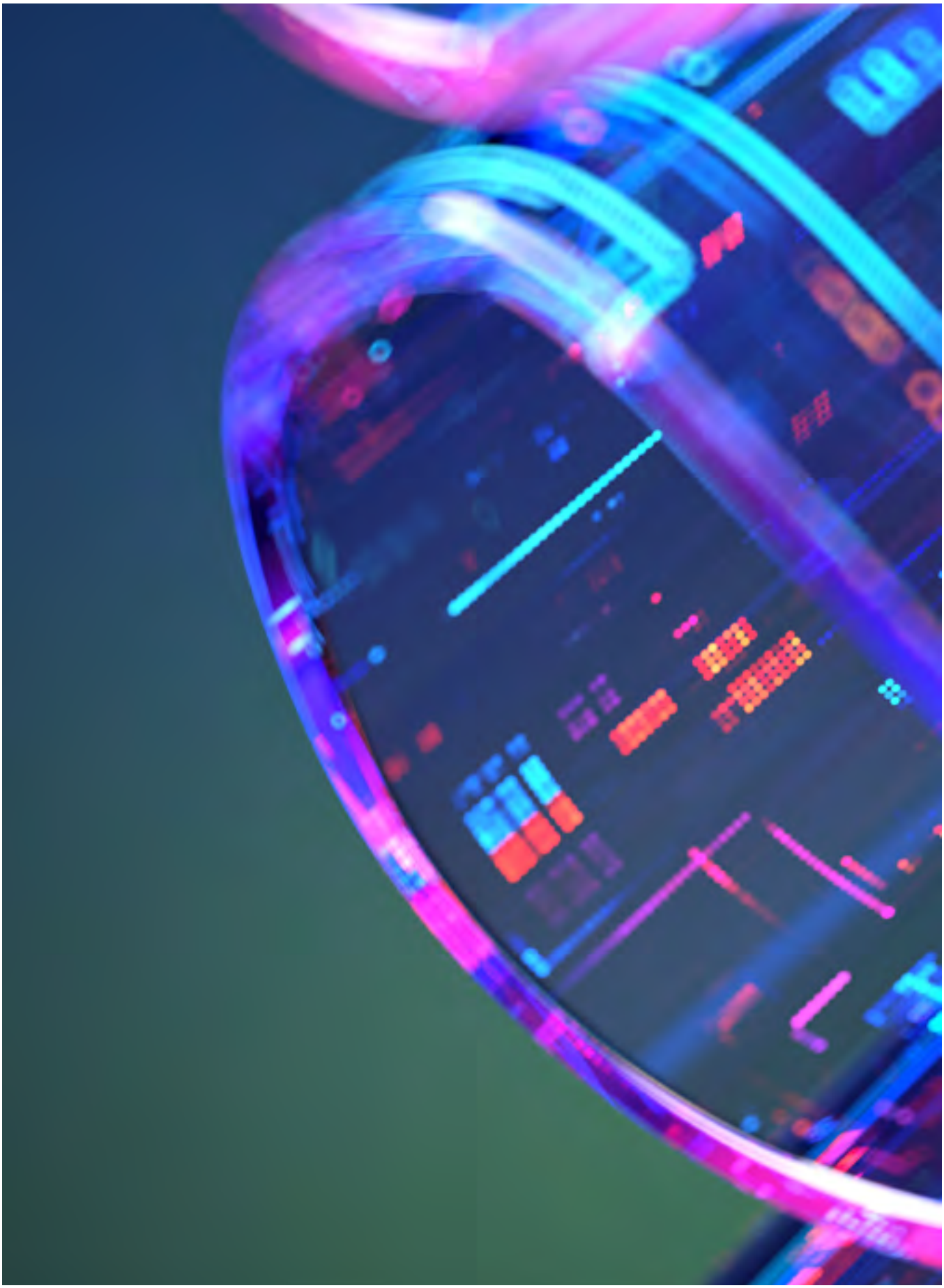
Politisk udspil · Maj 2026

Digital simplificering og suverænitet

11 veje til klare regler og digital forsyningssikkerhed

F&P FORSIKRING OG PENSION

Indhold



Tre udfordringer 11 løsninger

Introduktion

Europa har tre store udfordringer på det digitale område:

1. **Vi er bagud med innovationen.**
   Der er et innovationsgab mellem EU og tredjelande, som er særligt tydeligt på det digitale område. Vi er ikke gode nok til at mobilisere de samme innovationskræfter. Det er tydeliggjort ved, at alle de store tech-virksomheder ligger uden for Europa.

2. **Vi er for afhængige.**
   Fraværet af europæiske digitale løsninger betyder, at vi afhænger af cloud, infrastruktur og senest AI-løsninger fra tredjelandsudbydere.

3. **Vi er (mere) alene.**
   Den nye geopolitiske situation tydeliggør en helt ny udfordring. Selskaber uden for EU kan potentielt gøres til politiske våben. Uanset om selskaberne ønsker det – og uden at de kan gøre noget for at stoppe det.

Problemet er, som Draghi-rapporten også viser, at produktiviteten i EU divergerede fra USA i midten af 1990'erne særligt på det digitale område. Faktisk ville produktivitetsvæksten i EU over de seneste tyve år, hvis man ser bort fra teknologisektoren, i store træk have været på niveau med USA[1].

Blandt de primære årsager lister rapporten regulatoriske barrierer for innovation og barrierer for skalering af virksomheder.

Som følge af udviklingen ligger alle de store udbydere af digital infrastruktur, som AI og cloud-løsninger, uden for Europa, og vi har ikke alternativer, som kan matche dem på skala og kvalitet. Vores digitale forsyning afhænger med andre ord af de store cloud-udbydere.

Vi skal selvfølgelig kunne benytte os af andre lande, når de leverer en service af værdi. Danmark og EU ville aldrig være, hvor vi er i dag uden samhandel.

Brugen af de store cloud-udbydere er dog ikke uproblematisk. Udfordringen har primært været et dataproblem i forhold til overførsler af data til tredjelande. Nu er det også et geopolitisk problem, som kalder på en anden type handling.

[1] The Draghi report on EU competitiveness

Det helt centrale er, at vi skal sikre, at Europa også virker i morgen og i overmorgen.

Løsningen er ofte omtalt som "digital suverænitet", som vi desværre ofte ser oversat direkte til uafhængighed; europæisk selvforsyning, men selvforsyning, som afskærer os fra adgangen til de bedste digitale løsninger, er ikke en konkurrencedygtig løsning.

Digital suverænitet bør i stedet handle om at sikre kontrol. Kontrol over hvem, der kan tilgå systemer og vores data. Kontrol over hvem, der kan slukke.

Når vi taler suverænitet i sammenhæng med konkurrenceevne, ligger reel styrke ikke i uafhængighed, men i kontrol og valgmuligheder. At vi kan vælge mellem selvforsyning eller eksterne løsninger alt efter, hvad der giver mest værdi.

Vi skal derfor styrke rammerne for det digitale fundament, som vores virksomheder og myndigheder bygger på.

På kort bane skal vi sikre vores digitale forsyningssikkerhed, så vi har kontrol og ikke risikerer, at stikket bliver trukket, og vi skal simplificere vores regler for at styrke konkurrenceevnen uden at slække på beskyttelsen.

På lang bane skal vi se på, hvilke rammer vi kan sætte for at sikre digital forsyningssikkerhed fremadrettet - både via sikker adgang til tredjelandsløsninger, og ikke mindst ved at styrke grundlaget for at skabe europæiske alternativer.

I dette udspil kommer vi med 11 anbefalinger, som skal styrke Danmark og Europas konkurrenceevne ved at understøtte disse to områder:

1. Simplificering og klare regler.
2. Digital suverænitet og forsyningssikkerhed.

Anbefalinger

Overblik

Simplificering og klare regler

1) Reglerne gælder først, når vi ved, hvad de gælder
Ny digital regulering skal først gælde, når den nødvendige understøttelse via fx vejledninger og supplerende regler er klar.
Se hele anbefalingen på side 8.

2) Opgør med overlappende krav
Når sektorspecifik regulering overlapper med tværgående regulering, skal det være muligt at fjerne det overlap ved at give sektorreguleringen forrang.
Se hele anbefalingen på side 9.

3) Konsekvent regulering og vejledning på tværs af landegrænser
Når der laves nationale vejledninger, hvor der i forvejen findes en europæisk vejledning, skal den ansvarlige myndighed redegøre for nationale udvidelser efter et "forklar eller udelad"-princip.
Se hele anbefalingen på side 11.

4) Klare svar, når reguleringen er uklar
En tilsynsmyndighed på det digitale område skal kunne udstede et bindende svar i forhold til, hvilke krav der gælder for et digitalt system, og hvornår systemet opfylder kravene.
Se hele anbefalingen på side 12.

Suverænitet & digital forsyningssikkerhed

5) Træk ikke stikket: Hvordan sikrer vi vores digitale forsyning?
Klare og forudsigelige rammevilkår skal gøre det muligt at anvende storskala-cloud-løsninger – også når leverandøren har hovedsæde i et tredjeland.
Se hele anbefalingen på side 15.

6) Undgå krav om dobbelt drift
Det bør undgås, at brug af hyperscalers forudsætter spejling i et særskilt "rent" europæisk miljø.
Se hele anbefalingen på side 17.

7) Entydigt ansvar for den digitale forsyning
Ansvaret for at overholde EU-krav skal i højere grad placeres direkte hos leverandøren - og ikke overlades til individuelle kontraktforhandlinger mellem kunde og udbyder.
Se hele anbefalingen på side 18.

8) Bedre vilkår for investeringer
Det afsøges, hvordan der skabes bedre rammevilkår for skalering af digitale virksomheder i Europa.
Se hele anbefalingen på side 20.

9) Kapacitetsopbygning og markedsudvikling
Det offentlige er blandt de største cloud-kunder i EU. Offentlige udbud kan anvendes strategisk til at skabe efterspørgsel og opbygge åbne løsninger. Dertil skal markedet understøttes via EU-støtte målrettet cloud- og infrastrukturkapacitet.
Se hele anbefalingen på side 21.

10) Kortlæg kritisk åben software og støt vedligehold
Kortlæg, hvilke åbne systemer der kan betragtes som kritiske, fordi de udgør centrale elementer i vores digitale infrastruktur, og afsøg mulighederne for at støtte langsigtet vedligehold, sikkerhed og udvikling af disse.
Se hele anbefalingen på side 22.

11) Kritiske ressourcer - særskilt fokus på strøm
Adgang og tilgængelighed af strøm, må ikke blive en barriere for europæiske løsninger. Fokus på opbygning af pris- og miljøvenlig energiinfrastruktur og europæiske løsninger uden afhængighed af enkeltlande.
Se hele anbefalingen på side 23.

Simplificering og klare regler

Opgør med regulatoriske udfordringer

Det er let at pege på regulering som den gennemgående barriere for vores manglende konkurrenceevne på det digitale område. Men det er vigtigt at anerkende, at regulering findes, fordi vi ikke ønsker, at Danmark og EU ender som fx Kina eller USA.

Vi ønsker fokus på ansvarlighed og rettigheder. Det gør vi ved at omsætte vores værdier og fundamentale rettigheder til regulering.

Vi står bag den europæiske tilgang. Det betyder, at regulering er et grundvilkår, fordi det er nødvendigt for at bibeholde de værdier, vi ønsker at bevare - også selvom det koster på konkurrenceevnen.

Men det betyder ikke, at reguleringen skal være unødig besværlig eller blive en unødig barriere for vores digitale konkurrenceevne i Danmark og EU.
Derfor kommer vi i dette afsnit med en række konkrete forslag til at simplificere reguleringen, samtidig med at vi holder fast i den ansvarlige tilgang.

Reglerne gælder først, når vi ved, hvad de gælder

Anbefaling 1: Betinget anvendelse af lovgivning

Der mangler ikke tempo i udviklingen af ny lovgivning – særligt på EU-plan. Til gengæld må virksomhederne vente længere og længere på de vejledninger, delegerede retsakter, standarder og andet materiale, som skal skabe klarhed om omfang, processer og understøtte, at virksomhederne i praksis kan implementere reglerne.

Særligt når regulering bliver kompleks, er det reglen mere end undtagelsen, at den nødvendige vejledning først lander, når reguleringen er begyndt at gælde. Det sker primært, fordi det viser sig, at reglerne ikke var så lette at omsætte til praksis hos de ansvarlige myndigheder, som først forventet. Desværre løser vi problemet ved at skubbe opgaven over på virksomhederne.

Når vejledninger, standarder og andet understøttende materiale ikke er klar, så koster det unødige kræfter hos virksomhederne, som hver især må bruge ressourcer på at lave deres egen vurdering, af, hvad lovgiver egentlig har tænkt. Præcis den opgave, som vejledningerne skulle løse. Derfor er lovgiver nødt til at tage ansvar for, at der også er tid til at levere den nødvendige vejledning til virksomhederne i rimelig tid, **inden** reglerne gælder.

Hvis den nødvendige understøttelse er klar, når lovgivningen gælder, vil det reducere unødige byrder – uden det går på kompromis med den tiltænkte beskyttelse.

Den manglende afklaring skaber samtidig unødige barrierer i forhold til brugen af digital teknologi, fordi fx AI-projekter sættes på pause, mens virksomheder og myndigheder venter på den nødvendige afklaring.

Anbefaling
Vi anbefaler, at:

- Tidspunktet for anvendelsen af ny digital regulering er betinget af, at den nødvendige understøttelse er klar, og at der gives reel tid til implementering, inden reglerne finder anvendelse.
  Minimum seks måneder.

Fx at reguleringen først finder anvendelse seks eller 12 måneder efter den overordnet ansvarlige myndighed vurderer, at den nødvendige understøttelse – fx delegerede retsakter (RTS'er), vejledninger, standarder, mv. - er klar i den nødvendige kvalitet og formelt godkendt af de relevante organer i EU.

Opgør med overlappende krav

Anbefaling 2: Fjern overlappende krav gennem klare overens-stemmelsesvurderinger og hjemmel til oprydning i dobbeltkrav

På det digitale område har vi fået en række tværgående regler fx GDPR, AI-forordningen, cybersikkerhedskravene i Cyber Resilience Act, og mere er på vej. Den voksende mængde af tværgående regulering giver flere steder markante overlap med sektorspecifik regulering. Dette er en kendt udfordring i alle brancher med særregulering.
I den finansielle sektor overlapper fx GDPR, AI-forordningen og Cyber Resilience Act med sektorkravene i Solvens II og Digital Operational Resilience Act (DORA).

Det gør overholdelsen af regelsættene kompleks, og virksomhederne må bruge unødig tid på at opfylde overlappende krav. Lige nu lægges byrden ved overlappende regler alene hos virksomhederne. Det er ikke rimeligt.
Derfor er vi nødt til at se på mulighederne for at skabe mere sammenhæng mellem tværgående regler og sektorregler.

Der bør være et klart ansvar hos myndighederne i forhold til at kunne fjerne overlap i de regler, de er ansvarlige for. Men det juridiske værktøj til at løse denne opgave mangler.

Fortsættes på næste side

Eksempel: Oprydning i overlap

Et eksempel på udfordringen er sammenfaldet mellem Solvens II og AI-forordningen i forsikring- og pensionsbranchen. Solvens II pålægger selskaber risikostyring, governance og interne kontroller. Disse krav overlapper med AI-forordningens højrisikokrav.

Når et Solvens II-reguleret selskab anvender et højrisiko AI-system, bør det være muligt, at Solvens II-procedurer - som adresserer de samme risici som AI-forordningen (modelrisiko, governance, interne kontroller) - kan erstatte eller supplere kravene i AI-forordningen.

Tilgangen er allerede indarbejdet for nogle artikler i AI-forordningen, men der mangler en generel overordnet mekanisme, som lovteknisk gør det muligt at simplificere resterende overlap.

Anbefaling

Vi foreslår derfor:

- At der i tværgående regulering indarbejdes en generel regel, som giver mulighed for at fjerne krav, som overlapper med sektorregulering. Det kan ske, når krav i sektorregulering opfylder samme formål som tværgående krav og sikrer et tilsvarende beskyttelsesniveau.

I praksis kan det ske ved, at sektormyndighederne ved overlappende regler giver beføjelser til at:

1. vurdere overlap ved at gennemføre en overensstemmelsesvurdering.
2. fastsætte gældende betingelser for om sektorregulering kan komplimentere eller helt erstatte krav eller processer i tværgående regulering.

Ved EU-regulering styres brugen af værktøjet af de overordnede tilsynsmyndigheder på EU-niveau. For national regulering kan samme tilgang benyttes af nationale tilsyn.

Hvis sektorreguleringen alene komplimenterer tværgående krav, skal det være tydeligt, hvilke dele af tværgående krav, der løftes eller ikke løftes fuldt ud af sektorregulering.

Konsekvent håndhævelse og vejledning på tværs af landegrænser

Anbefaling 3: Når EU-reglerne er ens, skal de håndhæves på samme måde - uanset om du er i Danmark, Sverige eller Italien

Målet med harmoniserede regler er, at de skal fungere gnidningsløst på tværs af EU-grænser. Hvis vi ønsker at styrke et indre marked, skal vi også sikre, at vores regler er tydelige og ens på tværs af lande.

Manglende harmonisering skyldes fx, at tilsynsmyndighederne læser lovgivningen forskelligt, og nogle tilsynsmyndigheder omsætter lovgivningen til flere krav end andre.

Dertil opleves det, at nationale vejledninger går videre og sætter flere krav end en vejledning fra den overliggende europæiske tilsynsmyndighed.

Samtidig opstår byrder hos virksomhederne i forbindelse med, at der skal udarbejdes information eller rapportering, som alene eller primært er til brug for et tilsyn.

Der kan være gode grunde til, at det skal udarbejdes, men det bør altid kræve en ekstra overvejelse, når krav alene handler om information og rapportering til myndigheder og ikke direkte bidrager til beskyttelse og opfyldelse af lovens formål.

Anbefaling

Med dette afsæt har vi følgende anbefalinger:

- Når der laves nationale vejledninger på områder, hvor der i forvejen findes en europæisk vejledning, skal der udarbejdes et "konsistenstjek" af den nationale vejledning, hvor det vurderes om vejledningen går videre end den europæiske vejledning. Hvis vejledningen går videre, skal myndigheden forklare, hvorfor tilgangen er valgt eller fjerne udvidelsen.

- Hver eneste gang der udarbejdes regler eller vejledninger – både nationalt og på EU-plan – bør der være en grundig afvejning af formuleringer i forhold til dokumentationspligter og rapporteringskrav.

Hvis krav alene har til formål at informere en myndighed eller udarbejde dokumentation, som alene skal ligge klar til en myndighedsforespørgsel eller et tilsyn, skal det altid overvejes, om kravet kan løftes på anden vis - og det skal som minimum godtgøres, hvorfor kravet er nødvendigt - og hvilket detaljeniveau, der er tilstrækkeligt for at løfte lovens formål.

Klare svar, når reguleringen er uklar

Anbefaling 4: Indfør bindende svar på det digitale område

Antallet af sider i den digitale regulering udvikler sig (desværre) i samme tempo som teknologien. I proces er fx Digital Fairness Act, Digital Networks Act og EU Cloud and AI development Act. Nye regler skaber nye uklarheder og et behov for klare svar.

For at øge retssikkerheden, skabe klarhed og konsistent håndhævelse på tværs af EU's digitale regulering bør det være muligt at bede europæiske og nationale kompetente myndigheder om at afgive bindende svar, der præciserer forståelsen af de digitale regler for en konkret digital løsning.

Vi kender i dansk regi allerede tilgangen fra skatteområdet, hvor det er muligt at få et bindende svar, hvis man er i tvivl om, hvad en handling vil betyde for betaling af skat, moms eller afgifter.

Bindende svar på det digitale område vil give erhvervslivet mulighed for at opnå sikkerhed vedrørende anvendeligheden, omfanget af eller opfyldelsen af de digitale regler. Tilgangen er særskilt relevant for det digitale område, der ofte involverer nye eller komplekse teknologier, som udvikler sig hurtigt.

Anbefaling
Vi foreslår, at:

- En tilsynsmyndighed på det digitale område skal kunne udstede et bindende svar, der bekræfter om et specifikt digitalt system eller en afgrænset systemkonfiguration enten:
  1. falder ind under anvendelsesområdet for et bestemt regelsæt (Er vi omfattet?),
  2. er underlagt bestemte forpligtelser (Hvad er kravene?), eller
  3. ud fra en konkret vurdering anses for at opfylde gældende krav; og hvis ikke beskrivelse af de elementer, som udestår (Gør vi det rigtigt, hvad mangler?)

- Bindende svar bør som minimum etableres som en gennemgående mulighed ved brugen af regulatoriske sandkasser.

For at bevare fleksibilitet og undgå at fastlåse tilsynet, er de bindende svar systemspecifikke (knyttet til en konkret teknisk eller organisatorisk opbygning), eventuelt tidsbegrænsede, og underlagt revision eller tilbagekaldelse, hvis de konkrete omstændigheder ændrer sig.

Et bindende svar skal være retligt bindende for den udstedende myndighed, men ikke for domstolene. Svarene kan ikke ændre lovgivningen eller reducere beskyttelsesniveauet, men alene præcisere dens anvendelse og opfyldelse i en konkret situation.

Ser vi bredere end dansk kontekst, kunne bindende svar indføres som et generelt værktøj, der kan anvendes på tværs af EU's digitale dagsorden.

Digital suverænitet

Digital forsyningssikkerhed og konkurrenceevne

Digital suverænitet er evnen og retten til selvstændigt at kontrollere, regulere og beskytte sin digitale infrastruktur, data, teknologi og digitale processer - uden uforholdsmæssig afhængighed af eller indblanding fra eksterne aktører.

Vi står i en ny geopolitisk situation, som nødvendiggør, at vi ser mere kritisk på udbydere af digital infrastruktur fra tredjelande og vores afhængighed af dem. Det skyldes ikke kvaliteten i deres produkter, tiltroen til den enkelte aktør eller deres ageren, men alene den geografiske placering af deres hovedkvarter.

Der er en særskilt udfordring i forhold til de store tech-selskaber, der udbyder digital infrastruktur i form af fx cloudløsninger og software-as-a-service. De bliver kaldt hyperscalers - og er i overvejende grad udbydere placeret i tredjelande udenfor EU.

Flertallet af europæiske og danske virksomheder benytter de store hyperscaler-udbydere som en integreret del af deres forretning. Det gør de, fordi der ikke findes reelle alternativer til de services, den kvalitet eller den skala, som de store hyperscalers kan levere på AI, cloud og software-området. Disse leverandører udgør de facto kritisk digital infrastruktur.

Derfor er vi nødt til at forholde os til, at vi kan stå i en geopolitisk situation, hvor adgangen til leverandører placeret i udlandet begrænses eller i værste fald afskæres helt. Der kan blive slukket for forsyningen.

Etablering af europæiske alternativer vil tage tid. Selv med markante europæiske investeringer er det uvist, om det på lang sigt overhovedet er muligt at opnå samme kvalitet i europæiske løsninger.

Dermed er uafhængighed i form af krav om "selvforsyning" ikke en konkurrencedygtig løsning, hvis det afskærer os for adgang til de bedste løsninger.

Der findes ikke lette eller hurtige løsninger på udfordringen. Vi er i stedet nødt til at arbejde i to spor, der samlet set handler om at skabe digital forsyningssikkerhed:

1. **På kort sigt:** Sikre stabil og sikker adgang til eksisterende hyperscaler-løsninger uden at "trække stikket".

2. **På mellemlangt og langt sigt:** Opbygge europæisk kapacitet og reducere strategisk afhængighed - uden at svække konkurrenceevne og innovation. Kombineret med fortsat fokus på ikke at svække konkurrenceevnen ved at fjerne adgangen til state-of-the-art-løsninger, når disse ligger uden for EU.

Del 1: Anbefalinger med effekt på kort sigt

Træk ikke stikket: Hvordan sikrer vi vores digitale forsyning?

Anbefaling 5: Sikker og stabil adgang til vores digitale forsyning

Leverandører af digital infrastruktur og cloudservices er forsyningsvirksomheder, som vi ikke længere kan undvære.

En undersøgelse fra EU-parlamentet i december 2025 viser, at AWS, Microsoft Azure og Google Cloud sidder på omkring 70 pct. af EU-markedet.
Derfor vil alle brancher i større eller mindre grad blive ramt, hvis stikket trækkes - uanset om det sker via europæisk regulering eller fra den anden side af Atlanten.

For at undgå et digitalt blackout og for at bevare konkurrenceevnen, er det derfor vigtigt:

1. Ikke at trække stikket til hyperscaler-løsningerne.
2. Sikre vilkår, der bidrager til, at hyperscalers på sikker og ansvarlig vis kan levere ydelser i EU.

Den enkelte virksomhed har ikke ressourcer og forhandlingsposition til for alvor at ændre vilkårene, men adgangen til det samlede europæiske marked er en helt anden størrelse.

EU skal bruge sin markedsposition til at opbygge digital suverænitet, der sikrer, at vi selvstændigt kontrollerer, regulerer og beskytter vores digitale infrastruktur, data, teknologi og digitale processer - uden indblanding fra eksterne aktører.

Jurisdiktions-udfordringen

En af de største udfordringer for europæisk digital suverænitet er, at europæiske data, der ligger i løsninger fra tech-selskaber i tredjelande, ultimativt er underlagt jurisdiktion og lovgivning i tredjelandet fx via US Cloud Act, selvom serverne står i Europa.

Det betyder, at regeringer i tredjelande kan bruge tech-selskaberne som politiske instrumenter til at udnytte den europæiske afhængighed.

Løsninger som 'sovereign cloud', hvor data alene placeres i Europa og sikres med krypteringsnøgle, løser ikke problemet med jurisdiktion, da US Cloud Act fx åbner mulighed for, at leverandører tvinges til at aflevere krypteringsnøgle eller dekryptere data, hvis det er muligt for dem[2].

[2] European Software and Cyber Dependencies, Policy Department for Transformation, Innovation and Health Directorate-General for Economy, Transformation and Industry Authors: Vaida GINEIKYTE-KANCLERE, Militsa EGGERT, Goda SKIOTYTE - December 2025

Anbefaling
Der bør etableres klare og forudsigelige rammevilkår, som gør det muligt at anvende storskala-cloudløsninger - også når leverandøren har hovedsæde i et tredjeland.

- Der bør på EU-niveau indføres tekniske og regulatoriske garantier, der sikrer, at data forbliver og behandles inden for EU og alene er underlagt europæisk jurisdiktion.

- På EU-plan skal det afdækkes, hvordan man minimerer eller fjerne risikoen for, at administrationen i tredjelande kan tilgå eller slukke for adgang til systemer og/eller data i strid med EU-regler eller mod leverandørens vilje.

Herunder bør det afdækkes, hvilke muligheder der er i forhold til WTO-reglerne for at indføre særlige krav på området. Sådanne garantier vil gøre det muligt og mere sikkert at benytte tredjelandsleverandører, der driver datacentre i Europa.

Det skal sikres:
- At sådanne garantier får reel effekt for tredjelandsleverandører, der opererer datacentre i Europa.
- At regulering ikke utilsigtet bliver en barriere, der svækker europæiske virksomheders konkurrenceevne.
- At regler udformes med udgangspunkt i europæiske værdier og virksomheders behov - ikke leverandørernes forretningsmodeller.

Formålet er at skabe grundlaget for kontrolleret og sikker brug; ikke eksklusion af ikke-europæiske leverandører.

Undgå krav om dobbelt drift

Anbefaling 6

Anbefaling
Det bør undgås, at brug af hyperscalers forudsætter spejling i et særskilt "rent" europæisk miljø.

Dobbelt drift i form af parallel infrastruktur:
- Øger omkostninger markant,
- skaber teknologisk kompleksitet,
- reducerer effektivitet,
- uden nødvendigvis at forbedre den reelle sikkerhed.

Der bør i stedet fastlægges rammer, der fokuserer på robusthed, jurisdiktionsklarhed og leverandøransvar fremfor parallel infrastruktur.

Entydigt ansvar for den digitale forsyning

Anbefaling 7: Styrk leverandøransvaret på EU-niveau og skab et samlet regelsæt for digitale infrastrukturudbydere

Ansvar og sikkerhed går hånd i hånd. Kan ansvaret afskrives, så forsvinder den lovede sikkerhed. Det gælder, uanset om udbyder er placeret i et tredjeland eller i Europa.

Vi foreslår derfor, at det afsøges, hvordan ansvar for overholdelse af centrale EU-krav i højere grad placeres direkte hos leverandøren og ikke overlades til individuelle kontraktforhandlinger mellem kunde og udbyder.

Der findes ingen regulering, der eksplicit adresserer hyperscalers og andre udbydere, når de har en størrelse og udbredelse, som gør, at de i praksis er kritiske for vores digitale infrastruktur.

I stedet er reguleringen af digital infrastruktur fragmenteret. Regelsæt som DORA, NIS2-direktivet, Digital Markets Act, Digital Services Act og GDPR adresserer hver deres del af den digitale økonomi – finansiel robusthed, cybersikkerhed, markedsadfærd, platformansvar og databeskyttelse.

De enkeltstående regelsæt resulterer i et utal af overlap og enslydende krav, som virksomheder og myndigheder hver for sig skal løfte i deres aftaler med den samme fællesmængde af fx hyperscalers.
Det er bøvlet og besværligt, og det løfter ikke den samlede sikkerhed, at alle hver for sig skal bruge tid på at stille de samme krav til de samme udbydere.

Samtidig er der behov for, at reguleringen bidrager til at undgå, at virksomheder låses fast i enkelte løsninger, fordi fastlåsning og manglende mulighed for at skifte mellem leverandører svækker konkurrencen og udvikling/innovation.

Anbefaling
Vi anbefaler derfor, at der etableres en reguleringsramme for digital forsyning med kritisk volumen på tværs af sektorer, med:

- Ensartede krav til robusthed og sikkerhed
- Klar jurisdiktionsafklaring
- Samlet tilsyn
- Samordning med eksisterende regler

Konkret bør følgende reguleres for udbydere, der har en størrelse og udbredelse, som gør, at de er kritiske for vores digitale infrastruktur.

- Centrale compliance-krav skal løftes på lovniveau og pålægges leverandøren direkte (fx krav om rette sikkerhedsforanstaltninger, ansvar for kravene til egne underdatabehandlere, samt design af løsninger, der efterlever databeskyttelsesprincipperne). Det er væsentligt, at de enkelte virksomheder ikke hver for sig skal løfte tværgående lovkrav på aftaleniveau.

- Visse forpligtelser (fx datasikkerhed og regulatorisk overholdelse) skal ikke kunne fraskrives kontraktligt.

- Krav om at leverandørerne foretager sikkerhedsrevisioner og compliance-rapportering til EU-myndigheder.

- Et fælles europæisk tilsyn med reelle sanktionsmuligheder inspireret af strukturen i Forordning om digital operationel modstandsdygtighed i den finansielle sektor (DORA).

- Afdække om eksisterende krav til portabilitet af data, interoperabilitet og API-åbenhed er tilstrækkelige til at sikre, at virksomheder og myndigheder ikke låses fast i leverandørspecifikke systemer.

Del 2: Anbefalinger med effekt på lang og mellemlang sigt

Skab europæiske alternativer

Styrk europæisk og dansk digital infrastruktur

Fraværet af europæiske løsninger betyder, at der i dag ikke findes direkte alternativer til de store hyperscalers i Europa.

Mens hyperscalerne i dag løfter behovet for digital infrastruktur, cloud og AI, så vil tilstedeværelsen af europæiske alternativer kunne mitigere den geopolitiske risiko og øge konkurrencen på markedet.

Europæiske alternativer opstår ikke spontant i et marked, hvor globale aktører allerede opererer med massiv storskalaøkonomi. Hvis EU på længere sigt skal opbygge relevante alternativer, kræver det en aktiv industripolitisk indsats.

Men hvad skal der ske på den korte bane, hvis vi håber at se europæiske alternativer på den lange bane?

Vi anbefaler, at en aktiv indsats rettes mod tre indsatsområder:

- Kapacitetsopbygning og markedsudvikling.
- Bedre vilkår for investeringer.
- Stærke økosystemer.

Bedre vilkår for investeringer

Anbefaling 8

For at skabe europæiske alternativer skal europæiske tech-virksomheder have gode muligheder for at vækste, blive i Europa og styrke den digitale innovation her. Men ingen virksomheder vokser uden investeringer.

Mange virksomheder i vækstsegmentet i Danmark og Europa har i dag svært ved at tiltrække privat kapital. Desværre er oplevelsen, at det er lettere at investere fra og rejse penge i fx USA. Så mens mange digitale virksomheder starter i EU, så skaleres de uden for EU.

En mulighed for at rejse mere kapital kan være fra de store, institutionelle investorer herunder pensionsbranchen, som er store spillere i nogle europæiske lande. Her eksisterer en del barrierer, som skal overvindes, hvis mere kapital skal flyde til europæiske tech-virksomheder og -projekter.

En udfordring er blandt andet, at risikoen i især venture- og growth-virksomheder er større end i fx obligationer og børsnoterede aktier.

En anden er, at det er sværere og mere omkostningstungt for en europæisk institutionel investor at håndtere disse investeringer. Det kræver flere personer - ofte med specialistviden. Institutionelle investorer er underlagt et tilsyn, der ofte også kræver omfattende dokumentation og rapportering.

En tredje er, at Danmark og EU ikke i samme grad har dyrket gode økonomiske rammevilkår for venture og tech-virksomheder, sådan som det har været i USA i årtier. Og så har USA et meget stærkt, effektivt og veludbygget kapitalmarked – både i forhold til børsnoterede og ikke-børsnoterede markeder. Der er derfor behov for i højere grad at bygge bro mellem de institutionelle investorer og vækstvirksomhederne, hvis den europæiske investeringsmuskel for alvor skal aktiveres.

Anbefaling
Vi anbefaler derfor, at:

- Det afsøges, hvordan der skabes bedre rammevilkår for skalering af digitale virksomheder i EU. Herunder:
  - At medlemslandene skal have bedre mulighed for at etablere (nationale/statslige) fonde rettet mod vækstvirksomheder og sektorer med finansieringsudfordringer fx digitalinfrastruktur.

    Via statslig tabsgaranti (first loss) og/eller forrang ift. fordeling af muligt afkast (preferential treatment) skal de nationale fonde sænke risikoen for institutionelle investorer, som derigennem kan investere et væsentligt større beløb i vækstvirksomheder. Som led heri bør der laves et konkurrenceeftersyn af EU's statsstøtteregler med henblik på at øge fleksibiliteten i forhold til statsstøtte.

  - At der etableres flere europæiske fonde, som Scaleup Europe Fund, målrettet vækstvirksomheder, samt at European Tech Championship Initiative udbygges betydeligt i de kommende år. Der bør tillige arbejdes for muligheden for en europæisk fondsmodel med mulighed for tabsgaranti ved de særligt risikofyldte virksomheder og kritiske sektorer og teknologier, som kan supplere de nye, nationale fonde. Det kan fx være igennem Den Europæiske Investeringsbank og EIF.

Kapacitetsopbygning og markedsudvikling

Anbefaling 9

Anbefaling

Det offentlige er en af de største cloud-kunder i EU og har en tilsvarende interesse i at sikre digital suverænitet både i Danmark og EU. Derfor anbefales det, at offentlige udbud anvendes strategisk til at:

- Skabe efterspørgsel efter europæiske løsninger.
- Stille krav om interoperabilitet og dataportabilitet.
- Fremme flerleverandør-arkitekturer (multi-cloud).
- Opbygge løsninger som efterfølgende åbent kan benyttes.

Det skal dog ske uden protektionisme, der strider mod WTO-forpligtelser. Fokus bør være på kvalitet, funktionelle krav og sikkerhedsstandarder - ikke leverandørens nationalitet.

Samtidig bør markedet generelt understøttes via EU-støttede investeringsrammer målrettet cloud- og infrastrukturkapacitet (via EIB/InvestEU-lignende strukturer fx European Tech Champions Initiative).

Kortlæg kritisk åben software og støt langsigtet vedligeholdelse

Anbefaling 10

Open source indgår allerede i dag som en central komponent i cloud og it-systemer fx database-software og operativsystemer. En udfordring i økosystemet er vedligeholdelse - fx sikkerhedsbiblioteker, som vedligeholdes af små teams eller enkeltpersoner på frivillig basis.

Et stærkere open source-økosystem vil styrke mulighederne for at opbygge nye løsninger og øge konkurrencen på markedet.

Anbefaling
Det anbefales derfor, at:

1. Kortlægge kritisk åben software: Hvilke åbne systemer kan betragtes som kritiske, fordi de udgør centrale elementer på tværs af den digitale infrastruktur.

2. Afsøge mulighederne for at støtte langsigtet vedligehold, sikkerhed og udvikling af disse løsninger, fx gennem direkte støtte eller øremærkede midler i offentlige open source-baserede projekter eller oprettelse af EU-organ, som bidrager til opgaven.

Kritiske ressourcer

Anbefaling 11: Særskilt fokus på strøm

Ingen software uden hardware. Mens adgangen til fx kritiske råmaterialer er nødvendig for at bygge hardware, så er én ressource nødvendig for at holde digital infrastruktur kørende; nemlig strøm.

Modsat sjældne jordarter kan strøm ikke flyttes over store afstande. Dermed er adgangen til energi kritisk for at skalere digitale løsninger. Samtidig er pris- og miljøvenlig energi en stærk forudsætning for at tiltrække investeringer i særligt digital infrastruktur til EU.

Danmark kan med sine omfattende havvindressourcer spille en helt central rolle i forhold til at levere den nødvendige grønne strøm, men fordi adgangen til energinettet er udfordret, er placering af forbrug i forhold til produktion vigtig, og der kan være behov for at tænke forbrug og produktion sammen og fx gøre brug af lokale energisystemer med egen energiproduktion og energilagring i form af fx microgrids.

Der er et kapacitetsproblem under opbygning - og det vil også ramme mulighederne for at udbygge europæisk digital infrastruktur fx datacentre, der skal sikre suverænitet og kunne konkurrere med udenlandske løsninger.

Danmark har gode forudsætninger for prisgunstig og rigelige mængder strøm på grund af vind og sol. Omvendt er der betydelige udfordringer med at sikre nok kabel- og tilslutningskapacitet. Udbygningen af elnettet er derfor væsentlig i indsatsen for at udbrede den digitale udvikling i Danmark og Europa og opnå en højere grad af digital suverænitet.

Anbefaling
Vi anbefaler derfor, at der sættes særskilt fokus på:

- Opbygning af pris- og miljøvenlig energiinfrastruktur.
- Sikring af europæisk suveræne løsninger uden afhængigheder af enkeltlande, herunder stærkere samarbejde om og udvikling af fx el- og energiforsyning på tværs af landegrænser.
- Adgang og tilgængelighed af strøm må ikke blive en barriere for europæiske løsninger (i praksis både digitale og al anden industri). Dette sikres bl.a. gennem hurtigere myndighedsbehandling til godkendelse af projekter vedr. elnet og -projekter.

F&P

Philip Heymans Allé 1
2900 Hellerup
Telefon 41 91 91 91
fp@fogp.dk
www.fogp.dk