VEDLEGG

DET KONGELIGE DIGITALISERINGS- OG FORVALTNINGSDEPARTEMENT

Statsråden

Stortingets kommunal- og forvaltningskomite
0026 OSLO

Deres ref	Vår ref	Dato
	26/590-12	06. mars 2026

Dokument 8:119 S (2025-2026) Representantforslag fra stortingsrepresentantene Ingrid Fiskaa, Marthe Hammer, Sunniva Holmås Eidsvoll, Mirell Høyer-Berntsen, Kirsti Bergstø og Anne Lise Gjerstad Fredlund om digital suverenitet i en urolig tid

Jeg viser til Kommunal- og forvaltningskomiteens brev av 13. februar 2026 der dere ber om min uttalelse til Dokument 8:119 S (2025-2026) Representantforslag fra stortingsrepresentantene Ingrid Fiskaa, Marthe Hammer, Sunniva Holmås Eidsvoll, Mirell Høyer-Berntsen, Kirsti Bergstø og Anne Lise Gjerstad Fredlund om digital suverenitet i en urolig tid.

Innledning

Den mest alvorlige sikkerhetspolitiske situasjonen etter 2. verdenskrig gjør at arbeidet med digital sikkerhet og beredskap er en av regjeringens viktigste prioriteringer. Som statsministeren understreket i sin sikkerhetspolitiske redegjørelse 12. februar 2026: Vi lever i en tid med mer utilslørt maktbruk fra stormakter, større uforutsigbarhet og et enda større alvor. Dette arbeidet er avgjørende for å ivareta kritiske samfunnsfunksjoner og grunnleggende nasjonale funksjoner. Digital suverenitet bør ikke forstås som full nasjonal kontroll, men som vårt digitale handlingsrom – evnen til å handle selvstendig og strategisk i en digitalisert verden, også når vi er avhengige av andre.

Det digitale Norge er bygget på kritisk digital infrastruktur og et komplekst og omfattende digitalt økosystem, hvor det finnes strukturelle og systemkritiske avhengigheter med betydning for nasjonal sikkerhet og totalberedskap. Digital suverenitet kan ikke bygges gjennom norsk alenegang. Regjeringens garderingsstrategi, som prioriterer dypere og mer forpliktende samarbeid med nordeuropeiske partnere, gjelder like fullt på det digitale området

Postadresse: Postboks 8004 Dep 0030 Oslo
Kontoradresse: Akersg. 59 Telefon* 22 24 90 90
Org no.: 932 384 469

som på det militære. Det er behov for økt samarbeid og digital samhandling innenfor rammen av totalforsvaret og med allierte i Norden, EU og NATO.

Regjeringens strategiske retning, prioriteringer og tiltak for å ivareta digital sikkerhet er nedfelt i Meld. St. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet* og Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen - Forberedt på kriser og krig*. Regjeringen har utpekt 2026 til Totalforsvarsåret, og vil i løpet av året for første gang legge frem en langtidsplan for sivilt beredskap med særlig vekt på kritisk digital infrastruktur. Skal vi opprettholde og styrke vår digitale motstandskraft, er det viktig å delta i internasjonale samarbeid.

Nedenfor følger vurderinger av enkeltforslagene som er fremmet. Justis- og beredskapsministeren har gitt innspill til vurderinger av forslagene 2, 3 og 5. Næringsministeren har gitt innspill til vurderinger av forslag 6. Jeg vil understreke at disse vurderingene må leses i lys av den nasjonale sikkerhetsstrategiens tre pilarer; forsvarsevne, motstandsdyktighet og økonomisk sikkerhet, som alle har direkte relevans for digital suverenitet. Til sist gir jeg en overordnet og samlet vurdering av forslagene.

1. Stortinget ber regjeringen fastsette digital suverenitet som et overordnet mål i Norges digitaliseringsstrategi

I Norges digitaliseringsstrategi slår regjeringen fast at vi vil «sikre tilstrekkelig nasjonal kontroll med den delen av den digitale grunnmuren som understøtter kritiske samfunnsfunksjoner». I strategien slås det også fast at regjeringen frem mot 2030 vil styrke nasjonal digital sikkerhet og beredskap slik at kritiske samfunnsfunksjoner og grunnleggende nasjonale funksjoner blir ivaretatt. Videre slår regjeringens plan for Norge tydelig fast at både konkurransekraft og nasjonal sikkerhet er viktig fremover.

For å følge opp dette jobber aktivt for å øke vårt digitale handlingsrom. Med digitalt handlingsrom mener jeg evnen til å handle selvstendig og strategisk i en digitalisert verden, også når vi er avhengige av andre. Jeg oppfatter representantenes deler regjeringens ambisjon om at Norge skal ha mest mulig digitalt handlingsrom, og mener dette er godt dekket innenfor dagens strategi. Det er derfor ikke nødvendig med digital suverenitet som eget mål.

Begrepet digital suverenitet kan også være misvisende, ved at det kan gi inntrykk av at Norge skal gå alene. I arbeidet med å sikre diversitet, motvirke markedskonsentrasjoner og unngå «single points of failure» eller sårbarheter på det digitale området generelt og innen KI spesielt, – er ikke norsk alenegang svaret. Vi må samarbeide med andre.

Et styrket digitalt handlingsrom avhenger av tilgang på kritiske innsatsfaktorer som komponenter, kommunikasjonslinjer, datasentre, sky, programvare og KI-modeller («full-stack» eller verdikjedeavhengighet) – men også av hvordan vi bruker teknologien, hvilken kompetanse vi besitter, og hvilke reguleringer og normer som rammer den inn. Derfor samarbeider vi tett med Norden, EU og andre partnere for å sikre handlingsrom, felles

standarder og bedre alternativer. Den økte innsatsen for digitalt handlingsrom i Norden og EU styrker dette arbeidet, og Norge deltar konstruktivt i å forme den felles retningen.

Jeg viser for øvrig til svar på spørsmål 4.

2. **Stortinget ber regjeringen sikre oppretting av en nasjonal skytjeneste som eies og driftes av det offentlige, for lagring av data og som et offentlig arbeidsverktøy**

På oppdrag fra Justis- og beredskapsdepartementet (JD) har Nasjonal sikkerhetsmyndighet (NSM) gjennomført en konseptvalgutredning (KVU) for en nasjonal skytjeneste. KVUen har vært til ekstern kvalitetssikring. Det er valgt et konsept og besluttet oppstart av forprosjekt.

Det er store forskjeller i investerings- og driftskostnadene for de vurderte konseptene, hvor konseptet med en lukket statlig skytjeneste er dyrest. KVUen viser også til større usikkerhet mht. samfunnsøkonomiske gevinster enn hva som er vanlig for KVUer. En av kvalitetssikrers viktigste anbefalinger var å ikke gå videre med konseptet om en lukket statlig skytjeneste gitt denne usikkerheten uten videre utredninger.

Valgt konsept tar utgangspunkt i at det inngås avtale med én eller noen få leverandører som skal eie, levere, videreutvikle og drifte en lukket kommersiell skytjeneste. Valgt konsept gir staten tilgang på kompetanse, ressurser og innovasjonskraft. Det skal imidlertid stilles krav til nasjonal kontroll av skytjenesten som leverandørene må tilfredsstille og gi garantier for. I utgangspunktet skal Nasjonal skytjeneste også defineres som skjermingsverdig infrastruktur etter sikkerhetsloven og det skal gjennomføres en sikkerhetsgradert anskaffelse.

I forkant av forprosjektet er det besluttet å gjennomføre en kort avklaringsfase for å påse at konseptvalg, føringer og rammebetingelser for nasjonal skytjeneste fortsatt er relevante, sett i lys av den sikkerhetspolitiske situasjonen og teknologiske utviklingen. Den skjerpede situasjonen tilsier at vi løpende må vurdere om valgte konsepter gir tilstrekkelig sikkerhet og nasjonal kontroll. Det er tatt et overordnet konseptvalg, men dette skal konkretiseres i forprosjektet. Der vil man kunne vurdere hva markedet faktisk kan tilby og om de sikkerhetskravene som staten stiller kan oppfylles.

3. **Stortinget ber regjeringen utvikle en konsesjonsordning for innsamling, bruk og lagring av både offentlige data og persondata for kommersielle aktører. En slik konsesjonsordning må fastsette krav til hvilke data som kan brukes, til hvilke typer formål, hvor og hvordan de lagres, og om og hvordan de kan deles med ulike tredjeparter**

Jeg tolker representantenes bruk av ordene «offentlige data» til å være data som er offentlige etter offentleglova. Det er i dag en rett til viderebruk av offentlig informasjon, regulert i offentleglova § 1 andre punktum. Reglene om viderebruk ble tatt inn i offentleglova som ledd i nasjonal gjennomføring av EUs direktiv om viderebruk av offentlig informasjon (PSI-direktivet, Public Sector Information directive) fra 2003, senere endret i 2013. Med viderebruk menes i direktivet fysiske eller juridiske personers bruk av dokumenter (data) som

er i offentlige myndigheters besittelse, for andre kommersielle eller ikke-kommersielle formål enn det opprinnelige formålet.

Stadig flere offentlige og private aktører bruker for eksempel geodata til å løse lovpålagte oppgaver, levere tjenester og som grunnlag for næringsutvikling og innovasjon. Geografiske data skaper nye verdier og bidrar til at offentlig og privat sektor løser stadig flere samfunnsutfordringer, slik som tilpasning til et klima i endring, forebygging av naturfarer og bevaring av naturmangfold. Tilgang til geodata er også viktig for å ivareta hensynet til samfunnssikkerhet og håndtere krisesituasjoner. Bruken av fellesløsningene som Kartverket forvalter, har økt betraktelig de siste årene, fra omtrent 2 milliarder oppslag i 2011 til 18 milliarder oppslag i 2023.

Prinsippet om fri rett til viderebruk av offentlig informasjon (data) det er gitt innsyn i, er forankret i offentleglova § 7. Der står det at informasjon som det er gitt tilgang til, «kan brukast til eitkvart formål dersom ikkje anna lovgivning eller retten til ein tredjeperson er til hinder for det».

Regjeringen vil om kort tid legge frem for Stortinget et forslag til ny dataforvaltningslov som reviderer reglene for viderebruk av data, og gjennomfører EUs rettsakter åpne data-direktivet og dataforvaltningsforordningen i norsk rett. Formålet med loven er å legge til rette for økt bruk av data fra offentlig sektor i samfunnet, både for verdiskaping og for å styrke åpenheten i offentlig sektor.

Når det gjelder kommersielle aktørers innsamling og bruk av personopplysninger, inneholdt både personregisterloven fra 1978 og personopplysningsloven fra 2000, som nå er opphevet, krav om forhåndsgodkjenning - også omtalt som en konsesjonsordning. Dette var en ressurskrevende og lite hensiktsmessig ordning. Nettopp derfor gikk man bort fra denne ordningen da personvernforordningen ble innført i norsk rett i 2018. Personvernforordningen legger ansvaret for å sikre personvernet på aktørene (behandlingsansvarlige), og det er disse som må vurdere personvernkonsekvenser og hvilke tiltak som må iverksettes for å sikre personopplysningene. Jeg mener at dette er en riktig tilnærming, da det er aktørene som har best kjennskap til akkurat sin bransje og dermed er nærmes til å vurdere behov for tiltak.

Personvernforordningen setter strenge krav til personvernkonsekvensvurderingen som skal gjøres. Dette innebærer vurderinger av hvilke data som kan brukes og til hvilke formål, hvordan data skal lagres og hvem de kan deles med, slik representantene viser til i sitt forslag. Datatilsynet fører tilsyn med at regelverket følges, og vil kunne gi pålegg dersom regelverket ikke er fulgt. Blant annet kan Datatilsynet gi overtredelsesgebyr dersom de finner brudd på reglene. Jeg mener dette er en bedre ordning enn det gamle konsesjonssystemet vi hadde tidligere. Samtidig følger vi nøye med på om dagens tilsynsregime er tilstrekkelig rustet til å møte den skjerpede sikkerhetspolitiske situasjonen.

4. **Stortinget ber regjeringen utarbeide en nasjonal exit-strategi for utfasing av store internasjonale kommersielle IT-plattformer, slik som Microsoft 365, i statsforvaltningen og i virksomheter med kritiske samfunnsfunksjoner, slik danske myndigheter gjør, med sikte på overgang til nye systemer fortløpende i løpet av 2026**

Amerikanske selskap leverer verdensledende tjenester som er avgjørende for mange norske virksomheter. Eksempelvis benytter 75 prosent av norske, offentlige virksomheter Microsoft som leverandør. De amerikanske selskapene har levert brukervennlige, sikre og skalerbare tjenester over lang tid. Det er ikke i seg selv et problem. Men markedsdominansen har gjort mange land og virksomheter i offentlig og privat sektor avhengig av tjenester fra amerikanske selskaper.

Den skjerpede geopolitiske situasjonen gjør det nødvendig å vurdere slike avhengigheter i et nytt lys. Markedskonsentrasjonen av kritisk digital infrastruktur hos et fåtall aktører er en sårbarhet vi må ta på alvor – og som ikke kan håndteres gjennom ensidig nasjonal utfasing, men gjennom systematisk risikovurdering og økt handlefrihet. Det ansvaret påhviler staten og den enkelte virksomhet. Alle offentlige og private virksomheter må derfor vurdere hvilke avhengigheter de har, og hvilken risiko det kan medføre.

Regjeringen jobber for å øke vårt digitale handlingsrom. Regjeringen har blant annet styrket kontrollen over kritisk digital infrastruktur som mobil-, bredbånd, fibernettene og datasentre i Norge. Vi utvikler KI-systemer på norsk, og vi bygger kapasitet i norsk regnekraft, slik at vi kan trene og bruke KI-systemer her i landet. Vi bygger også kapasitet til å lagre mer data i Norge.

Det er også opprettet en tverrgående arbeidsgruppe under ledelse av Digitaliseringsdirektoratet, med deltakelse fra andre større statlig etater og KS. Gruppen skal vurdere hvordan man kan forbedre virksomheters endringsevne i bruken av skytjenester. Arbeidsgruppen skal utarbeide veiledning om endringsevne i bruken av skytjenester og sørge for oppdatert kunnskap om endringer i risikobildet som gjelder faktorer som regulatorisk risiko, digital suverenitet og geopolitisk innflytelse. Gruppen arbeider blant annet med å utforme prinsipper for dataportabilitet mellom skytjenester, vurdering av så kalte exit-kostnader, den skal følge med på den regulatoriske utviklingen i EU og til slutt skal den utarbeide forslag til tiltak ut fra identifiserte felles behov i forvaltningen.

Regjeringen mener generelt det er ønskelig med flere alternativer innenfor både skytjenester og programvare, gjerne europeisk baserte løsninger og gjerne basert på åpen kildekode. Men dette er ikke noe Norge kan løse alene. Derfor samarbeider vi tett med EU på regulering av teknologiganter. Vi samarbeider også i Norden, og innenfor det indre markedet, for at europeiske teknologiselskaper skal lykkes med å bygge alternative løsninger vi trenger.

Regjeringen ønsker at flere teknologiselskaper skal lykkes i Norge og Europa, og mener det er viktig at både offentlige og private virksomheter sprer risiko og unngår for stor avhengighet av noen få selskaper. Dette innebærer å være forberedt på å kunne flytte sine tjenester og

drift til andre løsninger ved behov. Dette ansvaret bør, som i dag, ligge i den enkelte virksomhet og være basert på deres behov og vurderinger.

5. **Stortinget ber regjeringen redegjøre for hvordan de bedre vil følge opp GDPR og sikre at sensitiv og samfunnskritisk informasjon om innbyggere utelukkende skal behandles i løsninger som er under norsk eller europeisk jurisdiksjon**

GDPR har ikke et forbud mot å overføre persondata til land utenfor Norge eller Europa eller bruke løsninger i slike land, men har som utgangspunkt at persondata bare kan overføres lovlig ut av EU/EØS dersom de har samme vern etter overføring som de har i EU/EØS. Alle virksomheter, både offentlige og private, har selv ansvar for å oppfylle kravene i personvernregelverket og sørge for at det ikke overfører eller på andre måter behandler personopplysninger ulovlig. Det norske Datatilsynet fører tilsyn med behandling av personopplysninger hos selskaper som er etablert her i Norge, mens selskaper etablert i andre europeiske land er underlagt datatilsynet i det aktuelle landet. Jeg opplever at risikoene forbundet med overføring av persondata til land utenfor Norge og Europa, er en problemstilling som Datatilsynet vier betydelig oppmerksomhet til. Den skjerpede sikkerhetspolitiske situasjonen tilsier at denne oppmerksomheten må opprettholdes og styrkes. Regjeringen følger derfor utviklingen tett.

6. **Stortinget ber regjeringen redusere leverandørlåsing ved å utarbeide regler for offentlig innkjøp av IT-løsninger som bruker åpne standarder og åpen kildekode med universell utforming og muliggjør interoperabilitet i offentlig sektor**

Innlåsingseffekter er generelt negativt for konkurransen i offentlige anskaffelser, og anskaffelsesregelverket har regler som kan motvirke dette. Oppdragsgiver må som den klare hovedregel avholde konkurranse når oppdragsgiver ønsker å kjøpe digitale løsninger. Det er kun snevre unntak for å benytte eksisterende leverandører av hensyn til eksisterende tekniske løsninger. Med hensyn til anskaffelser av IT-løsninger, gir digitaliseringsrundskrivet departementene, statens ordinære forvaltningsorganer, forvaltningsorganer med særskilte fullmakter og forvaltningsbedrifter en rekke føringer for hvordan IT-systemer skal se ut. Dette bidrar til å ivareta blant annet universell utforming og andre nedfelte overordnede arkitekturprinsipper. Slike oppdragsgivere er ansvarlige for at føringene følges opp i sine anskaffelser.

Europakommisjonen er i ferd med å revidere sitt anskaffelsesregelverk. Dette regelverket utgjør grunnlaget for hoveddelen av det norske regelverket. Et viktig formål med revisjonen er å øke Europas konkurransekraft, sikkerhet og motstandskraft, noe som også er viktige hensyn i norske innspill til revisjonen. Utkast til ny europeisk regulering er forventet lagt frem av Europakommisjonen i andre kvartal 2026.

Etter regjeringens vurdering er det på bakgrunn av dette ikke behov for å utarbeide ytterligere regler for offentlig innkjøp av IT-løsninger nå.

7. **Stortinget ber regjeringen styrke og videreutvikle interkommunale samarbeid og oppgavefellesskap som utvikler digitale løsninger for offentlig sektor, basert på åpne kildekoder og standarder**

Kommunene, som leverer de aller fleste tjenester inn mot innbyggere og næringsliv, har lenge brukt interkommunale samarbeid som strategisk virkemiddel og tilnærming mot en krevende ressurssituasjon. Det er kommunene som etablerer interkommunale samarbeid, inkludert kommunalt oppgavefellesskap. Det er derfor opp til kommunene som deltar i samarbeidet å sette rammene for hva det interkommunale samarbeidet skal gjøre. Dette gjelder økonomiske rammer, ambisjonsnivå og hvilke typer oppgaver eller produksjon av tjenester som skal ytes.

KS er regjeringens samarbeidspartner i digitaliseringsarbeidet i offentlig sektor. Dersom det er hensiktsmessig å støtte interkommunale samarbeid på digitaliseringsområdet, vil regjeringen drøfte dette med KS. KS har ansvar for å samordne medlemmenes behov og prioriteringer på digitaliseringsområdet og har etablert KS Digital som utvikler, drifter og forvalter digitale fellestjenester for kommuner og fylkeskommuner. KS Digital, i samarbeid med KS, vil utvikle kapasitet til å gjennomføre felles anskaffelser, leverandørstyring og avtaleforvaltning på vegne av kommuner og fylkeskommuner. KS Digital benytter åpen kildekode og relevante standarder i sitt utviklingsarbeid. KS og KS Digital har dialog med Direktoratet for forvaltnings og økonomistyring (DFØ, Markedsplass for skytjenester) for å vurdere samarbeid om nasjonale anskaffelser for offentlig sektor når det er aktuelt.

Det er kommunenes ansvar å ha programvare som dekker deres behov, selv om et interkommunalt samarbeid ev. anskaffer dette på vegne av dem. En rekke kommuner gjør allerede anskaffelser gjennom Markedsplass for skytjenester hos DFØ. For dem som har tilsluttet seg anskaffelsen, foreligger det nå rammeavtaler for skytjenester fra flere leverandører. Microsoft er ikke blant tilbyderne.

8. **Stortinget ber regjeringen ta nødvendige grep for å samarbeide tettere med nordiske og europeiske land om felles digitale løsninger og beredskap, hvor åpne kildekoder og digital suverenitet over digital infrastruktur er førende for samarbeidet**

Regjeringen samarbeider allerede tett både med Norden og med EU. Norden har et felles mål om å bli verdens mest integrerte region, også digitalt. Teknologisk suverenitet er prioritert i samarbeidet i Nordisk Ministerråd i 2026, og Norge har foreslått å fortsette satsingen på dette i 2027, da Norge tar over formannskapet.

Sammen med Norden og Baltikum har vi etablert Nordisk KI-senter, også kjent som New Nordics AI. Dette er et initiativ som samler regjeringer og næringsliv i Norden for å styrke regionens posisjon innen kunstig intelligens. Målet er å gjøre Norden-Baltikum til en samkjørt og ledende region for ansvarlig og bærekraftig bruk av KI, og gjennom dette styrke Nordens digitale konkurransekraft.

EU trapper opp innsatsen for europeisk konkurransekraft og forenkler regelverk for å styrke europeiske teknologimiljøer. Dette følger Norge tett. EUs forordninger om digitale tjenester (DSA) og digitale markeder (DMA) er eksempel på regelverk som setter grenser for tech-kjempenes makt. Regjeringen jobber med å innføre disse i norsk lov så raskt som mulig. Vi er også med i EUs DIGITAL-program for digital omstilling og bruk av innovative digitale teknologier i samfunnet og næringslivet. Dette bidrar til å sikre konkurransekraft og bygge felleseuropeiske kapasiteter innen digitale teknologier. Regjeringen vil forsterke dette samarbeidet.

Overordnet vurdering av representantforslaget
Regjeringen styrker Norges digitale handlingsrom; Norges evne til å bevare styring, sikkerhet og handlefrihet i en digital tidsalder. Det omfatter hele den digitale verdikjeden fra fysisk infrastruktur og nettverk, via maskinvare og skytjenester, til data, programvare og kunstig intelligens. Å redusere sårbarhet forutsetter at vi bygger flere alternative løsninger og partnerskap – at vi får flere ben å stå på digitalt.

Totalberedskapsmeldingen prioriterer å styrke digital motstandskraft og nasjonal kontroll over kritisk infrastruktur og strategisk viktige virksomheter, naturressurser, eiendom og verdier, hvor økt kompetanse innenfor digital sikkerhet er et foreslått tiltak. Vi jobber tett med våre nordiske naboer og med EU og øvrige allierte. Dette er avgjørende for å sikre handlingsrom, felles standarder og flere reelle alternativer. Vi deler målet om å styrke Norges digitale handlingsrom, som vi ønsker å forbedre gjennom det arbeidet jeg har beskrevet i dette brevet. Jeg kommer tilbake til Stortinget på relevant måte med de tiltakene som kommer ut av det pågående arbeidet knyttet til dette. Derfor mener jeg at intensjonen i representantforslaget er godt ivaretatt i regjeringens pågående arbeid, og at forslagene ikke bør vedtas.

Med hilsen

Karianne Oldernes Tung