



Styre
Universitetsstyret

Arkivsaksnr.
26/51640
Saksnr.
52/26

Dokumentdato
08.06.2026
Møtedato
18.06.2026

Orienteringssak: Digital suverenitet

Henvisning til bakgrunnsdokumenter

- [Styresak 38/26 Forskningssikkerhet og ansvarlig internasjonalt samarbeid](#)
- Styresak 27/26, Ledelsens gjennomgang av informasjonssikkerhet 2025

Saken gjelder

Akademisk frihet, institusjonell autonomi og uavhengighet er grunnleggende forutsetninger for universitetets samfunnsoppdrag, og vi må som universitet stå så fritt som mulig i valg av infrastruktur og teknologi som støtter opp om våre faglige prioriteringer.

Digital suverenitet har de siste årene fått økt oppmerksomhet basert på samfunnets grunnleggende avhengighet av informasjonsteknologi og de fleste virksomheters avhengighet av et fåtall store teknologiselskaper. I en verden der koblingen mellom politikk og teknologi er blitt tydeligere, samtidig som den geopolitiske uroen har økt, blir digital avhengighet, sårbarhet og suverenitet viktige parametere både på virksomhetsnivå og samfunnsnivå.

I lys av denne utviklingen er det naturlig at Universitetet i Bergen har et aktivt forhold til forutsetninger for og konsekvenser av digital suverenitet, om og eventuelt hvilke føringer og tiltak vi iverksetter. Saken legges fram til orientering for universitetsstyret.

Forslag til vedtak

Styret tar saken til orientering.

Tore Tungodden
Universitetsdirektør

08.06.2026/Tore Burheim

Saksframstilling

Digital suverenitet

Bakgrunn

Akademisk frihet, institusjonell autonomi og uavhengighet er grunnleggende forutsetninger for universitetets samfunnsoppdrag, og UiB må som institusjon sikre størst mulig frihet og handlingsrom til valg av infrastruktur og teknologi som støtter opp om faglige prioriteringer. Bruk av informasjonsteknologi er grunnleggende viktig for fagmiljøene og for administrasjonen, og vi må ha høy oppmerksomhet både om mulighetene som ligger i nye teknologier og på problemstillinger knyttet til kontroll over og tilgang til våre data og systemer.

Det finnes ingen autoritativ eller omforent definisjon av digital suverenitet. Begrepet tar utgangspunkt i et utfordringsbilde knyttet til økt avhengighet av et fåtall internasjonale teknologigiganter, deres geopolitiske koblinger, samt Europas avhengighet av import i store deler av verdikjeden innen informasjonsteknologi. De store teknologiselskapenes dominans og innlåsing kan begrense både det akademiske og institusjonelle handlingsrommet i bruk av informasjonsteknologi.

I en verden med økt geopolitisk uro kombinert med muligheter for å bruke tilgang til teknologi som et maktmiddel vil innlåsing i systemer og dominans av enkeltaktører også gi risiko for økt sårbarhet i leverandørkjeder, samt økt økonomisk risiko i form av uforutsette prisøkninger.

Framvekst og bruk av generativ kunstig intelligens (KI) har aktualisert problemstillingen ytterligere. KI vil være et viktig verktøy for universitetets faglige og administrative virksomhet, og vi må legge til rette for ansvarlig bruk samt bidra til at forskningsmiljøer som har nytte av KI i forskning får muligheten til å utforske muligheter innenfor gode rammer. UiB må etablere uavhengighet også innenfor KI så langt det er mulig.

Temaet digital suverenitet berører hele verdikjeden i vår bruk av informasjonsteknologi og problemstillingene er så komplekse at knapt noe land i verden kan etablere full digital suverenitet på egen hånd.

Digital suverenitet har særlig vært drøftet på europeisk nivå, med Danmark, Tyskland, Nederland og Frankrike i spissen. I Norge har temaet også fått økt oppmerksomhet. Nasjonal sikkerhetsmyndighet ([NSM](#)) trakk særlig fram samfunnets avhengighet av de tre teknologigigantene Microsoft, Google og Amazon som en nasjonal risiko i sin risikovurdering for 2026. Denne risikoen er også relevant for universitetene.

Selv om full digital suverenitet i Norge ikke vil være mulig, forhindrer ikke dette at man kan iverksette tiltak for å redusere sårbarheter, øke vår handlefrihet og sikre vår uavhengighet. Vi kan

også vurdere å inngå partnerskap og samarbeid med nære samarbeidspartnere, for eksempel i Norden og Europa, og derigjennom etablere økt regional digital suverenitet eller styrke vår handlefrihet.

Perspektiver på digital suverenitet og betydning for universitetene

Digital suverenitet i Europa er ofte drøftet ut fra tre ulike perspektiver og begrunnelser: Akademisk frihet og autonomi, samfunnsøkonomi og risiko. Disse perspektivene kan også være en hensiktsmessig tilnærming for universitetene.

1. Akademisk frihet, autonomi og internasjonalisering.

Mangel på digital suverenitet kan ramme universitetets grunnleggende verdier ved både å svekke den akademiske friheten og vår autonomi. Det kan gi økt usikkerhet om hvem som har tilgang til våre data og e-poster, medføre selvsensur, eller manglende tillit fra ¹tredjepart og fra dem som deler sensitive data med oss. Det kan for eksempel gjøre oss forsiktige med temaer noen oppfatter som kontroversielle. Dette perspektivet har for eksempel bidratt til at UiB søker å lagre forskningsdata enten lokalt eller hos nasjonale lagringstjenester.

Svekket digital suverenitet kan også ramme UiB som et internasjonalt forskningsuniversitet fordi det også omhandler forholdet mellom geopolitikk og teknologi, Europas langsiktige avhengighet av amerikanske teknologigiganter, og tilsvarende avhengighet av maskinvare fra Kina/Asia. Europa kan utsettes for press og få redusert handlingsrom gjennom ulike former for kontroll og begrensninger i leveransekedene.

2. Samfunnsøkonomisk. Dette er et sentralt tema på europeisk nivå. Europa importerer om lag 80 % av teknologien vi bruker, og har vist seg å ha begrenset evne til å omsette ideer og forskningsresultater til innovasjon, produkter og verdiskaping. EU har satt i gang en lang rekke tiltak, både regulatoriske², økonomiske og i langtidsbudsjettet.

For universitetene er dette knyttet til forsknings- og innovasjonsdelen av vårt samfunnsoppdrag, der europeiske universiteter inviteres til å bidra til å løse dette som en stor og viktig samfunnsutfordring. Denne dimensjonen kan antas å bli en vesentlig kilde til eksterntfinansiering de kommende årene, gjennom blant annet EUs konkurransefond, Horisont Europa og andre kilder.

¹ EUs Cloud Sovereignty Framework er et forsøk på å strukturere og vurdere grad av digital suverenitet og kontroll. Rammeverket er utviklet med sikte på anskaffelser og bruk av skytjenester.

² For eksempel Digital omnibus <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal?ref=eutechloop.com>

3. **Risiko.** Dette oppstår som en følge av markedskonsentrasjon, der de fleste virksomheter (inkludert universitetene) er avhengige av en eller flere blant et fåtall amerikanske teknologigiganter. Utfall av tjenester hos en eller flere av disse, eller i deres underliggende infrastruktur, har påvirket betydelig deler av samfunnet samtidig. Dette gjelder også universitets- og høyskolesektoren der datainnbruddet hos Instructure i mai 2026 illustrerte dette³. I tillegg finnes det en finansiell risiko gjennom innlåsing. Vi ser for eksempel at en leverandør som Microsoft har økt prisene til dels vesentlig. Gjennom innlåsing og små handlingsmuligheter svekkes vår forhandlingsposisjon når slike forhold oppstår.

Som det framkommer over, er digital suverenitet svært relevant for universitetets samlede virksomhet og for å ivareta vårt verdigrunnlag. Temaet berører akademisk frihet, institusjonell uavhengighet og virksomhetsrisiko. I tillegg ser vi en økonomisk risiko knyttet til konsentrasjon og innlåsing. Samtidig vil det være en del av vårt samfunnsoppdrag med å bidra med kunnskap og kompetanse for å løse en større samfunnsutfordring.

Politiske føringer i Norge

I Norge har diskusjonen og tiltakene knyttet til digital suverenitet ikke vært like framtrødende som i resten av Europa. På EU-nivå er det iverksatt en lang rekke tiltak⁴, både ut fra geopolitiske mål og som oppfølging av [Draghi-rapporten](#). Det forventes at ulike aspekter ved digital suverenitet vil bli viktige i EUs rammeprogram for forskning og innovasjon for perioden 2028–2034 og i EUs konkurransefond for samme periode. Dette gjelder særlig i [konkurransefondet](#) der *digitalt lederskap* er ett av fire områder.

Gjennom 2025 var det noe oppmerksomhet rundt temaet også i Norge, både i form av en avspeiling av europeisk aktivitet og utspill, men også selvstendige reaksjoner på geopolitisk uro og uforutsigbarhet kombinert med teknologiens mer fremtrødende rolle i samfunnsutviklingen. Oppmerksomhet rundt mange politiske utspill fra det nye amerikanske presidentskapet kombinert med viljen til å bruke teknologi som pressmiddel bidro til dette. Verbale angrep mot EUs reguleringer på digitaliseringsområdet, nedbyggingen av de amerikanske institusjonene som skal ivareta GDPR-tematikken, diskusjonene rundt Grønland, USAs sikkerhetsstrategi og USAs AI Act skapte oppmerksomhet. I tillegg laget NHO sin egen versjon av Draghi-rapporten.

I en pressemelding⁵ fra 22. april 2026 skriver digitaliseringsminister Karianne Tung at hun ønsker å styrke Norges digitale handlingsrom. Hun ønsker å vurdere en del tiltak, blant disse er:

³ Se styresak 51/26 Orienteringssak: Konsekvenser av datainnbrudd hos valgt leverandør av ny læringsplattform for UIB

⁵ <https://www.regjeringen.no/no/aktuelt/digitaliseringsministeren-vil-styrke-norges-digitale-handlingsrom/id3157046/>

⁵ <https://www.regjeringen.no/no/aktuelt/digitaliseringsministeren-vil-styrke-norges-digitale-handlingsrom/id3157046/>

1. En strategi for bruk av åpen kildekode i staten.
2. Oppdatere forskrift om IT-standarder i offentlig sektor ved å skjerpe krav til bruk av åpne formater i offentlig sektor, så vi ikke låses til enkelte programvarer.
3. Vurdere å stille krav til at statlige virksomheter gjør gode risikovurderinger og styrker sitt digitale handlingsrom.

Ifølge pressemeldingen er det nedsatt en tverrdepartemental arbeidsgruppe som arbeider med temaene, og det har vært dialog med UiB om temaet.

De nevnte tiltakene ligger godt innenfor utviklingen på europeisk nivå. For Universitetet i Bergen er alle tre relevante problemstillinger som kan håndteres. Bruk av åpen kildekode har UiB lang erfaring med, og dette benyttes i dag i flere sentrale systemer ved UiB. Det kan nevnes her at EU har en strategi for åpen kildekode og dette er et element i flere av tiltakene på europeisk nivå.

Status og vurderinger ved UiB

UiBs tilnærming er at vi i første omgang ønsker å sikre oss kontroll på våre data, og i særlig grad forskningsdata. Disse representerer noen av de viktigste informasjonsverdiene for UiB. Vi er opptatt av å redusere risiko og sikre oss et handlingsrom innen en akseptabel tidshorisont. Det innebærer at vi må sikre kontinuitet og kontroll på de store komplekse virksomhetsnære systemene, særlig knyttet til undervisning.

Med sikte på å kunne motvirke selvsensur vil det være formålstjenlig å kunne tilby skrivebords- og samhandlingsløsninger på alternative plattformer enn Microsoft Office. Gjennomgående for alle områdene er å sørge for at vi innehar nødvendige kapabiliteter for å sikre vårt handlingsrom og våre verdier. Dette omfatter både teknisk, organisatorisk og juridisk kompetanse og kapasitet.

Under følger en kortfattet oversikt over status for bruk av informasjonsteknologi, skytjenester og andre kritiske systemer ved UiB.

Maskinvare og infrastruktur: UiB kjøper dette i all hovedsak fra amerikanske leverandører, der produksjonen i stor grad skjer i Asia/Kina, men ofte monteres i Europa. Den maskinvaretilpassede programvaren utvikles i stor grad av globale, amerikanske selskaper, primært i USA. UiB har en betydelig mengde lokal lagring fysisk plassert ved UiB, i hovedsak for forskningsdata. UiB har ikke kinesiske leverandører av teknologi i vår infrastruktur, men vi legger til grunn at det finnes kinesiske underleverandører i verdikjeden. UiB er i ferd med å gå over fra kommersiell virtualisering av maskinvare til åpen kildekode med en supportavtale, blant annet som følge av en uakseptabel prisøkning.

Forskning: Forskningsdata lagres i stor grad lokalt ved UiB eller i nasjonale løsninger i regi av [Sigma2](#) i Lefdal. Vi arbeider for å inn eksisterende eller nye forskningssystemer på UiBs skyplattformer. Mange nasjonale og internasjonale forskningsprosjekter bruker også skyplattformer

som Google eller tilsvarende for samhandling. UiB bygger nå en agnostisk og fleksibel plattform og arkitektur for kunstig intelligens, som kjører på UiBs skyplattform, men som kan konsumere KI-løsninger der de er tilgjengelige, enten det er hos de store KI-leverandørene, hos partnere i Norge eller, for mindre modeller, lokalt ved UiB.

Undervisning: Området er variert. Dagens læringsplattform Canvas som er basert på åpen kildekode driftes lokalt på UiB, mens planlagt innført skyversjon av Canvas kjøres hos Amazon. UiB-Treet kjøres ved UiB, mens digital eksamen kjøres på en skytjeneste i Danmark. Tredjepartsportalen kjøres hos Microsoft i Nederland. Nytt felles studentsystem (Nye FS) og nytt samordnet opptak som utvikles av Sikt kjøres hos Amazon.

Kunstig intelligens: UiB har etablert dedikerte ressurser og en KI-plattform for forskning samt KI-infrastruktur i våre lokale skyløsninger. Alle disse er for mindre og mer spissede språkmodeller. I tillegg har man tilgang til den nasjonale supercomputeren Olivia, og en av Europas kraftigste maskiner, LUMI, i Finland – alle via Sigma2-strukturen.

Administrative systemer: Universitetet i Bergen bruker et betydelig antall skytjenester og andre eksterne tjenester innen administrasjon, og dette er det området der bruken av skytjenester som kjøres hos de amerikanske teknologigigantene er størst. Blant disse er Microsoft Office, e-post, samhandling og saksbehandling.

Basis IT-tjenester: UiB har en blanding av åpen kildekode og proprietære løsninger. Våre skyplattformer bygger på åpen kildekode, og det samme gjelder en lang rekke av de mange tekniske komponentene. Samtidig har vi mange servere og tjenester knyttet til Microsoft. Innen autentisering brukes både en amerikansk plattform for administrasjon av tilgangsstyring gjennom en fellestjeneste i sektoren, og Microsoft-autentisering og tofaktor.

Kort oppsummert er situasjonen på UiB sammensatt. For administrative tjenester er det mye bruk av de amerikanske skyplattformene direkte eller indirekte, og det samme gjelder for skrivebordsverktøy og samhandling. Lagring av brukerkataloger for ansatte og studenter skjer i sky og felles administrativ lagring er i ferd med å flyttes til sky. For basis infrastruktur og basis IT-tjenester bruker UiB mye åpen kildekode og enkelte europeiske leverandører. For forskningstjenester er det mye bruk av åpen kildekode og lagring i Norge, men ikke gjennomgående. Med hensyn på undervisning er det mye amerikanske skytjenester direkte eller indirekte med unntak av vår digitale læringsplattform som per dags dato kjøres lokalt hos UiB.

Gjennom UiB sin deltakelse i universitetsalliansen [CHARM-EU](#) vil ett av områdene innen IT-samhandling de kommende to årene være digital suverenitet. Det kan gi oss muligheter for samarbeid om privat sky, datasuverenitet gjennom lagringstjenester og teknologi, samt KI-suverenitet.

Retningsvalg

Universitetet i Bergen har tatt økt digital suverenitet inn som en strategisk føring i digitaliseringsarbeidet. Dette er grunnleggende viktig for å ivareta akademisk frihet og uavhengighet, men det handler også om risikostyring av den samlede virksomheten i et langsiktig perspektiv.

I arbeidet med styrket digital suverenitet er det flere ulike tilnærminger. Under er noen av de tiltak vi vurderer:

- Digital suverenitet i beslutninger innen digitalisering: I beslutninger knyttet til informasjonsteknologi og digitalisering bør digital suverenitet eksplisitt tas med i beslutningsgrunnlaget der det er relevant. En mulig måte å strukturere dette på er å besvare følgende fem spørsmål⁶⁶:
 - (a) På hvilken måte påvirker valget maktforholdene i vår leveransekjede og vår autonomi? Hvem har anledning til å endre teknologi, tilgang eller driftsforhold? Gir universitetet fra seg noe kontroll eller autonomi gjennom beslutningen som tas?
 - (b) Hva er beslutningens realistiske levetid? Ofte har valg mye lengre levetid og mer omfattende konsekvenser enn forespeilet. I hvor stor grad vil valget medføre konsekvenser som gjør det vanskeligere å endre valget i framtiden?
 - (c) I hvor stor grad utsettes vi for felles sårbarhet gjennom valgene vi gjør? I hvor stor grad rammes vi av felles feil eller bortfall av tjenester, og hvilke konsekvenser har dette? Hva er kontinuitetsplanen, og er den testet?
 - (d) I hvor stor grad er den valgte løsningen utskiftbar, og hvordan er byttemulighetene? Kompatibilitet mellom ulike leverandører, standardiserte og åpne format, fleksibilitet og interoperabilitet vil bidra til økt handlingsrom i framtiden. Her vil standarder være viktige.
 - (e) Har UiB kapasitet og kompetanse til både å styre og forvalte valget? Dette gjelder både funksjonell og teknisk bestillerkompetanse og kapasitet, samt drift og forvaltning.

Det kan være andre måter å strukturere problemstillingen på, men det vil være formålstjenlig å finne et felles rammeverk for dette.

- Vektlegge digital suverenitet i anskaffelser. UiB kan ta i bruk EUs Cloud Sovereignty Framework eller et tilsvarende rammeverk i anskaffelser der det er relevant og formålstjenlig. Det gir oss en mulighet til også å vurdere tilbud i et suverenitetsperspektiv. Endringer i anskaffelsesregelverket som trer i kraft 1. juli 2026, bør kunne gi mulighet for dette, da sikkerhets- og beredskapshensyn har fått en mer framtrødende plass. Man kan eventuelt etablere eller bruke enklere og mindre krevende rammeverk.

⁶⁶ Disse er en lett tilpasning av spørsmål hentet fra professor ved CBS, Jan Damsgaards nylige bok *Digital suverenitet*, Djøf Forlag, København, 2026.

- Justere teknologianbefalingene. UiBs teknologianbefalinger justeres i tråd med vurderinger av digital suverenitet og eventuelle statlige føringer på området. Dette vil for eksempel kunne medføre økt vektlegging av åpen kildekode, åpne standarder og eventuelle endringer som er antydnet i de statlige IT-anbefalingene. Samtidig er det, ut fra et europeisk perspektiv, viktig å bidra til å skape et europeisk IT-marked.
- Redusere avhengighet og sårbarhet. Iverksette tiltak for å redusere avhengighet av teknologigigantene direkte eller indirekte, særlig på de mest kritiske områdene. Dette må vurderes ut fra hva som er vanskeligst å bytte i en kritisk situasjon, og hva som er mest kritisk for virksomheten ved et eventuelt bortfall av tjenester. En måte er å vurdere exit-strategier, men vel så viktig er valg av løsninger.

Universitetsdirektøren sine kommentarer

Digital suverenitet har betydning for universitetenes grunnleggende verdier knyttet til akademisk frihet, uavhengighet og institusjonell autonomi. Digital suverenitet påvirker vår evne til å opprettholde kontroll over egne data, egen digital infrastruktur og teknologiske løsninger. Det sikrer at samfunnet fungerer sikkert og uavhengig i en urolig tid, og er et område der risikobildet har endret seg raskt de siste årene.

Forventningene til universitetets bevissthet og handlekraft på området har derfor også økt. Å avvente situasjon og utvikling med tanke på nasjonale eller sektorvise løsninger er ikke en farbar vei gitt kompleksiteten i vår faglige og administrative virksomhet. Å ta riktige teknologivalg er strategisk viktig for å ivareta universitetets verdier og samfunnsoppdrag. En sentral premiss i arbeidet med digital suverenitet er at de valg vi tar i dag vil kunne ha langsiktige implikasjoner.

Utbredelsen av kunstig intelligens har bidratt til ytterligere å skjerpe risikobildet. Kunstig intelligens er en svært kraftfull teknologi som skaper verdi, men samtidig er den ikke verdinøytral. UiBs arbeid med å etablere en KI-plattform og -arkitektur er i tråd med målet om å redusere universitetets avhengighet, øke vår handlefrihet og vil gjøre det vesentlig enklere for UiB å bytte språkmodeller. Dette arbeidet handler ikke bare om suverenitet, men også ut fra ambisjoner om å ivareta kvalitet i takt med endringer i teknologiutviklingen.

Det omfattende datainnbruddet i den digitale læringsplattformen Canvas viser sårbarheten og risikoen i markedskonsentrasjon i plattformtjenester for en sektor. At store deler av en sektor i hele Europa, Nord-Amerika og Australia blir rammet samtidig, med 275 millioner ansatte og studenter fordelt på 9000 institusjoner, viser sårbarheten, jf. styresak 51/26.

Universitetsdirektøren legger opp til at administrasjonen skal vektlegge digital suverenitet i større grad i digitaliseringsarbeidet ved UiB. Styret vil bli holdt orientert om dette arbeidet, og der det er relevant få seg forelagt saker som vedrører strategiske veivalg og prioriteringer på feltet.

08.06.2026/Tore Burheim

