Skyspor

EXIT-STRATEGI · UTKAST TIL BESLUTNING

Skyavhengigheter utenfor Europa i Havforskningsinstituttet

Risikovurdering, norske og europeiske alternativer, og en plan for exit i fire faser. Basert på ekstern kartlegging av hi.no.

DATO	VERSJON	EKSPONERINGSINDEKS	GRADERING
20.10.2026	0.9 utkast	74 av 100	Åpen

OM DOKUMENTET

Slik bruker dere dette utkastet

Dette er et utkast til exit-strategi for Havforskningsinstituttet. Det bygger på det som er synlig fra utsiden, og er ment som grunnlag for en intern kartlegging og en beslutning i ledelsen.

01	Sammendrag for ledelsen
02	Bakgrunn og risikobilde
03	Funn: avhengighetsregister og personvernerklæring
04	Risikovurdering per område
05	Norske og europeiske alternativer
06	Exit-plan i fire faser
07	Gjennomføring per område
08	Krav til anskaffelse og kontrakt
09	Styring, roller og måltall
10	Neste steg: 30, 60 og 90 dager
A–D	Vedlegg: metode, teknisk bevisliste, kilder og ordliste

Hva dokumentet er, og hva det ikke er

Kartleggingen bruker offentlige signaler: DNS-poster, sertifikater, nettsidenes kode og hvem som eier serverne. Den ser ikke fagsystemer, interne nettverk eller avtaler. Der virksomhetens egen personvernerklæring navngir leverandører, er de tatt med i kapittel 3. Funn er derfor indikasjoner som må bekreftes internt.

Dokumentet gir ingen juridisk vurdering. Der det vises til regelverk, er det for å peke på hvilke krav som er relevante, ikke for å konkludere om etterlevelse.

01 · SAMMENDRAG FOR LEDELSEN

Havforskningsinstituttet har høy eksponering mot skytjenester utenfor Europa

EKSPONERINGSINDEKS

74 / 100

HØY

Delt 17.–19. plass av 110, der 1. plass har høyest indeks. Leverandør sett i 9 av 12 områder, 9 med funn utenfor Europa. Etter fase 1 og 2 i planen: **50.0**. Etter fase 3: **0**.

Den eksterne kartleggingen av hi.no fant 16 avhengigheter utenfor Europa i 9 av 12 områder. Leverandørene har hovedkontor i USA.

Den tyngste avhengigheten er Microsoft 365-plattformen, som her omfatter e-post (Exchange Online), kontorpakke og fillagring, Teams, enhetsstyring (Intune) og identitet (Entra ID). Disse tjenestene henger sammen, og exit bør planlegges som ett prosjekt med identitet til slutt.

Microsoft bekrefter at hi.no hører til en Entra-tenant registrert i Microsofts region for Europa. Det avgjør hvor dataene lagres, men tenanten leveres fortsatt av et amerikansk selskap og er omfattet av CLOUD Act.

Nettstedet driftes hos Microsoft Azure (USA).

På nettsidene lastes 5 tjenester fra leverandører utenfor Europa, blant annet Google Analytics, BootstrapCDN og Google Fonts. Dette er raske gevinster som kan fjernes på noen uker.

CAA-posten i DNS tillater sertifikater fra Amazon, DigiCert, HARICA og Let's Encrypt.

Personvernerklæringen nevner i tillegg 2 leverandører utenfor Europa som den tekniske kartleggingen ikke fant: Mailchimp og Facebook.

Eksponeringsindeksen er 74 av 100 (høy). Delt 17.–19. plass av 110, der 1. plass har høyest indeks. 3 statlige virksomheter har samme indeks.

Kartleggingen fant også spor av 1 norsk eller europeisk tjeneste: Sikt (Uninett).

FUNN UTENFOR EUROPA	OMRÅDER BERØRT	NORSKE OG EUROPEISKE	SUBDOMENER UTENFOR EUROPA
16	9	1	0

Anbefalte beslutninger

01 **Vedta et mål for digital suverenitet.**
Ledelsen bestemmer hvilket suverenitetsnivå ulike typer informasjon skal ha, og hvem som eier exit-planen.

02 **Gjennomfør de raske gevinstene innen tre måneder.**
Sporing og analyse og Tredjepartsinnhold på nettsidene. Tiltakene er billige og reversible.

03 **Still krav om europeisk eierskap ved neste anskaffelse.**
Gjelder Nettsted: drift, CDN og DNS og KI-tjenester. Bruk kravene i kapittel 8.

04 **Start en forstudie for Microsoft 365-plattformen.**
Mål: pilot med én avdeling innen 12 måneder. Identitet flyttes sist.

05 **Dokumenter avhengighetene dere beholder.**
jsDelivr og Let's Encrypt: noter avhengigheten. Gjør en enkel vurdering ved neste fornyelse. For sertifikater: legg inn en europeisk reserve, se kapittel 10.

02 · BAKGRUNN OG RISIKOBILDE

Hvorfor avhengighetene må vurderes nå

Spørsmålet er ikke om tjenester fra leverandører utenfor Europa er lovlige å bruke. Det er de, i dag. Spørsmålet er om virksomheten har vurdert risikoen, og om det finnes en vei ut hvis forutsetningene endrer seg.

Tre risikoer som ofte blandes sammen

Våre vurderinger. Sannsynlighet og konsekvens er skjønn, ikke målte data.

RISIKO	HVA DET BETYR	SANNSYNLIGHET	KONSEKVENS
Rettslig tilgang	Myndighetene i landet der leverandøren hører hjemme, kan kreve utlevering av data leverandøren kontrollerer, også når dataene ligger i Europa. Mest kjent er amerikanske CLOUD Act og FISA 702. Leverandøren kan bestride kravet. [4]	Lav	Høy
Sanksjoner og avstengning	En tjeneste kan bli stengt av politiske grunner. Den internasjonale straffedomstolen mistet tilgang til en sentral e-postkonto i 2025 etter sanksjoner. [3]	Lav	Svært høy
Kommersiell innlåsing	Prisøkninger, endrede lisensvilkår, tvungne migreringer og slutt på støtte. Denne risikoen realiseres jevnlig og koster mest over tid.	Høy	Middels

Regelverk og rammer som er relevante

- **Digitalsikkerhetsloven** (i kraft 1. oktober 2025) gjennomfører det første NIS-direktivet (NIS1) i norsk rett. NIS2 er ikke gjennomført i Norge ennå og ventes som endringer i loven. Virksomheter som leverer samfunnsviktige tjenester, må styre risiko i leverandørkjeden. [9]
- **Personvernforordningen (GDPR)** krever et gyldig grunnlag for overføring av personopplysninger til land utenfor EØS. For USA gjelder EU-US Data Privacy Framework i dag, men de to forrige rammeverkene ble kjent ugyldige i 2015 og 2020. [8]
- **Sikkerhetsloven og arkivloven** stiller egne krav til skjermingsverdig informasjon og til at arkivverdig materiale kan bevares og leveres ut.
- **Stortinget** ba i 2026 regjeringen kartlegge Norges digitale avhengigheter løpende, med første rapport innen utgangen av 2026 (Innst. 225 S (2025-2026)). [1]
- **EUs rammeverk for suverenitet i skyen** (Cloud Sovereignty Framework) scorer tjenester fra SEAL-0 til SEAL-4 på åtte mål, og brukes allerede i europeiske anskaffelser. [6]
- **Cloud and AI Development Act (CADA)** er et forslag fra juni 2026 med fire sikkerhetsnivåer. Nivå 3 krever europeisk eierskap og kontroll. Forslaget er ikke vedtatt, og EØS-relevansen er ikke avklart. [7]

Kontroll, ikke lokasjon. Data i et europeisk datasenter er fortsatt underlagt et annet lands jurisdiksjon hvis leverandøren er kontrollert derfra. «Driftet i EU» er derfor ikke det samme som «under europeisk jurisdiksjon». Vurder arbeidslastene mot kravet om europeisk eierskap.

03 · FUNN

Avhengighetsregister

Tabellen viser tjenestene utenfor Europa som kartleggingen fant, sortert etter samlet risiko. Risikoen vurderes på tre akser: rettslig tilgang (R), sanksjoner og avstengning (S) og kommersiell innlåsing (I).

OMRÅDE	TJENESTE	LAND	R	S	I	INNSATS
Enhetsstyring `enterpriseenrollment.hi.no → enterpriseenrollment.manage.microsoft.com`	Microsoft Intune	US	●●●	●●●	●●●	Middels
E-postplattform `spf.protection.outlook.com`	Exchange Online (Microsoft 365)	US	●●●	●●●	●●●	Høy
Kontor og samhandling `Entra tenant, tenant_region_scope=EU, sign-in Managed`	Microsoft 365	US	●●●	●●●	●●●	Høy
Identitet og tilgang `enterpriseregistration.hi.no → enterpriseregistration.windows.net`	Microsoft Entra ID	US	●●●	●●●	●●●	Høy
Kontor og samhandling `lyncdiscover.hi.no → webdir.online.lync.com`	Microsoft Teams	US	●●●	●●●	●●●	Høy
KI-tjenester `anthropic-domain-verification-hh9bgj=mIXcsd6mRvJPKGfQte7qOSqsw`	Anthropic (Claude)	US	●●●	●●●	●●○	Lav
Kontor og samhandling `atlassian-sending-domain-verification=47ac593a-be93-4457-974d-698bd2c75fe6`	Atlassian (Jira, Confluence)	US	●●●	●●○	●●●	Lav
Nettsted: drift, CDN og DNS `cdnjs.cloudflare.com`	Cloudflare CDN	US	●●●	●●●	●●○	Middels
Nettsted: drift, CDN og DNS `2603:1020:e01:16::b AS8075 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US`	Microsoft Azure	US	●●●	●●●	●●○	Middels
Sporing og analyse `www.google-analytics.com`	Google Analytics	US	●●●	●○○	●○○	Lav
Tredjepartsinnhold på nettsidene `maxcdn.bootstrapcdn.com`	BootstrapCDN	US	●●○	●○○	●○○	Lav
Tredjepartsinnhold på nettsidene `fonts.googleapis.com`	Google Fonts	US	●●○	●○○	●○○	Lav
Tredjepartsinnhold på nettsidene `ajax.googleapis.com`	Google Hosted Libraries	US	●●○	●○○	●○○	Lav
TLS-sertifikater `Let's Encrypt TLS`	Let's Encrypt	US	●○○	●●○	●○○	Lav

OMRÅDE	TJENESTE	LAND	R	S	I	INNSATS
Sporing og analyse app-script.monsido.com	Monsido (Acquia)	US	●●	●	●	Lav
Tredjepartsinnhold på nettsidene cdn.jsdelivr.net	jsDelivr	US	●●	●	●	Lav

Spor av norske og europeiske tjenester

NO Sikt (Uninett)

Oppgitt i personvernerklæringen

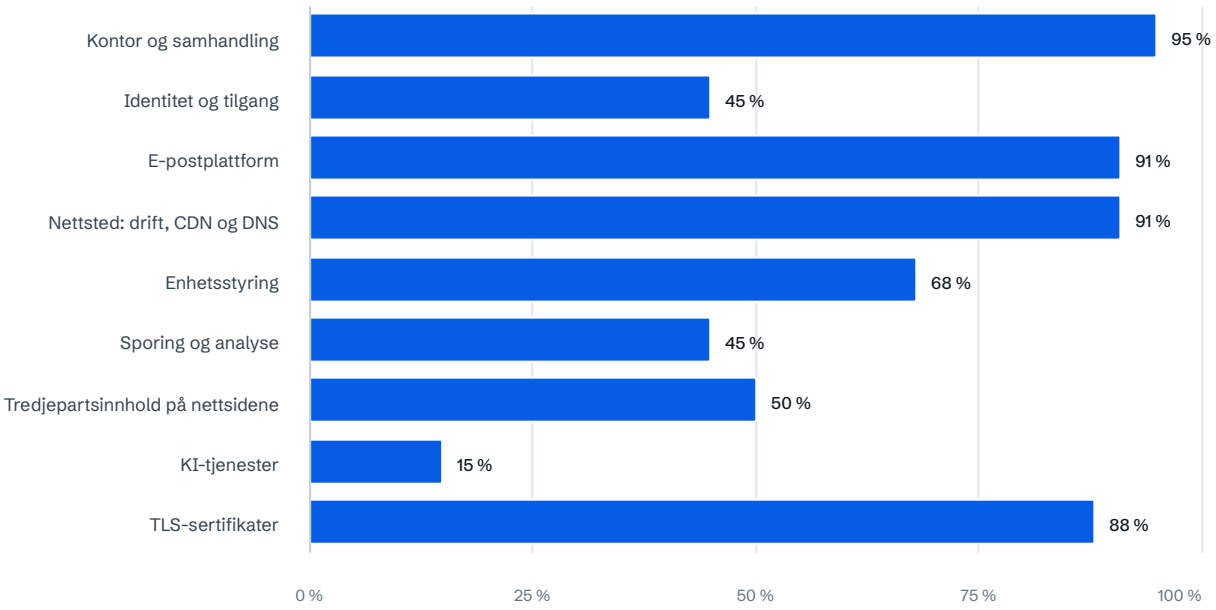
Leverandører og produkter som virksomheten selv navngir i personvernerklæringen. Et navn viser at tjenesten er nevnt, ikke nødvendigvis at den er i bruk. Funnene påvirker ikke eksponeringsindeksen.

LEVERANDØR	LAND	PRODUKTER	GRUNNLAG	SKANN
UTENFOR EUROPA				
Google	US	Google Analytics	Nevnt i teksten	Også funnet
Intuit	US	Mailchimp	Nevnt i teksten	Ikke funnet
Meta	US	Facebook	Nevnt i teksten	Ikke funnet
Monsido	US	Nettstatistikk	Nevnt i teksten	Også funnet

Kilder: www.hi.no/hi/om-oss/havforskningsinstituttet-sin-personvernerklering · www.hi.no/hi/om-oss/informasjonskapsler

Hvor vanlig er avhengigheten?

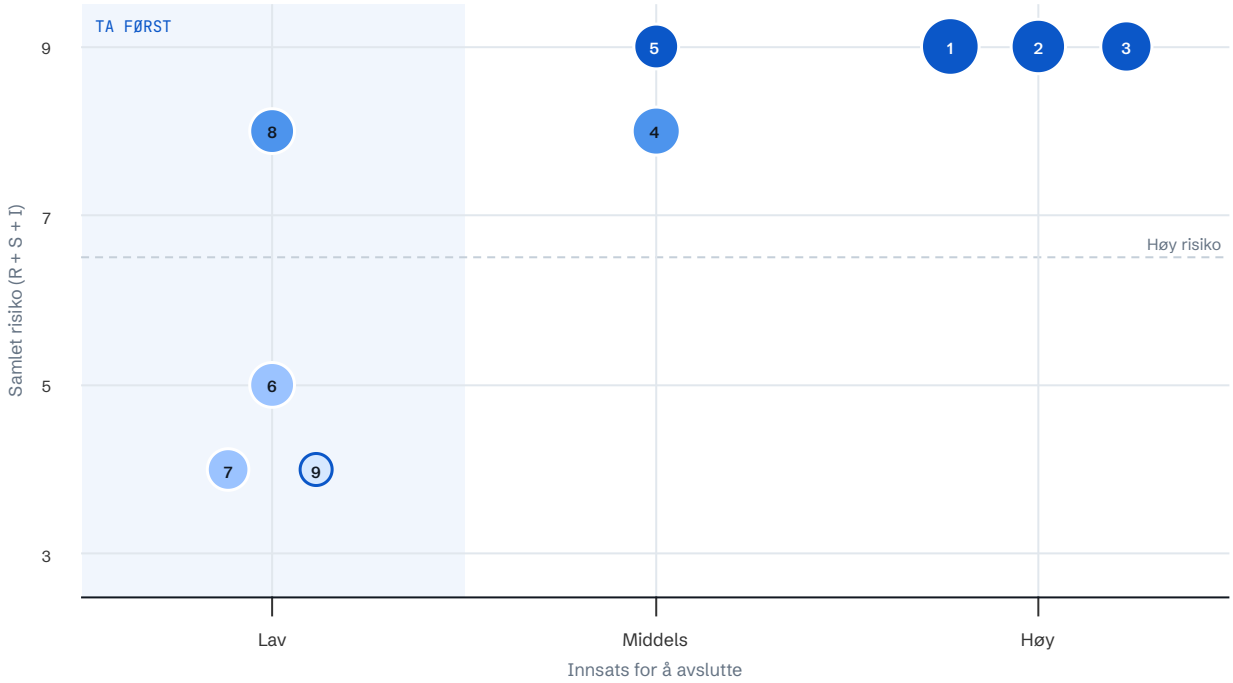
Andel av de statlige virksomhetene med samme område



04 · RISIKOVURDERING

Risiko og innsats per område

Matrisen plasserer hvert område etter høyeste risiko og innsatsen som trengs for å avslutte avhengigheten. Områder med høy risiko og lav innsats bør tas først. Boblenes størrelse viser hvor mye området veier i indeksen. Tallene i boblene viser radene i tabellen under.



OMRÅDE	VEKT	RISIKO (AV 9)	INNSATS	FASE	STRATEGI
1. Kontor og samhandling	16	9	Høy	3	REDUSER, DERETTER AVSLUTT
2. Identitet og tilgang	14	9	Høy	3	REDUSER, DERETTER AVSLUTT
3. E-postplattform	12	9	Høy	3	REDUSER, DERETTER AVSLUTT
4. Nettsted: drift, CDN og DNS	10	8	Middels	2	AVSLUTT
5. Enhetsstyring	8	9	Middels	3	REDUSER, DERETTER AVSLUTT
6. Sporing og analyse	8	5	Lav	1	AVSLUTT (RASK GEVINST)
7. Tredjepartsinnhold på nettsidene	6	4	Lav	1	AVSLUTT (RASK GEVINST)
8. KI-tjenester	0	8	Lav	2	AVSLUTT
9. TLS-sertifikater	0	4	Lav	4	AKSEPTER OG DOKUMENTER

Kontor og samhandling

Store datamengder og høy brukerpåvirkning. Kostnaden ligger i opplæring, dokumentkompatibilitet og integrasjoner, ikke i lisensene. Microsoft-tjenestene henger sammen. Planlegg dem som én plattform, ikke hver for seg.

Identitet og tilgang

Identitet er den dypeste innlåsingen. Stopper tjenesten, stopper også tilgangen til alt som er koblet til den.

E-postplattform

All korrespondanse med innbyggere og leverandører passerer her. Kalender og delte postkasser er den vanskelige delen av en migrering.

Nettsted: drift, CDN og DNS

Nettstedet er innbyggernes inngang til tjenestene. Driftsleverandøren ser all trafikk, og DNS er en enkelt feilkilde for hele domenet.

Enhetsstyring

Enhetsstyringen har administratortilgang til alle klientene. I skolen gjelder det ofte tusenvis av elevenheter.

Sporing og analyse

Sporing samler data om innbyggerne og krever samtykke etter ekomloven. Den er sjelden nødvendig for å levere tjenesten. Flere europeiske datatilsyn har konkludert med at tidligere bruk av Google Analytics innebar ulovlig overføring. I dag kan overføringen baseres på EU-US Data Privacy Framework, men det rettslige grunnlaget har falt to ganger før.

Tredjepartsinnhold på nettsidene

Hver innlasting sender innbyggerens IP-adresse til leverandøren. Det er en overføring av personopplysninger, ofte uten at noen har vurdert den. En tysk domstol har tidligere ilagt erstatning for å laste Google Fonts uten samtykke (LG München, 2022). Lav risiko. Filene er åpne kodebiblioteker. Å legge dem på eget nettsted er en enkel jobb som også hindrer at besøkendes IP-adresser sendes til tredjepart.

KI-tjenester

Tre spørsmål avgjør risikoen: hvem som har trent modellen, hvem som drifter den, og hvor beregningen skjer. API-tilgang kan begrenses av sanksjoner og eksportregler.

TLS-sertifikater

Lav risiko. Sertifikatutstederen ser ikke trafikken. Risikoen er at utstedelse eller fornyelse stopper, og den reduseres ved å ha to utstedere klare. Behold og dokumenter. Ha en europeisk utsteder klar som reserve.

05 · ALTERNATIVER

Norske og europeiske alternativer

Alternativene er utgangspunkt for en markedsdialog, ikke en anbefaling av én leverandør. Norske leverandører er nevnt først der de finnes. Et alternativ er ikke automatisk bedre, og hvert valg krever en vurdering av arbeidslasten.

Kontor og samhandling

Erstatter: Microsoft 365, Microsoft Teams og Atlassian (Jira, Confluence)

ALTERNATIV	LAND	TYPE	BESKRIVELSE
Nextcloud Hub	DE Tyskland	Selvdrift eller tjeneste	Filer, deling, kalender, chat og videomøter. Kan driftes selv eller av norsk leverandør.
openDesk	DE Tyskland	Selvdrift	Komplett digital arbeidsplass fra tyske ZenDiS, bygget på Nextcloud, Open-Xchange, Collabora og Element. Som skytjeneste er den bare tilgjengelig for medlemmer av den tyske innkjøpsavtalen govdigital. Ellers må den driftes i egne datasentre eller hos en skyleverandør. Ingen større leverandører i Norge tilbyr den ennå. Valgt av Den internasjonale straffedomstolen (ICC).
LibreOffice	DE Tyskland	Åpen kildekode	Kontorpakke fra The Document Foundation. Valgt av det danske digitaliseringsdepartementet.
Collabora Online	UK Storbritannia	Selvdrift eller tjeneste	Dokumentredigering i nettleseren, bygget på LibreOffice. Integreres i Nextcloud og openDesk.
Pexip	NO Norge	Tjeneste eller selvdrift	Norsk videomøteleverandør med løsning som kan driftes i egen infrastruktur. Brukes i offentlig sektor og forsvar.
Whereby	NO Norge	Tjeneste	Norsk tjeneste for videomøter i nettleseren, uten installasjon.
Element (Matrix)	UK Storbritannia	Selvdrift eller tjeneste	Kryptert chat og samarbeid på den åpne Matrix-protokollen. Kan driftes helt i egen infrastruktur.
OpenProject	DE Tyskland	Selvdrift eller tjeneste	Prosjekt- og oppgavestyring med åpen kildekode. Del av openDesk.
XWiki	FR Frankrike	Selvdrift eller tjeneste	Wiki og kunnskapsbase fra Frankrike, med import fra Confluence.

Identitet og tilgang

Erstatter: Microsoft Entra ID

ALTERNATIV	LAND	TYPE	BESKRIVELSE
Keycloak (selvdrevet)	OSS Åpen kildekode	Åpen kildekode	Identitetsplattform med SAML og OIDC, driftet i egen eller norsk infrastruktur.
Univention Nubus	DE Tyskland	Selvdrift eller tjeneste	Identitets- og katalogtjeneste. Brukt i tysk skole og forvaltning, og i openDesk.
Zitadel	CH Sveits	Selvdrift eller tjeneste	Sveitsisk identitetsplattform med OIDC og SAML. Har amerikanske investorer på eiersiden.

E-postplattform

Erstatter: Exchange Online (Microsoft 365)

ALTERNATIV	LAND	TYPE	BESKRIVELSE
JCloud ComSuite	NO Norge	Tjeneste	Norskeid. Kontorpakke i skyen med e-post, kalender, filområde og IP-telefoni. Produktsiden oppgir ikke hvor dataene lagres.
Open-Xchange	DE Tyskland	Selvdrift eller via leverandør	E-post og kalender for store organisasjoner. Leveres ofte via en lokal driftspartner.
grommunio	AT Østerrike	Selvdrift eller via partner	Østerriksk gruppevare som erstatter Exchange. Støtter Outlook, ActiveSync og delte postkasser. Test ressurskalendere i en pilot før dere bestemmer dere.
openDesk	DE Tyskland	Selvdrift	Komplett digital arbeidsplass fra tyske ZenDiS, bygget på Nextcloud, Open-Xchange, Collabora og Element. Som skytjeneste er den bare tilgjengelig for medlemmer av den tyske innkjøpsavtalen govdigital. Ellers må den driftes i egne datasentre eller hos en skyleverandør. Ingen større leverandører i Norge tilbyr den ennå. Valgt av Den internasjonale straffedomstolen (ICC).
Infomaniak kSuite	CH Sveits	Tjeneste	E-post, lagring og kontorverktøy fra sveitsisk leverandør.

Nettsted: drift, CDN og DNS

Erstatter: Cloudflare CDN og Microsoft Azure

ALTERNATIV	LAND	TYPE	BESKRIVELSE
Myra Security	DE Tyskland	CDN og DDoS-vern	Tysk CDN, DDoS-vern og DNS med vekt på kritisk infrastruktur.
Bunny.net	SI Slovenia	CDN	Innholdsnettverk og DNS fra Slovenia.
Link11	DE Tyskland	DDoS-vern	Tysk leverandør av DDoS-vern og CDN.
Safespring	SE Sverige	Skyplattform	Nordisk sky med datasentre i Norge og Sverige.
Redpill Linpro	NO Norge	Drift og skyplattform	Nordisk leverandør av drift og sky basert på åpen kildekode.
JCloud	NO Norge	Skyplattform	Norskeid. VPS med dedikerte ressurser, databaser (blant annet PostgreSQL, MySQL/MariaDB, MongoDB og Redis) og tilgang til GPU. Datasentre i Oslo og Stavanger. ISO 27001-sertifisering er under arbeid.
UpCloud	FI Finland	Skyplattform	Finsk skyplattform med europeiske datasentre.
OVHcloud	FR Frankrike	Skyplattform	Europas største skyleverandør, med fransk eierskap.

Enhetsstyring

Erstatter: Microsoft Intune

ALTERNATIV	LAND	TYPE	BESKRIVELSE
Relution	DE Tyskland	Tjeneste eller selvdrift	Enhetsstyring for iPad, Windows og Android. Mye brukt i tysk skole.
baramundi Management Suite	DE Tyskland	Selvdrift eller tjeneste	Klient- og enhetsstyring fra Tyskland.
Matrix42	DE Tyskland	Selvdrift eller tjeneste	Enhets- og tjenestestyring fra Tyskland.

Sporing og analyse

Erstatter: Google Analytics og Monsido (Acquia)

ALTERNATIV	LAND	TYPE	BESKRIVELSE
Matomo (selvdrevet)	OSS Åpen kildekode	Åpen kildekode	Webanalyse som driftes på egen server. Kan settes opp uten informasjonskapsler.
Plausible	EE Estland	Tjeneste	Enkel webanalyse uten informasjonskapsler, med drift i EU.
Piwik PRO	PL Polen	Tjeneste	Polsk webanalyse med drift i EU. Eies av danske Cookie Information Group.
Siteimprove	DK Danmark	Tjeneste	Dansk plattform for kvalitet, tilgjengelighet og analyse. Brukt av flere norske kommuner.
Analyse av serverlogger	NO Norge	Tiltak	Besøksstatistikk fra nettstedets egne logger. Ingen kode i nettleseren.

Tredjepartsinnhold på nettsidene

Erstatter: BootstrapCDN, Google Fonts og Google Hosted Libraries

ALTERNATIV	LAND	TYPE	BESKRIVELSE
Selvhosting på eget domene	NO Norge	Tiltak	Last ned filene og server dem fra eget nettsted. Ingen leverandør, ingen overføring.
Bunny.net	SI Slovenia	CDN	Innholdsnettverk og DNS fra Slovenia.

KI-tjenester

Erstatter: Anthropic (Claude)

ALTERNATIV	LAND	TYPE	BESKRIVELSE
Mistral AI	FR Frankrike	Tjeneste og åpne modeller	Fransk utvikler av språkmodeller. Flere modeller kan driftes selv.

ALTERNATIV	LAND	TYPE	BESKRIVELSE
Norske språkmodeller	NO Norge	Åpne modeller	Modeller fra Nasjonalbibliotekets KI-lab og NorwAI (NTNU), driftet på norsk eller europeisk infrastruktur.
JCloud AI	NO Norge	Tjeneste	Norskeid. KI-API som kjører på GPU-er, med mulighet for egne modeller og GPU-tilgang fra VPS. Hvilke modeller som tilbys og hvor beregningen skjer, står ikke oppgitt.
Åpne modeller i egen drift	OSS Åpen kildekode	Tiltak	Modeller med åpne vekter driftet på europeisk eller norsk GPU-kapasitet. Ingen data forlater egen kontroll.

TLS-sertifikater

Erstatter: Let's Encrypt

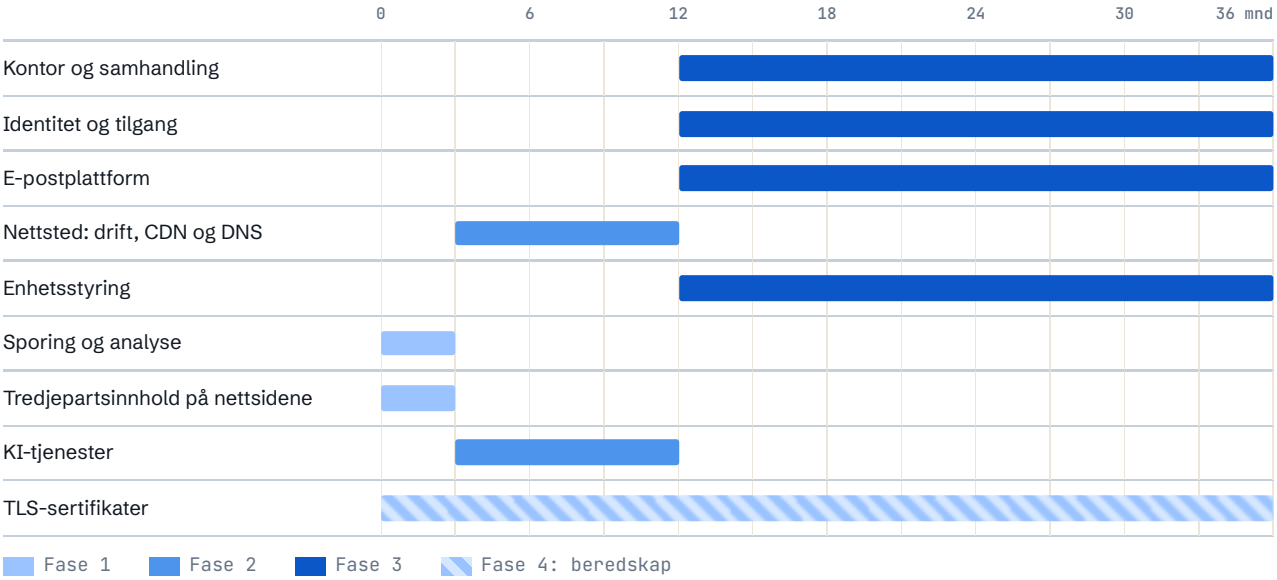
ALTERNATIV	LAND	TYPE	BESKRIVELSE
HARICA	GR Hellas	Sertifikatutsteder	Gresk akademisk sertifikatutsteder med støtte for ACME.
Certum	PL Polen	Sertifikatutsteder	Polsk sertifikatutsteder fra Asseco. Støtter ACME for automatisk fornyelse.
Actalis	IT Italia	Sertifikatutsteder	Italiensk sertifikatutsteder.

> Eierskap, hovedkontor og driftssted endrer seg. Verifiser hver leverandør før anskaffelse. Oversikten ble sist kontrollert oktober 2026.

06 · EXIT-PLAN

Exit i fire faser

Rekkefølgen følger én regel: start med det som er billig og reversibelt, og ta identiteten sist. Eksisterende løsning driftes parallelt til hver bølge er bekreftet. Varighetene er typiske rammer og må justeres etter intern kartlegging.



FASE 1 · 0 TIL 3 MÅNEDER

Raske gevinster

Tiltak som er billige, reversible og gir synlig effekt. De krever lite mer enn en beslutning og noen dagers arbeid.

- **Sporing og analyse:** Google Analytics og Monsido (Acquia). Vurder Matomo (selvdrevet), Plausible og Piwik PRO.
- **Tredjepartsinnhold på nettsidene:** BootstrapCDN, Google Fonts og Google Hosted Libraries. Vurder Selvhosting på eget domene og Bunny.net.

FASE 2 · 3 TIL 12 MÅNEDER

Infrastruktur og tjenester

Bytte av drift, utsending og enkeltstående skytjenester. Krever anskaffelse og testing, men lite opplæring av brukere.

- **Nettsted: drift, CDN og DNS:** Cloudflare CDN og Microsoft Azure. Vurder Myra Security, Bunny.net og Link11.
- **KI-tjenester:** Anthropic (Claude). Vurder Mistral AI, Norske språkmodeller og JCloud AI.

FASE 3 · 12 TIL 36 MÅNEDER

Plattform og identitet

De store avhengighetene: kontorplattform, e-post, enheter og identitet. Gjøres i bølger, med pilot først og eksisterende løsning i drift parallelt.

- **Kontor og samhandling:** Microsoft 365, Microsoft Teams og Atlassian (Jira, Confluence). Vurder Nextcloud Hub, openDesk og LibreOffice.
- **Identitet og tilgang:** Microsoft Entra ID. Vurder Keycloak (selvdrevet), Univention Nubus og Zitadel.
- **E-postplattform:** Exchange Online (Microsoft 365). Vurder JCloud ComSuite, Open-Xchange og grommunio.
- **Enhetsstyring:** Microsoft Intune. Vurder Relution, baramundi Management Suite og Matrix42.

FASE 4 · LØPENDE

Exit-beredskap

Avhengigheter som er akseptable å beholde, eller som ikke har et realistisk alternativ i dag. De dokumenteres med en testet exit-plan.

- **Tredjepartsinnhold på nettsidene:** jsDelivr.
- **TLS-sertifikater:** Let's Encrypt.

07 · GJENNOMFØRING

Steg for steg, per område

Stegene beskriver en typisk gjennomføring. De forutsetter at områdets eier er utpekt, og at dagens løsning er dokumentert før arbeidet starter.

Kontor og samhandling

12 TIL 36 MÅNEDER

1. Kartlegg bruken: lisenser, team og kanaler, delte områder, integrasjoner og automatiseringer.
2. Klassifiser informasjonen etter sensitivitet, og sett et mål for suverenitetsnivå per klasse.
3. Velg målarkitektur. En hybrid løsning der sensitive data flyttes først, er ofte mest realistisk.
4. Gjennomfør en pilot med én avdeling i 8 til 12 uker, med opplæring og målepunkter.
5. Migrer i bølger. Behold dagens plattform i lesemodus i en overgangsperiode.
6. Avslutt lisenser, eksporter arkivverdig materiale og dokumenter slettingen hos leverandøren.

Identitet og tilgang

12 TIL 24 MÅNEDER

1. Kartlegg alle applikasjoner som logger inn via dagens identitetsplattform, og hvilke protokoller de bruker (SAML, OIDC, LDAP).
2. Etabler en europeisk eller selvdrevet identitetsplattform parallelt, med samme brukerkatalog som kilde.
3. Koble mot ID-porten og Feide der innbyggere, elever eller ansatte skal logge inn med nasjonale løsninger.
4. Flytt applikasjoner i bølger, de enkleste først. Test flerfaktor og tilgangsregler for hver bølge.
5. Avslutt den gamle plattformen sist, når ingen applikasjoner er avhengige av den.

E-postplattform

6 TIL 18 MÅNEDER

1. Kartlegg postkasser, delte postkasser, ressurskalendere, regler og integrasjoner som sender e-post.
2. Velg ny plattform og sett opp domenet parallelt med en egen testsone.
3. Migrer postkasser og kalendere i bølger med verktøy som bevarer mappestruktur og metadata.
4. Bytt MX-poster, og oppdater SPF, DKIM og DMARC samtidig. Senk TTL på forhånd.
5. Behold gammel plattform i lesemodus til arkivering og eksport er bekreftet.

Nettsted: drift, CDN og DNS

1 TIL 6 MÅNEDER

1. Eksporter DNS-sonen og dokumenter alle poster. Senk TTL to uker før bytte.
2. Velg europeisk drift og CDN med DDoS-vern. Still krav om europeisk eierskap i anskaffelsen.
3. Sett opp nettstedet hos ny leverandør, test med midlertidig vertsnavn og last.
4. Bytt DNS i et lavtrafikkvindu, og behold gammel drift i to uker som tilbakefall.

Enhetsstyring

6 TIL 12 MÅNEDER

1. Kartlegg enheter per type og eier, og hvilke policyer og apper som rulles ut i dag.
2. Velg europeisk enhetsstyring og bygg policyene på nytt i en testgruppe.
3. Flytt enheter i bølger, gjerne ved naturlige utskiftninger eller skoleårsstart.
4. Behold produsentenes egne registreringsprogram (for eksempel Apple School Manager) og koble dem til ny løsning.

Sporing og analyse

1 TIL 4 UKER

1. Vurder om sporingen faktisk brukes til beslutninger. Fjern det som ikke brukes.
2. Erstatt nødvendig analyse med en europeisk, informasjonskapselfri løsning eller analyse av serverlogger.
3. Oppdater personvernerklæringen og samtykkeløsningen. Ofte kan samtykkebanneret fjernes helt.

Tredjepartsinnhold på nettsidene

1 TIL 4 UKER

1. Last ned skrifttyper og biblioteker og legg dem på eget domene. Lisensene tillater det i de fleste tilfeller.
2. Erstatt innebygde kart med Kartverkets tjenester eller en norsk kartleverandør.
3. Last video først når brukeren klikker, eller flytt video til en europeisk plattform.
4. Legg inn en Content-Security-Policy som hindrer at nye tredjepartskilder sniker seg inn.

KI-tjenester

2 TIL 6 MÅNEDER

1. Kartlegg hvem som bruker tjenesten, til hva, og hvilke data som sendes inn.
2. Vedta retningslinjer for hvilke opplysninger som kan brukes i KI-verktøy.
3. Etabler en testet europeisk eller selvdrevet reservemodell for kritisk bruk.
4. Gjennomfør en personvernkonsekvensvurdering (DPIA) for bruk med personopplysninger.

Exit-beredskap for det som beholdes

ÅRLIG

1. Beskriv hvorfor avhengigheten er akseptert, og hvem som har akseptert den.
2. Dokumenter hvordan data eksporteres, i hvilket format og hvor lang tid det tar.
3. Test eksporten minst én gang i året, og rapporter resultatet til ledelsen.
4. Vurder avhengigheten på nytt ved hver kontraktsfornyelse.

08 · ANSKAFFELSE OG KONTRAKT

Krav som gir exit-mulighet

Digital suverenitet kan brukes som kvalifikasjonskrav eller tildelingskriterium innenfor anskaffelsesregelverket, så lenge kravene er saklige, forholdsmessige og knyttet til leveransen. Kravene under kan tilpasses hver anskaffelse.

- [ ] **Jurisdiksjon og eierskap.** Leverandøren oppgir morselskap og hvilke lands myndigheter som kan kreve utlevering av data.
- [ ] **Suverenitetsnivå.** Minstenivå (SEAL-gulv) per suverenitetsmål, tilpasset informasjonens sensitivitet.
- [ ] **Europeisk eierskap for sensitive arbeidslaster.** Vurder kravet i CADA nivå 3 som tildelingskriterium der det er relevant.
- [ ] **Dataretur.** Alle data leveres tilbake i åpent, dokumentert format innen avtalt frist ved avslutning.
- [ ] **Exit-bistand.** Leverandøren plikter å bistå ved overgang til ny leverandør, til avtalt pris.
- [ ] **Sletting.** Dokumentert sletting hos leverandør og underleverandører etter avslutning.

- [ ] **Underleverandører.** Full oversikt over underleverandører, med varsel og innsigelsesrett ved endringer.
- [ ] **Nøkkelkontroll.** Kunden kan holde krypteringsnøklene selv for sensitive data.
- [ ] **Logger og drift.** Hvor logger lagres, og hvem som har driftstilgang fra hvilket land.
- [ ] **Åpenhet om myndighetskrav.** Leverandøren varsler om krav om utlevering så langt loven tillater, og publiserer åpenhetsrapporter.
- [ ] **Revisjon.** Rett til innsyn og revisjon, også hos sentrale underleverandører.

Bruk relevante Statens standardavtaler (SSA) for drift og skytjenester som utgangspunkt, og legg kravene inn i bilagene. En kravspesifikasjon bør tilpasses tjenesten, datatypene og exit-kravene i den aktuelle anskaffelsen.

09 · STYRING OG OPPFØLGING

Roller, måltall og kostnaden ved å vente

ROLLE	ANSVAR I EXIT-ARBEIDET
Virksomhetsleder	Eier strategien, vedtar suverenitetsmål og aksepterer gjenværende risiko.
IT-sjef eller digitaliseringsleder	Eier exit-planen og leder gjennomføringen fase for fase.
Sikkerhetsleder	Vurderer risiko og påser at krav i digitalsikkerhetsloven og sikkerhetsloven ivaretas.
Personvernombud	Vurderer overføringsgrunnlag og konsekvenser for personvernet (DPIA).
Innkjøp	Legger kravene inn i anskaffelser og kontrakter.
Arkivleder	Påser at arkivverdig materiale eksporteres og bevares.
Tillitsvalgte og brukere	Deltar i pilot og opplæring. Brukeraksept avgjør om exit lykkes.

Måltall

MÅLTALL	I DAG	MÅL
Eksponeringsindeks	74	50.0 etter 12 måneder, 0 etter 36 måneder
Tredjepartskilder utenfor Europa på nettstedet	5	0 etter 3 måneder
Arbeidslaster klassifisert etter sensitivitet	Ukjent	100 % etter 6 måneder
Beholdte avhengigheter med testet exit-plan	0	Alle, testet årlig

Hva skjer om virksomheten ikke gjør noe?

Avhengighetene blir dypere for hvert år, fordi nye tjenester bygges på samme plattform. Kostnaden ved en senere exit øker, mens forhandlingsposisjonen svekkes. Samtidig vil spørsmålene fra Stortinget, tilsynsmyndigheter, revisjon og presse komme, uavhengig av om virksomheten har svarene.

10 · NESTE STEG

De første 90 dagene

NÅR	TILTAK
30 dager	Utpek eier av exit-planen. Bekreft funnene i dette utkastet internt. Fjern sporing og tredjepartskilder som ikke brukes.
60 dager	Gjennomfør en intern kartlegging av fagsystemer og dataflyt. Klassifiser arbeidslastene. Legg inn en europeisk reserve for sertifikater.
90 dager	Legg frem strategi og suverenitetsmål for ledelsen. Vedta planen for fase 2 og 3, og sett av budsjett til forstudie og pilot.

Før dette blir en beslutning

Bekreft funnene internt. Knytt hver avhengighet til data, kontrakt, systemeier og en testet mulighet for uttrekk eller erstatning.

VEDLEGG A · METODE

Hvordan kartleggingen ble gjort

Kartleggingen ble gjennomført 20.10.2026 mot hi.no. Den samler bare signaler som er offentlig tilgjengelige for alle.

- **DNS:** navnetjenere, MX-poster, SPF, DMARC, DKIM og verifiseringsposter som viser hvilke skytjenester domenet er koblet til.
- **Kjente Microsoft-poster:** autodiscover, lyncdiscover, enterpriseenrollment og enterpriseregistration.
- **Drift:** IP-adresser og hvem som eier nettverket (ASN), og CNAME-kjeder til drifts- og CDN-leverandører.
- **Sertifikat:** hvem som har utstedt TLS-sertifikatet.
- **Nettsider:** forsiden, opptil fem sentrale undersider og tredjepartsskript, analysert for eksterne kilder.
- **Subdomener:** 73 kandidater fra sertifikatlogger og en ordliste, hvorav 4 svarte.
- **Personvernerklæring:** erklæringen og tilhørende sider ble funnet via lenker fra forsiden. Publiserte behandlingsprotokoller (Samsvar) ble lest som strukturerte data. Teksten ble sammenlignet med en liste over kjente produkter og leverandører.

Eksponeringsindeksen

Hvert område har en vekt etter hvor kritisk det er. Indeksen er summen av vektene for områdene der kartleggingen fant minst én avhengighet utenfor Europa. Områder med bare aksepterte avhengigheter teller 25 prosent.

OMRÅDE	VEKT	OMRÅDE	VEKT
Identitet og tilgang	14	Fjerntilgang	4
Kontor og samhandling	16	E-postplattform	12
E-postutsending og e-postsikkerhet	4	Enhetsstyring	8
Nettsted: drift, CDN og DNS	10	Tredjepartsinnhold på nettsidene	6
Sporing og analyse	8	TLS-sertifikater	0
KI-tjenester	8	Fagsystemer og andre skytjenester	8

Begrensninger

- Interne systemer, fagsystemer og avtaler er ikke synlige utenfra, med mindre personvernerklæringen nevner dem.
- At en leverandør er nevnt i personvernerklæringen, betyr ikke at tjenesten er i bruk. Leverandører som ikke står på produktlisten, blir ikke fanget opp.
- En verifiseringspost viser at en konto er opprettet, ikke at den er i aktiv bruk.
- Tjenester som bare brukes av ansatte via nettleser, etterlater ofte ingen spor i DNS.
- Kartleggingen er et øyeblikksbilde. Nettsider og DNS endres.

VEDLEGG B · TEKNISK BEVISLISTE

Alle funn

TJENESTE	LAND	LAG	BEVIS
Anthropic (Claude)	US	DNS	`anthropic-domain-verification-hh9bgj=mIXcsd6mRvJPKGfQte7qOSqsw`
Atlassian (Jira, Confluence)	US	DNS	`atlassian-sending-domain-verification=47ac593a-be93-4457-974d-698bd2c75fe6`
Google Search Console	US	DNS	`google-site-verification=TYoXJYTSeSJ5GYfqavXe_8L7IICe1EYgIIfF35MFxWU`
Exchange Online (Microsoft 365)	US	DNS	`spf.protection.outlook.com`
Microsoft Entra ID	US	DNS	`enterpriseregistration.hi.no → enterpriseregistration.windows.net`
Microsoft Intune	US	DNS	`enterpriseenrollment.hi.no → enterpriseenrollment.manage.microsoft.com`
Microsoft Teams	US	DNS	`lyncdiscover.hi.no → webdir.online.lync.com`

TJENESTE	LAND	LAG	BEVIS
Microsoft Azure	US	Drift	2603:1020:e01:16::b AS8075 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US
Microsoft 365	US	Innlogging	Entra tenant, tenant_region_scope=EU, sign-in Managed
BootstrapCDN	US	Nettside	maxcdn.bootstrapcdn.com
Cloudflare CDN	US	Nettside	cdnjs.cloudflare.com
Google Analytics	US	Nettside	www.google-analytics.com
Google Fonts	US	Nettside	fonts.googleapis.com
Google Hosted Libraries	US	Nettside	ajax.googleapis.com
Monsido (Acquia)	US	Nettside	app-script.monsido.com
jsDelivr	US	Nettside	cdn.jsdelivr.net
Let's Encrypt	US	Sertifikat	Let's Encrypt TLS
Silktide	UK	Nettside	analytics.silktide.com
Sikt (Uninett)	NO	Subdomene	kart.hi.no → AS224 UNINETT - Sikt - Kunnskapssektorens Tjenesteleverandor, NO

VEDLEGG C · KILDER

Kilder

Tallene i hakeparentes i teksten viser til denne listen.

1. Innst. 225 S (2025–2026), kommunal- og forvaltningskomiteen. stortinget.no
2. Dok. 8:119 S (2025–2026), representantforslag om digital suverenitet. stortinget.no
3. ICC, Microsoft og openDesk: tidslinje. sota.io
4. Microsoft tells French lawmakers it can't protect user data from US demands (juli 2025). sdxcentral.com
5. Denmark's Digital Ministry shifts from Microsoft to LibreOffice (juli 2025). computing.co.uk
6. EU Cloud Sovereignty Framework, versjon 1.2.1 (oktober 2025). Europakommisjonen
7. The EU Cloud and AI Development Act in depth (juni 2026). insideglobaltech.com
8. EU General Court rejects challenge to EU-US data transfer framework (september 2025). scl.org
9. Nye krav for kritiske virksomheter fra oktober 2025. deloitte.com

VEDLEGG D · ORDLISTE

CLOUD Act	Amerikansk lov fra 2018 som lar myndighetene kreve data fra amerikanske leverandører, uansett hvor dataene lagres.
FISA 702	Amerikansk hjemmel for etterretning rettet mot personer utenfor USA.
DPF	EU-US Data Privacy Framework. Grunnlaget for overføring av personopplysninger til sertifiserte amerikanske selskaper.
SEAL	Suverenitetsnivå fra 0 til 4 i EUs Cloud Sovereignty Framework.

CADA	Cloud and AI Development Act. Forslag til EU-forordning fra juni 2026.
Tenant	Organisasjonens egen instans i en skytjeneste, for eksempel i Microsoft 365.
MX, SPF, DKIM, DMARC	DNS-poster som styrer hvem som mottar og får sende e-post for domenet.
CDN	Innholdsnettverk som leverer nettsider fra servere nær brukeren, ofte med DDoS-vern.
ASN	Nummeret som identifiserer hvem som eier et nettverk på internett.
Arbeidslast	Et system eller en tjeneste med tilhørende data, vurdert som én enhet.
Exit-plan	En dokumentert og testet plan for hvordan en avhengighet kan avsluttes.