe de asymmetrier for dataadgang, som bankerne i dag står overfor og medføre konkurrenceforvridning pga. krav om obligatorisk deling i nogle sektorer kontra frivillige eller mindre omfattende krav i andre. Et første skridt kunne være at øge portabilitet af data fra teleselskaber, forsyningsselskaber og e-handel, hvilket vil lette større genbrug af data på tværs af sektorer og åbne muligheder for nye og forbedrede produkter og tjenester. FIDA mener, at der er behov for klare og ensartede regler for datadeling. Uden klare principper for, hvordan data deles på en standardiseret og automatisk måde, bliver det vanskeligt at realisere ambitionerne. Derudover giver det en økonomisk skævvridning mellem brancher, da fx bankerne skal bruge ressourcer på at stille data til rådighed via API'er, mens andre sektorer ikke skal. Med hensyn til sikre datadelingsmekanismer, er API'er at foretrække, da de rummer en række fordele, herunder at garantere maksimal interaktion, fjerne adgangsbarrierer og muliggøre direkte og realtids dataadgang. Der er behov for at definere tydeligere, hvilke data der deles og i hvilken form. Endvidere er der behov for klarhed i forhold til ansvar for data, hvor der fx i PSD2 er klarhed over ansvaret for data, når den deles med tredjeparter. FIDA finder dog, at det er positivt, at deling af data med gatekeeper platforme begrænses, og at der ikke må udbydes en konkurrerende tjeneste baseret på de data, som deles.

**Finansforbundet** mener, at særligt dataetikken bliver relevant med kravet om, at produkter skal følge designprincipper om let adgang til data for virksomheder og i visse tilfælde offentlige myndigheder. Hvor der i forslaget lægges vægt på gennemsigtighed over for tredjepart om, hvilke data, der er tilgængelig i et produkt, og hvordan de tilgås, bør der tilsvarende lægges vægt på dataetik fx transparens og overblik over for forbrugerne. Finansforbundet

mener endvidere, at hvor den underliggende tese i forslaget er at sikre forbrugerne kontrol over egen data ved at give dem ret til at flytte data fra en virksomhed til en anden, er der samtidig risiko for, at det omvendt over tid, kan reducere overblik og følelsen af kontrol. Det bør derfor overvejes, hvordan denne rettighed udmøntes i praksis over for forbrugerne, og hvordan forbrugeren kan sikres et overblik over de data, der er delt over tid, samt hvordan samtykke trækkes let og effektivt tilbage. Overblikket over, hvor der er givet samtykke til opsamling, opbevaring, brug og videreformidling eller salg af data er svær at etablere. Der kunne med fordel afsøges løsninger til at skabe forståeligt overblik og nutidsbillede af den enkeltes aktuelle datasituation.

**Forbrugerrådet TÆNK** mener, det er positivt, at forbrugerne får styrkede rettigheder i forhold at få adgang til, bruge og overføre de data, som deres digitale produkter og tjenester indsamler og genererer. I praksis er IoT-data ofte ikke let tilgængelige for forbrugerne, som har begrænsede muligheder for at portere IoT-data. En vigtig problemstilling, som forslaget bør kunne afhjælpe, er fx at sikre, at digitale el-biler fremover skal dele data med selvstændige værksteder, som hidtil har været forhindret i at konkurrere på lige vilkår, fordi de ikke har haft adgang til bilproducenternes data. Ligeledes vil forslaget kunne åbne for små startups, som fx er optagede af dataetik, og som ønsker at innovere i data ved at give forbrugerne indsigt i og kontrol med, hvilke data de har liggende hos techgiganter. Dermed kan dataindsamling blive mere gennemsigtig og anvendelig for forbrugerne, og nye virksomheder kan drage nytte af data, som især techgiganter profilerer af at råde over i dag.

**Forbrugerrådet TÆNK** støtter, at forslaget forhindrer gatekeeper virksomheder i at få kommerciel fordel af den adgang til datadeling, som forslaget giver brugerne, idet forslaget skal styrke konkurrencen ved at lade andre end techgiganterne få adgang til deres data og bryde gatekeepernes datamonopol lidt op. Forbrugerrådet ser positivt på, at forbrugerne med loven får klageadgang og reglerne er bødesanktioneret, idet Forbrugerrådet dog bemærker, at effektiv håndhævelse er essentiel for, at regelsættet får betydning i praksis.

**Forbrugerrådet Tænk** er meget optaget af, at den øgede adgang til at dele og innovere pba. data ikke blot genererer mere data på endnu flere hænder, særligt hvad angår persondata, som også er omfattet af forslaget. Forslagets formål skal udøves i respekt for de grundlæggende rettigheder til privatliv og databeskyttelse efter databeskyttelsesloven. Det betyder, at forslaget skal sikre, at forbrugerne ikke kan samtykke sig ud af grundlæggende beskyttelsesregler efter databeskyttelsesloven, samt at en given indtægt for videresalg af egne data ikke skal kunne underminere intentionerne i databeskyttelsesloven.

**IT-Branchen** bemærker, at forslaget bestemmelse om videregivelse af forretningshemmeligheder til brugere, tredjeparter og offentlige organer forudsætter en opretholdelse af fortrolighed om forretningshemmeligheder. Det er iøjnefaldende og problematisk, at det ikke af bestemmelsen fremgår, på hvilken måde dataindehaverens interesser vil blive beskyttet, eller hvordan dataindehaveren vil blive gjort bekendt med, at forretningshemmeligheder er blevet kompromitteret. IT-Branchen mener, at det vil være praktisk vanskeligt, hvis bevisbyrden for, at et sådant misbrug har fundet sted, påhviler den oprindelige dataindehaver. IT-Branchen finder det besynderligt, at foranstaltninger angående forretningshemmeligheder differentierer, afhængigt af, hvorvidt modtageren er bruger eller tredjepart.

#### Forpligtelser for dataindehavere, der er retligt forpligtede til at stille data til rådighed

**F&P** finder det betænkeligt, at det ikke er præciseret, hvad der ligger i, at dataindehavere kan kræve "rimelig" compensation. Der bør præciseres, hvilke elementer, der kan indgå i denne beregning, herunder omkostninger ved udvikling, indsamling og opbevaring af data.

**FIDA** hilser forslaget indførelse af horisontale principper, der gælder når dataindehavere forpligtes til at dele data i fremtidige initiativer, meget velkommen, navnlig princippet om compensation. Hvis der skal skabes en europæisk dataøkonomi, er det væsentligt, at der er en forretningsmodel for alle part i datadelingen, dvs. både for den virksomhed, som deler data, og for den virksomhed, der anvender data. Der er i den forbindelse behov for en mere præcis beskrivelse af, hvad der menes med "rimelig compensation" og principper for at fastsætte dette.

**IT-Branchen** mener, at forslaget pålægger dataindehavern en urimelig bevisbyrde, idet denne skal kunne bevise at betingelserne for at gøre data tilgængeligt er ikkediskriminerende, når en virksomhed anser betingelserne for at være diskriminerende. Det er uklart, hvorfor datamodtagere skal have ret til at fremsætte generelle påstande uden at underbygge deres argumenter.

#### Urimelige vilkår vedrørende dataadgang og -anvendelse mellem virksomheder

**F&P** mener, at det bør afklares, hvordan "urimeligt vilkår" skal fortolkes i forhold til dansk lovgivning og aftaleloven.

**KL** bemærker, at når kommunerne anvender techgiganter sociale medier, påtvinges de at acceptere techgiganternes kommercielle videreanvendelse

af data ud fra aftalevilkår, som ikke er til forhandling, og hvor styrkeforholdet mellem techgiganterne og kommunerne misbruges. KL mener, at det vil være oplagt, at disse aftalevilkår adresseres i kapitlet om urimelige vilkår vedrørende dataadgang og -anvendelse mellem virksomheder.

Tilrådighedsstillelse af data for offentlige myndigheder og unionens institutioner, agenturer eller organer på grundlag af et ekstraordinært behov

**DE** mener, at der bør indtænkes sikkerhedsforanstaltninger, som beskytter virksomhederne mod uretmæssige forespørgsler fra myndigheder, samt at det bør være mere tydeligt præcis hvilke kriterier, der skal være opfyldt, før en situation kan betegnes som en offentlig nødsituation.

**DI** noterer sig, at der gives ret til, at myndigheder kan forlange data, som ikke ellers er tilgængelige på markedet, fra private parter. Det bemærkes, at det er uklart hvornår noget er en nødsituation. Ydermere gives ret til at kræve private data udleveret såfremt, det er en afgrænset lovfæstet opgave i offentlighedens interesse. DI mener, at det vil give meget vide rammer, for at bede private virksomheder om at udlevere data til myndighederne, og DI bakker således ikke op om dette i sin nuværende form. Det bør konkretiseres yderligere, hvornår der kan stilles krav om at udlevere data. I den forbindelse mener DI, det er vigtigt, at den klageinstans, der udpeges til at afgøre sager om udlevering af offentlige data, er uafhængig og har indsigt i, hvornår der er tale om data, der indeholder forretnings-hemmeligheder. Endvidere mener DI, at det er uhensigtsmæssig, hvis man vil fremme en dataøkonomi, at offentlige myndigheder ikke skal betale markedsprisen for adgang til data. Kompensation bør lægges så tæt op af markedspris som muligt ved at se på prisen for sammenlignelige typer af data. DI foreslår, at prisfastsættelsen sker ved fri forhandling.

**FIDA** mener, det er et positivt skridt, at der indføres en harmoniseret ramme for datadeling mellem virksomheder og myndigheder, men mulighederne for at dele data med henblik på "ekstraordinære behov i tilfælde af at udføre en specifik opgave i offentlighedens interesse" er for brede og skal præciseres yderligere. Det er også vigtigt at præcisere hvilken type data, virksomhederne skal dele. FIDA finder det uhensigtsmæssigt, at der kan fastsættes nationale regler parallelt med EU-reglerne. Eksistensen af en offentlig nødsituation bestemmes i henhold til de respektive procedurer i medlemsstaterne eller relevante internationale organisationer, hvilket indebærer en risiko for fragmentering. I forslaget skelnes mellem forskellige scenarier for at stille data til rådighed, og hvor data til imødegåelse af en offentlig nødsituation stilles gratis til rådighed, begrænses dataindehaverens kompensation i de to andre scenarier til de marginale omkostninger ved at levere data. Forslaget anerkender således, at der er en balance, der skal drages mellem offentlige og private interesser, men det er bekymrende,

at der skelnes mellem hvad der er nødvendigt, og hvad der kunne være be-  
lejligt. FIDA mener endvidere, at det er uklart, hvordan forslaget spiller  
sammen med allerede eksisterende krav til virksomhederne om at levere  
data til offentlige myndigheder, og om det fremover vil være muligt at få  
betaling på flere områder. Der er endvidere behov for klarhed over, hvor-  
dan kompensation skal opgøres.

**IT-Branchen** bemærker, at forslaget giver offentlige organer mulighed for  
at indhente data i tilfælde, hvor der er tale om et ”ekstraordinært behov”,  
mens der ikke inkluderes sikkerhedsforanstaltninger for dataindehaveren i  
tilfælde af u hensigtsmæssig brug af data, som kan skade dataindehaveren.  
IT-Branchen er således bekymret for, at forslaget giver en bred statslig ad-  
gang til data uden nogen specifikke former for sikkerhedsforanstaltninger.

**KL** mener ikke, at kommunerne skal betale på markedsvilkår for at få ad-  
gang til data hos private aktører i nødsituationer. KL mener endvidere, at  
det ikke virker rimeligt, at leverandøren kan afslå en dataanmodning med  
henvisning til at anmodningen ikke er skrevet tilstrækkeligt klart, koncist  
og i et almindeligt sprog, idet sådanne krav kan medføre procesbæspænd i  
reelle nødsituationer.

#### Skift mellem databehandlingstjenester

**DE** mener, Kommissionen ikke i tilstrækkelig grad anerkender det kom-  
plekse forhold, som kendetegner markedet for cloudtjenester. DE bakker  
fuldt op om at fjerne unødvendige barrierer for, at virksomheder kan skifte  
leverandør, men det fremstår i forslaget, som om det at skifte cloudleveran-  
dør er en simpel dataoverførsel. Det bemærkes, at der bl.a. er stor forskel  
på typen af tjenester, de forskellige leverandører stiller til rådighed, data-  
mængden og -arkitekturen, samt at den kontraktuelle fordeling af ansvar  
mellem kunde og leverandør medfører, at kunde-leverandør forholdet på  
dette marked er kendetegnet ved et stort behov for teknisk rådgivning og  
projektstyring. Disse forhold bør afspejles i forslaget.

**DI** støtter formålet om at gøre det nemmere for brugerne at skifte udbydere.  
DI finder dog, at tidsrammen for at kunne flytte data er urealistisk, såfremt  
der er tale om store kontrakter med en stor mængde data. Bestemmelserne  
for skifte og portabilitet bør derfor nuanceres ud fra type og omfang af data.  
I forslaget distingveres mellem krav til leverandører af infrastruktur-tjene-  
ster (fx IAAS for cloudtjenester), som typisk er højt standardiserede og  
kommercialiserede, og softwaretjenester (som PaaS eller SaaS), der typisk  
er mere komplekse og skræddersyede. DI mener, at det er vigtigt at holde  
fast i denne distinktion og udbrede den til de øvrige artikler om skifte og  
portabilitet. Man bør være opmærksom på, hvornår der stilles krav til funk-  
tionel ækvivalens, hvilket kan give mening for IaaS-tjenester, der mere er



et standard vareprodukt, mens det ikke giver mening ved PaaS eller SaaS, hvor man alene kan overføre data, ikke funktioner. Hvis kravet om at opnå funktionel ækvivalens efter et skift også gælder ved overførsel af data fra softwaretjenester, vil det i sidste ende kunne betyde, at alle cloududbydere af softwaretjenester skal anvende ens teknologi eller dataformater. Det vil resultere i øget ensartethed i softwareudbuddet og dermed færre valgmuligheder for kunderne. Det kan på sigt skade innovationen blandt europæiske virksomheder og brugere. DI ser derfor gerne, at begrebet ”funktionel ækvivalens” som minimum defineres klart i forslaget.

**IT-Branchen** bemærker, at forslaget har en legitim ambition om at fjerne forhindringer for, at cloudkunder skifter leverandør. Dog mener IT-Branchen, at forslagets forsøg på at sammenligne skift af cloudtjeneste med en relativt enkel migration af lagrede data eller gratis portabilitets-operationer i henhold til persondataforordningen ikke afspejler de mange forskellige cloudtjenester, datamængden og datakompleksiteten, det delte ansvar mellem cloududbydere og kunder, samt behovet for specialiseret teknisk assistance og projektledelse. Denne rigide tilgang vil have utilsigtede konsekvenser for konkurrencen og innovationen.

**KL** ser umiddelbart positivt på fastsættelsen af krav til skift mellem data-behandlingstjenester, idet KL finder, at det vil gøre det lettere for kommunerne at skifte fra cloudleverandører, der ikke vil kunne opfylde de skærpede krav til tredjelandsoverførsler, som følger af persondataforordningen og Screms II-dommen.

#### Beskyttelse af andre data end personoplysninger i internationale sammenhænge

**DI** bemærker, at forslaget sætter rammer for internationale overførsler af data. DI mener, at det i den forbindelse er vigtigt, at bestemmelserne er i overensstemmelse med anden regulering af internationale dataoverførsler, herunder den nye aftale om Transatlantic Data Privacy Framework.

**IT-Branchen** noterer sig, at forslaget indeholder bestemmelser om tekniske, juridiske og organisatoriske tiltag for at undgå overførsel eller adgang til ikke-persondata opbevaret i EU. Det mener IT-Branchen kan være diskriminerende overfor cloudtjenesteudbydere etableret i EU, som kan være underlagt love i en anden jurisdiktion, som kan være i strid med EU-lov. Af den årsag mener IT-Branchen, at det kan påvirke større datastrømninger, idet det vil være en forudsætning, at der foreligger en forudgående juridisk vurdering af en potentiel konflikt med EU-lovgivning. Alt dette taget i betragtning vil formentlig svække EU-virksomheders muligheder for vækst og for at konkurrere internationalt, da det begrænser deres valg af teknologi og EU's innovationskapacitet.

**KL** vurderer, at de udfordringer, kommunerne har med tredjelandes udleveringsanmodninger i forhold til persondata, med forslaget umiddelbart også vil komme til at gælde øvrige oplysningstyper. Dog mener **KL**, at det er positivt, at man med forslaget forsøger at undgå en Schrems II-sag på øvrige typer data ved at regulere udleveringsanmodninger. **KL** bemærker, at undtagelsesbestemmelserne er uklare.

### Interoperabilitet

**DI** støtter, at forslaget lægger op til større interoperabilitet mellem forskellige cloudtjenester. **DI** mener, at de tekniske elementer deri er vigtigt for at opnå interoperabilitet i praksis, hvorfor specifikationerne for interoperabilitet bør fastlægges i dialog med virksomhederne og andre relevante aktører. Ydermere bør de afspejle internationale standarder og praksis på området.

**Dansk Standard (DS)** bemærker, at forslaget bygger på principperne i det såkaldte New Legislative Approach. Denne metode går ud på, at et direktiv eller en forordning udformes som rammelovgivning som i brede vendinger beskriver de essentielle krav, og at der identificeres europæiske standarder, som, når de efterleves, kan give formodning om overensstemmelse med lovgivningen. På den måde defineres de essentielle krav, mens de tekniske specifikationer defineres i harmoniserede standarder. Dette er væsentlig lettere for virksomhederne end at skulle dokumentere, at de efterlever lovgivningen direkte, fordi der ikke står noget i loven om, hvordan man rent teknisk lever op til lovens krav, og benyttes især af mindre virksomheder. Når der kommer nye varetyper på markedet eller når ny teknologi skaber øgede risici eller mulighed for større sikkerhed, kan de tekniske standarder løbende revideres og godkendes af Kommissionen. Der bliver færre behov for at justere lovgivningen, som derved bliver agil. Det kan i den forbindelse være vigtigt at fastholde krav om rimelige overgangsordninger, således at virksomheder kan nå at omstille sig til nye krav, med alt hvad det indebærer for både produktionsprocesser og dokumentation.

**Dansk Standard** mener, at det er uheldigt, at Kommissionen giver sig selv mulighed for at udstede fælles tekniske specifikationer ved brug af delegerede retsakter og derved detailregulere området. Denne mulighed bør begrænses, så den kun anvendes, hvis Kommissionen har forsøgt at anmode om harmoniserede standarder, og proceduren gøres transparent, således at der fx skal gennemføres en bred offentlig høring, hvor alle interessenter har mulighed for at bidrage, som det er tilfældet når der udvikles harmoniserede standarder. Kommissionen har i sin standardiseringsstrategi fra februar 2022 annonceret, at man vil lave en ensartet tilgang til denne problemstilling på tværs af lovgivningsområder. Det er uklart, om forslaget vil være omfattet af den nye horisontale tilgang.

**FIDA** mener, at der er behov for en præcisering af samspillet mellem bestemmelserne om interoperabilitet i datastyringsloven og forslaget.

**Finansforbundet** mener, at forsvarende de udpegede fælles europæiske dataområder, vil et fælles europæisk finansielt dataområde kunne bidrage til innovation, den grønne omstilling og styrke integrationen af europæiske kapitalmarkeder. Drivkraften for delingen af data bør dog først og fremmest være forbrugerens interesse. Der skal derfor sikres positive og gavnlige forhold for forbrugerne, samt et balanceret hensyn til både datasikkerhed, -beskyttelse og dataetik.

**KL** ønsker klarhed over, hvorvidt de krav, der stilles til "operatører af dataområder" gælder de kommunale systemer. KL vurderer, at operatører af dataområder skal leve op til en række krav til beskrivelse af indhold, struktur og tekniske værktøjer til at stille oplysninger til rådighed. Umiddelbart flugter denne type beskrivelseskrav godt med den måde, danske myndigheder og kommuner har arbejdet med IT-arkitektur gennem længere tid. Dog bemærker KL, at særlige europæiske krav kan medføre en merudgift og et ressourcetræk, der kan føre til krav om økonomisk kompensation. KL bemærker herudover, at der sker et abstraktionsskred, hvor visse punkter har et teknologineutralt afsæt, mens der samtidig rettes krav direkte mod en konkret teknologi i form af intelligente kontrakter, hvilket forekommer som et unaturligt spring indenfor rammerne af den konkrete regulering. Tilsvarende bemærkning kan knyttes til den meget løsningsrettede regulering af interoperabilitet for data i cloudbaserede løsninger. KL mener, at det forekommer udfordrende, hvis det bærende element i forslaget er, om data befinder sig i en cloud fremfor eksempelvis on-premise. KL vurderer, at der ved udarbejdelse af europæiske standarder sikres indflydelse fra nationale standardiseringsorganer, hvortil KL henleder opmærksomheden på det mangeårige arbejde med fællesoffentlig standardisering gennemført i dansk regi med udvikling af både fælleskommunale og fællesoffentlige standarder og arkitekturkrav og -regler.

#### Gennemførelse og håndhævelse

**Dansk Standard** noterer sig, at der lægges op til en ambitiøs lovgivning, der stiller store krav til virksomheders og myndigheders kompetencer og viden på området, hvorfor det er vigtigt, at der indføres rimelige overgangsperioder.

**Finansforbundet** mener, at forslaget forudsætter øget nationalt og europæisk tilsyn og den nødvendige finansiering. Der kan som eksempel på finansiering til øget tilsyn findes inspiration i den danske finansielle sektors tilsynsmodel, hvor Finanstilsynet er forankret under en offentlig myndighed, men fuldt finansieret af det finansielle områdes virksomheder.

**IT-Branchen** bemærker, at håndhævelsen er delt mellem forskellige tilsynsmyndigheder og overlades til de individuelle medlemsstater. IT-Branchen er bekymret for, at denne skønsbeføjelsestilgang vil resultere i forskellige praksisser i de respektive medlemslande, hvilket ikke stemmer overens med ambitionen om at skabe en harmoniseret retlig ramme.

**KL** bemærker, at kommunerne ingen kommercielle interesser har i data, og kommunerne bør derfor ikke kunne bødesanktioneres i medfør af forslaget.

#### Sui generis-retten i henhold til direktiv 1996/9/EF

**KL** savner klarhed over, hvorvidt det har betydning for kommunerne, at *sui generis*-retten ikke finder anvendelse på databaser, hvor brugernes ret til udøvelse af deres adgangsret til IoT-data forhindres.

### **9. Generelle forventninger til andre landes holdninger**

Der er fortsat flere udeståender, herunder i forhold til:

- hvornår der foreligger et ekstraordinært behov for data hos offentlige myndigheder
- hvorvidt mikro- og små virksomheder skal undtages krav om datadeling
- hvor strenge kravene skal være til interoperabilitet mellem databehandlingstjenester, og
- hvilke krav der skal stilles angående overførsler af ikke-persondata til tredjeparter.

På telerådsmødet den 6. december vil det tjekkiske formandskab præsentere en fremskridtsrapport. Efter rådsmødet ventes formandskabet at fremsætte et tredje kompromisforslag.

### **10. Regeringens generelle holdning**

Regeringen hilser forslaget om en dataforordning velkommen og støtter ambitionen om at øge adgangen til og anvendelsen af data og sikre en mere retfærdig fordeling af data, herunder adressere techgiganters datamonopol. Regeringen anser således adgangen til og anvendelsen af data som et væsentligt fundament for udviklingen af digitale teknologier og tjenester, der kan fremme vækst, innovation og konkurrenceevne, og som derigennem kan bidrage til genopretningen af økonomien og til at løse klimaudfordringen.

Regeringen mener, at digitaliseringen skal tjene samfundets interesser ved, at digitalisering bidrager til at adressere samfundets udfordringer, mens etisk,

ansvarlig og sikker digitalisering går hånd i hånd med digital vækst. Regeringen arbejder for, at den digitale økonomi i Europa generelt kendetegnes ved et højt niveau af tillid og tryghed, samt en stærk digital konkurrenceevne baseret på innovationsfremmende og teknologineutrale rammevilkår, uden unødige byrder og barrierer.

Regeringen støtter målet om at stille flere data til rådighed for anvendelse og ser forslaget som en vigtig mulighed for at fremme en datadrevet europæisk økonomi. Regeringen finder det vigtigt, at forordningens initiativer understøtter en effektiv, ansvarlig og sikker adgang til og anvendelse af data, som skaber reel værdi for borgere og virksomheder. Endvidere mener regeringen, at virksomheders datadeling og -anvendelse skal fremmes gennem etablering af klare, forståelige og horisontale rammer for datadeling, samt gennem øget interoperabilitet mellem tjenester og decentraliseret dataudveksling.

Regeringen støtter hensigten om at etablere horisontale rammer for datadeling, der efter behov kan suppleres af sammenhængende sektorspecifik regulering. Regeringen ser positivt på, at der etableres horisontale rammer for obligatorisk datadeling, der skal finde anvendelse ved fremtidig sektorspecifik regulering. Der er behov for nærmere afklaring af de individuelle betingelser, herunder hvorvidt vilkårene for at kræve godtgørelse er tilstrækkeligt klare.

Generelt skal afklaring også bidrage til at konkretisere de økonomiske konsekvenser

Regeringen bakker op om etablering af horisontale rammer, der skal beskytte mikrovirksomheder og SMV'er mod urimelige aftalevilkår i forbindelse med datadeling. Det skal sikres, at den konkrete udformning af rammerne opnår den rette balance mellem at favne potentielle urimelige vilkår og give tilstrækkelig juridisk klarhed. Regeringen hilser yderligere initiativer til fremme af frivillig datadeling velkommen.

Regeringen ser positivt på, at brugere af IoT-genstande og -tjenester får en adgangsret til data, der genereres af de produkter, de ejer, lejer eller leaser, samt mulighed for at dele disse data med tredjeparter. Regeringen er enig i, at en regulatorisk omfordeling af data genereret af flere parter skal baseres på klare vilkår og gennemsigtighed. Regeringen vil have fokus på, at incitamentet for at indsamle og lagre data ikke fjernes.

Regeringen er enig i, at der kan være fordele ved, at offentlige myndigheder får adgang til virksomhedsdata til gavn for almenvellet særligt i samfundsmæssige kriser, men regeringen finder det essentielt, at en sådan adgangsret afgrænses til de situationer, hvor der foreligger et specifikt formål på baggrund af en offentlig nødsituation. Endvidere skal der være en klar definition af, hvad der udgør en offentlig nødsituation, herunder at der skal være tale om

en overhængende og midlertidig krise. Regeringen finder, at offentlige myndigheders adgang til og indsamling af oplysninger fra virksomhedsorganisationer eller virksomheder skal ske gennem en rimelig, forudsigelig, nem og transparent proces. Endvidere mener regeringen, at alene de kompetente myndigheder i den medlemsstat, en dataindehaver er etableret i, bør kunne kræve data stillet til rådighed på baggrund af dataforordningen, så adgang til virksomhedsdata på tværs grænser går igennem de nationale myndigheder.

Regeringen mener, at øget dataportabilitet, der sikrer en effektiv flytning af data mellem forskellige systemer og tjenester, er nødvendig for at forbedre markedet for cloudtjenester til fordel for både borgere, virksomheder og offentlige myndigheder. Regeringen støtter grundlæggende forslaget tilgang, hvor de tekniske udfordringer relateret til interoperabilitet mellem cloudtjenester søges håndteret gennem fælles standarder og formater. Regeringen finder det imidlertid vigtigt, at forpligtelserne til tjenesterne er teknisk realiserbare for både brugere og omfattede tjenester, og at der ikke skabes u hensigtsmæssige incitamentsstrukturer samt øget afhængighed af techgiganternes digitale infrastruktur.

Regeringen arbejder for, at systemer og tjenester, der kan behandle, dele og give adgang til data, bygger på fælles standarder og kan arbejde på tværs af hinanden. Derfor støtter regeringen forslaget til styrke interoperabilitet for data, hvor regeringen vil have fokus på at sikre fri og åben deltagelse i europæiske dataområder og decentral databehandling. Endvidere finder regeringen, at der er behov for klarhed over de beføjelser, Kommissionen tillægges til at udforme delegerede og implementerende retsakter, samt standarder i udmøntningen af bestemmelserne.

Regeringen finder, at dataøkonomien er grænseoverskridende af natur, hvorfor tiltag til at fremme den europæiske dataøkonomi skal fungere i den globale økonomi og respektere internationale samarbejdspartnere og handelsaftaler.

Regeringen mener, at effektiv håndhævelse er vigtigt for at opnå ambitionerne med forslaget. I den forbindelse finder regeringen, at der kan blive behov for, at sager af en vis størrelse eller grænseoverskridende karakter håndteres af et europæisk tilsyn. Regeringen vil arbejde for, at der ikke indføres unødige byrder for det offentlige i forbindelse med tilsyn og håndhævelse.

## **11. Tidligere forelæggelse for Folketingets Europaudvalg**

Sagen har været forelagt Folketingets Europaudvalg til orientering den 19. maj 2022. Der blev oversendt grund- og nærhedsnotat den 11. april 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**

*Formålet med drøftelsen på rådsmødet er at få en første politisk pejling fra medlemslandene på basis af formandskabets fremskridtsrapport. Forhandlingerne er på et tidligt stadie, og regeringen kan byde drøftelsen velkommen.*

*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<sup>4</sup> (herefter 'forslaget'). Forslaget har til formål at fastsætte fælles krav til cybersikkerhed i alle produkter med digitale elementer<sup>5</sup> (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<sup>6</sup>. 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.
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).

---

<sup>4</sup> KOM (2022) 454 – EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020

<sup>5</sup> Defineret som: ethvert software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der skal bringes i omsætning separat

<sup>6</sup> JOIN (2020) 18 – Final - EU's strategi for cybersikkerhed for det digitale årti



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<sup>7</sup>.

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 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.

---

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

Forordningen skal harmonisere EU's regler og undgå overlappende krav på området for cybersikkerhed. Forordningen skal især supplere NIS2-direktivet<sup>8</sup>, 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 radioudstyr reguleret af en delegerede retsakt<sup>9</sup> under radioudstyretdirektivet<sup>10</sup> om cybersikkerhed, der vil blive ophævet efterfølgende.

### 3. **Formål og indhold**

Formålet med drøftelsen på rådsmødet er at få en første politisk pejling i forhold til forslaget baseret på formandskabets fremskridtsrapport.

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'<sup>11</sup>. 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.

Produkter er som udgangspunkt alene underlagt producenternes egen evaluering af, hvorvidt de lever op til kravene. Kommissionen har dog udar-

---

<sup>8</sup> 2020/0359 (COD): Forslag om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148

<sup>9</sup> 2022/30/EU

<sup>10</sup> 2014/53/EU

<sup>11</sup> 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)).

bejdet 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<sup>12</sup> 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<sup>13</sup> (fx cloud-løsninger) 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 antivirus-programmer. 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: Forpligtelser 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 at de er korrekt leveret, installeret og vedligeholdt og anvendes til det tilsligtede formål eller på måder, som med rimelighed kan forudses.

<sup>12</sup> "essential requirements", jf. bilag 1 til forordningen.

<sup>13</sup> 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

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<sup>14</sup>. 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<sup>15</sup>. 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. 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

<sup>14</sup> Computer Security Incident Response Team

<sup>15</sup> Jf. Cyber Security Act (CSA), forordning 2019/881/EU om ENISA (EU's Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi.

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<sup>16</sup>. 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<sup>17</sup> 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<sup>18</sup>. 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*<sup>19</sup> til:

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

<sup>16</sup> I overensstemmelse afgørelse 768/2008/EF om fælles rammer for markedsføring af produkter.

<sup>17</sup> 2019/1020/EU

<sup>18</sup> Cyber Security Act, forordning 2019/881/EU

<sup>19</sup> Jf. artikel 290 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF)

- 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 supplerung 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. 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 informationsikkerhed for domænenavnssystemer og visse digitale tjenester<sup>20</sup>, samt

---

<sup>20</sup> Lov nr. 436 af 08/05/2018, der implementerer EU direktiv (EU) 2016/1148 (NIS)

GDPR<sup>21</sup>. Produktloven<sup>22</sup> 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<sup>22</sup>. 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 udmonter 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

<sup>21</sup> 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)

<sup>22</sup> 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 u hensigtsmæssige 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 radioudstyringsdirektivet 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<sup>23</sup> og radioudstyringsdirektivet<sup>24</sup>. 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<sup>25</sup>, 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 stadig 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.

---

<sup>23</sup> Forslag til forordning om maskinprodukter, 2021/0105(COD)

<sup>24</sup> Direktiv 2014/53/EU

<sup>25</sup> 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 underlæggende 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 unødigt 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 u hensigtsmæssigt 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 spørgsmålstejn 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 for 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 spørgsmålstejn 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 fremtidssikkert.

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 produkt-specifikke 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.

## Rådskonklusioner vedr. fremtidssikring af europæisk transport på indre vandveje (NAIADES III)

*Nyt notat*

KOM-dokument foreligger ikke.

### 1. Resumé

*På rådsmødet (Transport, Telekommunikation og Energi) 5. og 6. december 2022 vil rådskonklusionerne vedr. transport ad indre vandveje være på dagsordenen til godkendelse. Rådskonklusionerne tager afsæt i Kommissionens handlingsplan for at flytte mere godstransport til indre vandveje og at føre sektoren i retning af klimaneutralitet i 2050 ved hjælp af klimaforebyggelse og -tilpasning samt sikring af rammevilkårene for sektoren. Fra dansk side støtter man formålet om grøn omstilling af transportsektoren, herunder transport ad indre vandveje, så længe der ikke foretages tiltag/ændringer, der giver lande som Danmark en ny pligt til at implementere reglerne om indre vandveje.*

### 2. Baggrund

Kommissionen har den 24. juni 2021 med meddelelsen ”NAIADES III: fremtidssikring af transport ad indre vandveje” fremsat en handlingsplan for transport ad indre vandveje for 2021-2027 (KOM(2021) 324). Med udgangspunkt i handlingsplanen har det tjekkiske EU-formandskab udarbejdet forslag til rådskonklusioner.

Formålet med Kommissionens handlingsplan er at flytte mere godstransport til indre vandveje og at føre sektoren i retning af nul drivhusgasemissioner senest i 2050. Kommissionen lægger i handlingsplanen op til, at man vil støtte projekter til udvikling af infrastrukturen i indlandshavne og sejløb samt justere kravene til fartøjer, der sejler på indre vandveje.

Konteksten for handlingsplanen er den europæiske grønne pagt, som fastsætter et ambitiøst mål om at flytte en betydelig del af de 75 pct. af den indenlandske fragt, der i øjeblikket transporteres ad vej, over til indre vandveje og jernbaner.

### 3. Formål og indhold

Med rådskonklusionerne skitseres der en række områder, hvor transport ad indre vandveje skal forbedres og effektiviseres. Konkret opfordres der i rådskonklusionerne til, at der i sektoren for indre vandveje fokuseres på klimaforebyggelse og -tilpasning, herunder flådefornyelse og infrastruktur. Der lægges endvidere op til at efterse rammevilkårene for sektoren herunder ift. digitalisering, arbejdstageres forhold og kvalifikationer.

Der lægges i konklusionerne op til, at der tages hensyn til de forskellige medlemsstaters interne forhold samt at der tilvejebringes finansieringen til initiativerne både i eksisterende EU-programmer samt i medlemslandene.

#### **4. Europa-Parlamentets holdning**

Europa-Parlamentets holdning til konklusionerne foreligger ikke.

#### **5. Nærhedsprincippet**

Ikke relevant.

#### **6. Gældende dansk ret og forslagets konsekvenser**

Rådskonklusionerne har ikke i sig selv lovgivningsmæssige konsekvenser.

#### **7. Konsekvenser**

Rådskonklusionerne har ikke i sig selv økonomiske konsekvenser.

#### **8. Høring**

Forslaget til rådskonklusioner om NAIADES III - Fremme af en fremtids-sikret transport ad indre vandveje i Europa blev sendt i specialudvalgshøring i Skibsfartspolitisk specialudvalg med frist den 8. september 2022.

Der er modtaget høringssvar fra Danske Havne. Danske Havne stiller sig positiv over for tiltag, der vil øge nærskibsfarten og mængden af gods på sø. Danske Havne efterspørger mere fokus på klimatilpasning.

#### **9. Generelle forventninger til andre landes holdninger**

Der forventes opbakning til rådskonklusionerne fra medlemslandene – navnlig fra lande med en betydelig transport ad indre vandveje.

De medlemslande, der ikke har indre vandveje, forventes at lægge vægt på, at rådskonklusionerne ikke indeholder tiltag, der forpligter disse lande til at implementere reglerne om indre vandveje.

#### **10. Regeringens generelle holdning**

Danmark har ikke indre vandveje i EU-retlig forstand, og man har i Danmark valgt at regulere skibsfarten efter den internationale regulering fastsat af IMO (FN's søfartsorganisation) samt EU's søsikkerhedsregler som f.eks. reglerne for passagerskibe.

Fra dansk side støtter man formålet om grøn omstilling af transportsektoren, herunder transport ad indre vandveje, så længe der ikke foretages tiltag/ændringer, der giver lande - som Danmark - en ny pligt til at implementere reglerne om indre vandveje.