



NASJONAL SKYTJENESTE

KONSEPTVALGUTREDNING (KVU)

Forord

På oppdrag fra Justis- og beredskapsdepartementet (JD) har Nasjonal sikkerhetsmyndighet (NSM) gjennomført en konseptvalgutredning (KVU) om etablering av en nasjonal skytjeneste.

Utredningen er gjennomført som et prosjekt i NSM, med faglig støtte fra Menon Economics, Holte Consulting og A-2 Norge. Ressurser fra Sopra Steria AS har også vært innleid som prosjektfaglig støtte på deler av arbeidet.

NSM vil rette en stor takk til alle som har bidratt til utredningen. Dette gjelder spesielt alle de statlige virksomhetene som har besvart utredningens spørreundersøkelse, alle markedsaktører og leverandørindustri som har bidratt med kunnskap og informasjon, og alle andre som har møtt utredningens spørsmål og behov for avklaringer med positiv interesse og engasjement.

En spesiell takk også til referansegruppen (se Vedlegg A) for stort engasjement og gode faglige diskusjoner og innspill underveis i arbeidet.

Dette dokumentet, med vedlegg, utgjør sluttrapporten fra KVU-arbeidet.

Oslo, 26. januar 2023

Harald Næss, NSM

Prosjektleder

Forord	2
Ordliste	5
Kortfattet sammendrag	8
Sammendrag	10
1 Om utredningen.....	20
1.1 Bakgrunn og mandat	20
1.2 Avgrensninger	21
1.3 Grensesnitt mot andre prosjekter	24
1.4 Metodisk tilnærming til utredningen	24
1.5 Innhold i KVVU-rapporten	25
2 Problembeskrivelse.....	26
2.1 Beskyttelsesverdige data og systemer i statsforvaltningen	27
2.2 Utfordringer ved bruk av skytjenester	34
2.3 Utfordringer ved utvikling på egne plattformer	40
3 Behovsanalyse	44
3.1 Behov for å sikre beskyttelsesverdige data og systemer i hele krisespekteret ..	46
3.2 Behov for å utnytte mulighetene som ligger i moderne skytjenester	50
4 Strategiske mål	57
4.1 Samfunnsmål	57
4.2 Effektmål	57
4.3 Mulige målkonflikter og prioritering av effektmål	58
4.4 Sammenheng med andre overordnede målsetninger	59
5 Rammebetingelser for konseptvalg	60
5.1 Rammebetingelser knyttet til leverandører og behandling av data	60
5.2 Rammebetingelser knyttet til regelverk om offentlige anskaffelser og statsstøtte	62
6 Mulighetsstudie	63
6.1 Definerings av det relevante mulighetsrommet	63
6.2 Utforming av konsepter	66
6.3 Nedvalg av konsepter	72
7 Alternativanalyse.....	75
7.1 Beskrivelse av analyserte alternativer	77

7.2	Vurdering av samfunnsøkonomiske virkninger	82
7.3	Vurdering av usikkerhet	99
7.4	Fordelingsvirkninger	108
7.5	Samlet vurdering og anbefaling	109
8	Føring for forprosjektfasen	114
8.1	Videreføring av utredningsprosjektet	114
8.2	Utdypende om skjermingsverdige informasjonssystemer	115
8.3	Eierstyring	116
8.4	Finansiering	116
8.5	Sentralt styringsdokument	118
8.6	Organisering	120
8.7	Gjennomføring	120
8.8	Avhengigheter til andre prosjekter	124
8.9	Kontraktstrategi	124
8.10	Suksessfaktorer	126

Vedlegg til rapporten:

Vedlegg A	Behovskartlegging
Vedlegg B	Rammebetingelser etter sikkerhetsloven
Vedlegg C	Juridiske vurderinger - Notat Haavind (del 1)
Vedlegg D	Virt-1902: Muligheter for en moderne IT-plattform
Vedlegg E	Mulighetsstudien
Vedlegg F	Juridiske vurderinger - Notat Haavind (del 2)
Vedlegg G	Estimering av konsepter
Vedlegg H	Usikkerhetsanalyse
Vedlegg I	Erfaringer fra andre land
Vedlegg J	Nasjonal kontroll

Ordliste

Under følger en liste av sentrale begreper som benyttes i utredningen, både i hoveddokumentet og i vedleggene.

Ord	Beskrivelse
Allmenn sky	Eies og driftes av en kommersiell aktør. Her deles ressurser med andre kunder. Kundene deler på prosesseringskapasiteten og lagringen. Ofte tilbys standardiserte løsninger som er like for alle kunder. Ofte benyttes begrepet «offentlig sky», men erfaringsmessig kan noen forveksle dette med tilknytninger til offentlig sektor, det begrepet unngås derfor i denne utredningen. Der det siteres direkte fra andres dokumenter, beholdes imidlertid begrepet "offentlig sky". På engelsk benyttes begrepet «public cloud».
Beskyttelsesverdige data og systemer	Dette er en samlebetegnelse for informasjon og informasjonssystemer som en nasjonal skytjeneste skal kunne behandle. Dette inkluderer data som er skjermingsverdig ugradert. Det inkluderer også andre data som er viktig for å sikre statsforvaltningens evne til å ivareta viktige offentlige tjenester og innfri krav til informasjonssikkerhet i regelverk ut over sikkerhetsloven.
IKT-tjenester på egendriftet plattform	I denne utredningen referer begrepet til en virksomhets IKT-tjenester på egendriftet plattform. Slike tjenester kan benytte virtualisering for å skille det fysiske laget, men mangler muligheten til rask og dynamisk skalering. Dette er IKT-tjenester som har en mer tradisjonell driftsmodell, og der innkjøp og (opp)skalering av tjenester må planlegges i god tid. Slike tjenester kan være plassert i virksomhetens eget datasenter (engelsk: on-premises), eller i co-location datasenter (kunden leier plass i et kommersielt datasenter). Der det siteres direkte fra andres dokumenter beholdes begrepet "on-prem(ises)".
Kommersiell tilbyder	I denne utredningen referer begrepet kommersiell tilbyder til en aktør som operer i skymarkedet og skaper en fortjeneste ved å utvikle og selge tjenester. En kommersiell tilbyder kan tilby en eller flere av tjenestemodellene.
Krisespekter	Begrepet krisespekter referer til ulike grader av påkjenning og/eller konsekvensene vårt samfunn eller vi som nasjon kan stå overfor, og benyttes ofte i sammenheng med totalforsvarskonseptet. Krisespekteret går gjerne over tre mulige tilstander: fred, krise eller en form for væpnet konflikt. <i>Fred</i> er en normaltilstand, og innebærer fravær av kriser, konflikter eller væpnet konflikt. En <i>krise</i> innebærer en uønsket situasjon med høy grad av usikkerhet og potensielt uakseptable konsekvenser for de enkeltpersoner, organisasjoner eller stater som rammes. En <i>væpnet konflikt</i> den mest alvorlige tilstand, og kan innebære en borgerkrig, en invasjon, en okkupasjon, eller en blanding av disse.
Lagring	Dette er prosessen der data lagres i elektronisk eller optisk form. Målet er å kunne finne og behandle disse dataene senere. Det benyttes ulike former for lagring, dette er avhengig av hvilken type data som skal lagres. På engelsk benyttes begrepet «storage».
Leverandørinnlåsing	Innlåsing innebærer at man har valgt IKT-produkter eller IKT-tjenester som «låser» kunden til en eller flere spesifikke leverandører. Man blir låst til produktet/tjenesten fordi det er store kostnader forbundet med å avslutte bruken av leverandørens produkter og tjenester. Slik innlåsing kan også bidra til å holde

Ord	Beskrivelse
	leverandørens mulige konkurrenter ute av et marked. På engelsk blir dette ofte omtalt som «vendor lock-in».
Lukket skytjeneste	En lukket skytjeneste er avgrenset til en bestemt kundegruppe, en eller flere sektorer, en eller flere virksomheter, det vil si med en begrensning i hvem som kan bli kunde/bruker av skytjenesten. I en lukket skytjeneste er de underliggende ressursene, som maskin- og programvare, dedikert til å understøtte denne skytjenesten. Ofte benyttes det litt tvetydige begrepet «privat sky», men det unngås i denne utredningen da ordet privat både kan lede mot noe som er utenfor offentlig sektor, noe som berører privatpersoner eller noe som ikke er allmenn sky. Den første og andre betydningen er ikke relevant her.
Nasjonal kontroll	Med nasjonal kontroll menes her at beskyttelsesverdige data og systemer i statsforvaltningen er underlagt norsk jurisdiksjon og reell teknisk kontroll, og at aktører fra andre land ikke har tilgang til og kontroll over data. Som et utgangspunkt innebærer dette at data lagres og behandles i Norge, og at maskinvare og alle programvarelag driftes fra Norge. Nasjonal kontroll innebærer også at data og tjenester skal være tilgjengelige i fred, krise, væpnet konflikt samt gjenopprettelsscenario. Dette for å sikre statens styringsdyktighet, handlefrihet og evne til å levere grunnleggende tjenester til befolkningen gjennom hele krisespekteret. Vedlegg J beskriver nærmere nasjonal kontroll.
Offentlig sky	Se "allmenn sky".
On-prem(ises)	Se "IKT-tjenester på egendriftet plattform".
Prosessering	Informasjonsbehandling. Dette kan for eksempel være matematiske kalkuleringer eller ulike typer transformeringer av data. På engelsk benyttes begrepet «compute».
Sikkerhetskopi	En sikkerhetskopi er en kopi av informasjon eller programvare (programvare som for eksempel virtuelle datamaskiner og virtuelle nettverk). Slikt bør kopieres jevnlig slik man kan gjenskape informasjon og systemer dersom den opprinnelige lagringen går helt eller delvis tapt. En sikkerhetskopi bør i størst mulig grad isoleres fra den opprinnelige lokasjonen for å forhindre at informasjon og programvare blir skadet ved feil eller dataangrep. På engelsk benyttes begrepet «backup».
Skjermingsverdig ugradert	Informasjon betegnes som skjermingsverdig i sikkerhetsloven dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig, jf. sikkerhetsloven § 5-1. Dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende (konfidensialitet), skal informasjonen sikkerhetsgraderes, jf. § 5-3. Dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen går tapt, blir endret eller blir utilgjengelig (integritet og tilgjengelighet), er informasjonen skjermingsverdig, men skal ikke sikkerhetsgraderes. Denne kategorien betegnes som skjermingsverdig ugradert informasjon.
Skytjeneste	Skytjenester er skalerbare tjenester som leveres over internett. Ved bruk av skytjenester betaler kunden bare for den kapasiteten som blir bestilt. Dette skiller seg fra tradisjonell tjenesteutsetting, da kunden betaler for tilgjengelig ressurser uansett om de benyttes eller ikke.

Ord	Beskrivelse
Spesialutviklede løsninger	Spesialutviklede løsninger er laget for å dekke enkelte spesielle behov i en virksomhet. Spesialutviklede løsninger er aktuelle når virksomhetenes behov ikke dekkes av hyllevare- eller standardløsninger. Mange fagsystemer i offentlig forvaltning er spesialutviklede løsninger, som understøtter ett eller flere fagområder. Eksempler på dette er fagsystem i det statlige barnevernet (BiRK), statsbudsjettets samhandlingsverktøy for budsjettdata (Budmod), utlendingsmyndighetenes datasystem for utlendings- og flyktningesaker (DUF).
Standardløsninger	Standardløsninger er systemer som er kommersielt utviklet for en større kundegruppe, men som kan tilpasses enkeltkunder gjennom konfigurering og oppsett. Eksempler på standardløsninger er saks- og arkivsystem (for eksempel ePhorte, Public 360, DocuLive), økonomi- og lønssystemer (for eksempel SAP, Agresso/Unit4, Visma), ERP-løsninger (for eksempel SAP, Oracle) og pasientjournalssystemer (EPJ).
Tjenestemodeller for sky	
IaaS	IaaS er en forkortelse for «Infrastructure as a Service» og er en modell hvor kunden får tilgang til infrastruktur bestående av virtuelle servere og virtuelle nettverk, hvor de kan utvikle og drifte egne IKT-løsninger. Kunden har kontroll over operativsystem, programvare og applikasjoner, men har ikke kontroll over underliggende fysisk maskinvare og underliggende programvare.
PaaS	PaaS er en forkortelse for «Plattform as a Service» og er en modell hvor kunden får tilgang til en plattform, hvor kunden kan utvikle og drifte egne applikasjoner. Kunden har kontroll over applikasjonene, men har i utgangspunktet ikke kontroll over maskinvare, servere, nettverk, operativsystem eller annen programvare som inngår i plattformen. PaaS-tjenester vil for eksempel tilby en database-plattform eller en container-plattform.
SaaS	SaaS er en forkortelse for «Software as a Service» og er en modell hvor kunden benytter leverandørens applikasjoner via internett. Kunden har i utgangspunktet ikke kontroll over verken maskinvare, servere, nettverk, operativsystem, programvare eller applikasjoner. Eksempler er verktøy som Microsoft Office 365, flere Nextcloud tjenester, norske arkivsystemtjenester, videokonferansesystemer som Zoom og filagringstjenester som Dropbox og norske Jottacloud.

Kortfattet sammendrag

Staten forvalter betydelig mengder ugraderte data og systemer som krever særskilt beskyttelse. Etter hvert som Statsforvaltningens bruk av skytjenester øker, vil også mer av de beskyttelsesverdige dataene og systemene flyttes ut i sky. Bruk av skytjenester gir tilgang på moderne teknologi med stor fleksibilitet som det er vanskelig å oppnå med IKT-løsninger utviklet og driftet på egen plattform. Med bruk av skytjenester gir imidlertid virksomhetene fra seg en del av kontrollen over infrastruktur, systemer og data som lagres og behandles i skyen. Det innebærer at dersom dagens utviklingstrender fortsetter, vil om lag 80 prosent av beskyttelsesverdige data og systemer ligge i skybaserte løsninger innen ti år. De fleste av disse løsningene vil være helt eller delvis utenfor norsk jurisdiksjon og kontroll.

Manglende nasjonal kontroll vil svekke myndighetenes evne til sikre dataenes og systemenes konfidensialitet, integritet og tilgjengelighet. Det gir økt risiko for forringelse eller bortfall av sentrale offentlige tjenester som kan få store konsekvenser for samfunnet, både i fred, krise og i en væpnet konflikt. Statlige virksomheter har derfor behov for funksjonelle og kostnadseffektive skytjenester som gir tilstrekkelig grad av nasjonal kontroll over beskyttelsesverdige data og systemer. Det vil imøtekomme behovet for å sikre beskyttelsesverdige data og systemer i hele krisespekteret, og legge til rette for å utnytte mulighetene som ligger i moderne skytjenester.

Statlige virksomheter har av denne grunn behov for tilgang på funksjonelle og kostnadseffektive skytjenester som gir tilstrekkelig grad av nasjonal kontroll over beskyttelsesverdige data og systemer. For å imøtekomme disse behovene er det identifisert flere mulige løsninger som vil gi høyere grad av nasjonal kontroll over beskyttelsesverdige data og systemer. Det er i alternativanalysen vurdert fem alternative konsepter:

K1: Reguleringskonseptet innebærer å klargjøre og eventuelt styrke dagens regelverk i tillegg til at det etableres eller styrkes en statlig tilsynsmyndighet og rådgivningstjeneste.

K2: Statlig skymegler - en liten sentralenhet opererer som en skymegler som kobler enkeltvirksomheter med flere parallelle statlige tjenesteleverandører.

K3: Lukket statlig sky - staten etablerer enten en ny eller gir ansvar til en eksisterende statlig virksomhet, som eier og drifter skyløsningen på norsk jord underlagt norsk jurisdiksjon.

K4: Lukket kommersiell sky - staten inngår en avtale med et fåtall kommersielle aktører som eier, leverer, videreutvikler og drifter skyløsningene.

K7: Kombinasjonskonseptet - kombinerer en statlig eid og driftet lukket skyløsning (K3) og en lukket kommersiell sky (K4). Beskyttelsesverdige data som må sikres med høy grad av nasjonal kontroll, lagres og behandles i den statlige skyen, mens andre beskyttelsesverdige data kan virksomhetene velge å lagre og behandle i den kommersielle skyen med middels grad av nasjonal kontroll.

Tabellen nedenfor oppsummerer de samfunnsøkonomiske virkningene av konseptene.

Tabell -0-1 - Oppsummering av prissatte og ikke-prissatte virkninger relativt til nullalternativet med rangering i parentes. De ikke-prissatte virkningene vurderes på en fem-delt skala (svært liten, liten, middels, stor, svært stor)

Virkning	Konsept 1	Konsept 2	Konsept 3	Konsept 4	Konsept 7
Prissatte virkninger, MNOK i 2022-kroner					
Ikke-prissatte virkninger					
Virkninger av økt nasjonal kontroll	Liten positiv virkning	Middels positiv virkning	Svært stor positiv virkning	Middels positiv virkning	Stor positiv virkning
Virkninger av endret funksjonalitet / fleksibilitet	Middels negativ virkning	Liten negativ virkning	Liten negativ virkning	Svært liten negativ virkning	Svært liten negativ virkning
Samlet rangering etter prissatte og ikke-prissatte virkninger	(4)	(5)	(2)	(2)	(1)

Den samfunnsøkonomiske analysen viser at kostnadene som følger av økt grad av nasjonal kontroll er relativt store. Manglende nasjonal kontroll kan imidlertid medføre betydelige konsekvenser, særlig i en krise eller væpnet konflikt. Verdien av økt nasjonal kontroll og forskjeller i funksjonalitet og fleksibilitet er svært vanskelig å anslå, og det er derfor krevende å vurdere den samlede samfunnsøkonomiske lønnsomheten av de ulike konseptene.

Hvilket konsept som bør gjennomføres blir derfor i all hovedsak et spørsmål om hvilken risiko for tap eller forringelse av sentrale tjenester man er villig til å akseptere. Med manglende grunnlag for å vurdere hvor stor denne risikoen er, er dette mer et spørsmål om politiske prioriteringer enn samfunnsøkonomifaglige vurderinger.

Ut ifra en totalvurdering anbefaler utredningen at kombinasjonskonseptet K7 tas med til videre planlegging. Selv om det ikke er tilstrekkelig grunnlag til å fastslå at dette alternativet er det mest samfunnsøkonomisk lønnsomme, gir konsept 7 tilstrekkelig fleksibilitet til å finne en hensiktsmessig balansegang mellom nasjonale sikkerhetsinteresser og behovet for kostnadseffektive og funksjonelle løsninger. Hvilke krav til nasjonal kontroll som stilles til de ulike delløsningene og hvilke data og systemer som bør plasseres hvor, kan vurderes nærmere når mer detaljert informasjon om de relevante dataene og systemene foreligger.

Sammendrag

Staten forvalter betydelige mengder ugraderte data og systemer som krever særskilt beskyttelse. Dette er data og systemer som er avgjørende for at staten skal kunne levere nødvendige tjenester av tilstrekkelig kvalitet i både fred, krise og krig, samt i et eventuelt gjenopprettingsscenario. Det er derfor sentralt at disse dataene og systemenes konfidensialitet, tilgjengelighet og integritet er tilstrekkelig ivaretatt og under nasjonal kontroll. Dette kan være særskilt utfordrende ved bruk av skytjenester.

Bruk av skytjenester er en tydelig trend på tvers av både virksomheter og sektorer. Ønske om bedre kostnadskontroll, mer fleksibilitet og tilgang til moderne teknologi er viktige årsaker til at statlige virksomheter velger skyløsninger når de skal utvikle eller anskaffe digitale tjenester. Selv om det er mange gode grunner til å benytte skytjenester, er det viktig at virksomhetene er bevisste på hvilke tjenester som settes ut og hvem som får ansvar for å levere disse.

Justis- og beredskapsdepartementet (JD) har derfor gitt Nasjonal sikkerhetsmyndighet (NSM) i oppdrag å gjennomføre en konseptvalgutredning (KVU) for etablering av en nasjonal skytjeneste for ugradert, skjermingsverdig informasjon og andre beskyttelsesverdige data.

KVUen skal vurdere og rangere statsforvaltningens reelle behov for en nasjonal skytjeneste for behandling og lagring av skjermingsverdig, ugradert informasjon. Det skal også vurderes om det er annen beskyttelsesverdig informasjon som bør inngå i en nasjonal skytjeneste. Virksomheter som allerede er omfattet av FDs tonivå-plattform¹, eller hvor det er besluttet at de skal benytte plattformen, skal ikke være en del av denne utredningen.

Mengden data som produseres og benyttes forventes å øke kraftig, hvilket forsterker behovet for effektive og skalerbare løsninger. For en stadig mer digitalisert statsforvaltning, innebærer det at konsekvensene av digitale angrep for statens evne til å levere samfunnskritiske tjenester, blir mer omfattende. Dette øker igjen behovet for økt nasjonal kontroll over lagring og behandling av beskyttelsesverdige data og systemer.

Problem

Bruk av skytjenester gir tilgang på moderne teknologi med stor fleksibilitet som det er vanskelig å oppnå med IKT-løsninger utviklet og driftet på egen plattform. Med bruk av kommersielle skytjenester gir imidlertid virksomhetene fra seg en del av kontrollen over infrastruktur, systemer og data som lagres og behandles i skyen. Det svekker statens evne til å sikre dataenes konfidensialitet, integritet og tilgjengelighet. Virksomheter i statsforvaltningen forvalter betydelige mengder data og systemer som har et ekstra behov for beskyttelse. Det kan dreie seg om å beskytte personopplysninger, helsedata, finansielle data, ulike registre eller informasjon om infrastruktur og transportsystemer i Norge. Manglende kontroll over slike data og systemer kan svekke statens evne til å sikre leveranser av helt sentrale offentlige tjenester i fred, krise og væpnet konflikt.

¹ Se kapittel 1.3 i hoveddokumentet og Bilag B i Vedlegg A for en omtale av dette prosjektet.

Alternativet til å ta i bruk skytjenester er å anskaffe og drifte nødvendige systemer og infrastruktur i egen regi. Dette gir stor kontroll, men gjør det vanskeligere å utnytte stordriftsfordeler som skyløsninger kan tilby knyttet til infrastruktur, driftsressurser og store kompetansemiljøer. Å få til gode løsninger i egen regi kan kreve vesentlige investeringer og tilstrekkelig kompetanse og ressurser til å drifte og oppdatere systemer for sikre nødvendig tjenestekvalitet. Dette kan være krevende, særlig for mindre virksomheter. Over tid kan det føre til økte kostnader, mindre effektiv tjenesteproduksjon og i verste fall lavere kvalitet på statlige tjenester.

Det grunnleggende problemet vi har avdekket i denne utredningen er:

«Manglende kontroll over beskyttelsesverdige data og systemer i sky»

Figuren nedenfor gir en forenklet framstilling av årsak-virkningskjedene i problemstillingen.



Figur 0-1 – Illustrasjon av sentrale årsak-virkningsmekanismer

Kombinasjoner av sky og løsninger på egen plattform, eller ulike varianter av lukkede og hybride skyløsninger, kan gi god funksjonalitet uten tap av kontroll. Anskaffelser av skytjenester kan imidlertid være komplisert. Det kan kreve betydelig kompetanse og innkjøpsmakt å forhandle fram avtaler som sikrer tilstrekkelig grad av kontroll til en forsvarlig kostnad. Det kan også være krevende for den enkelte virksomhet å vurdere hvilke konsekvenser et eventuelt tap av tilgjengelighet og konfidensialitet for egne data vil kunne ha for andre virksomheter og samfunnet for øvrig. I mange tilfeller er ulike offentlige virksomheters tjenester tett sammenvevd med, og avhengige av andre virksomheters data, systemer og tjenester. Redusert tilgang til og integritet for en virksomhets data og systemer, kan derfor få betydelige konsekvenser utenfor den virksomheten som er direkte berørt. Videre vil totalen av data og systemer utenfor norsk kontroll påvirke hvor sårbare vi er for trusler og sanksjoner i en krise eller krig.

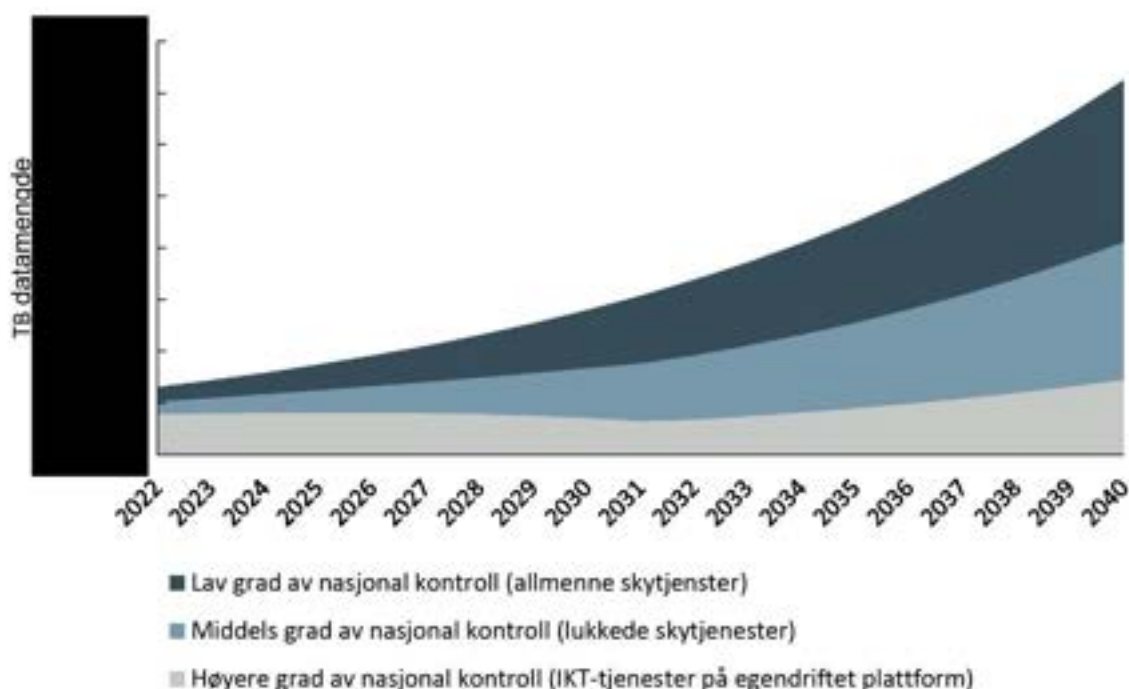
Det grunnleggende dilemmaet mellom behovet for å sikre tilstrekkelig kontroll over data og systemer, og samtidig kunne utnytte de fordelene skyteknologi gir, er derfor et nasjonalt problem og ikke bare en utfordring for den enkelte virksomhet.

Problemene vil trolig øke over tid. Selv om mange statlige virksomheter allerede har tatt i bruk skyløsninger, er det fortsatt en betydelig andel virksomheter som har systemer med stor teknisk gjeld, og med stort behov for å videreutvikle og fornye sine IKT-løsninger.

Mengden data som produseres og konsumeres forventes å øke kraftig, hvilket forsterker behovet for effektive og skalerbare løsninger.

Behov

Norge har behov for funksjonelle og kostnadseffektive skytjenester som gir tilstrekkelig grad av nasjonal kontroll over beskyttelsesverdige data og systemer, samtidig som det legges til rette for videre digitalisering og effektivisering av statlig sektor. Etterspørselen etter skytjenester er stor, både fra kommersielle og offentlige virksomheter. Det er også stor etterspørsel etter å kunne bruke skytjenester til lagring og behandling av beskyttelsesverdige data og systemer. Dersom dagens utviklingstrender fortsetter, vil om lag 80 prosent av beskyttelsesverdige data og systemer ligge i skybaserte løsninger fra 2032 og ut analyseperioden. Denne forventede utviklingen er vist i figuren nedenfor.



Figur 0-2: Forventet framtidig utvikling i hvor beskyttelsesverdige data og systemer lagres og behandles fram mot 2040. Kilde: Utredningens spørreundersøkelse (NSM 2022), Kartlegging av drift og forvaltning av IKT-løsninger i statlige virksomheter (A-2 Norge 2021) og DataSphere and StorageSphere Report (IDC 2022)

Utviklingen av flere, bedre og mer digitaliserte offentlige tjenester øker statsforvaltningens etterspørsel etter mer kapasitet, ytelse og tjenesteutvikling. Siden omfanget av informasjon som behandles, lagres og deles i statsforvaltningen blir stadig større, øker virksomhetenes behov for fleksible og kostnadseffektive IKT-løsninger med høy grad av funksjonalitet - noe som kan oppnås med bruk av skytjenester.

Uten tilstrekkelige risiko- og konsekvensvurderinger vil imidlertid den nasjonale kontrollen over disse dataene og systemene bli kraftig svekket. Det kan få store konsekvenser, da enkelte tjenester som behandler beskyttelsesverdige data er så kritiske for samfunnet at de må være tilgjengelige og inneholde korrekt informasjon i fred, krise og væpnet konflikt, samt ved et gjenopprettings-scenario. Dersom disse tjenestene faller bort eller innholdet i dataene er endret uten at det er autorisert, vil det påvirke statens evne til å levere sentrale tjenester. Det er derfor et behov for å sikre de beskyttelsesverdige dataene og systemene i hele

krisespekteret. For å sikre beskyttelsesverdige data i statsforvaltningen, må staten ha kontroll både over hvor data lagres og behandles, og over hvem som har tilgang til slike data.

De statlige virksomhetene står derfor overfor et vanskelig dilemma der de må veie behovet for å kjøpe inn tjenester med høy funksjonalitet, til lavest mulig kostnad, mot behovet for nasjonal kontroll over beskyttelsesverdige data. Dette dilemmaet vil ikke uten videre løses av seg selv. Hver enkelt virksomhet har selv ansvar for å vurdere hva som er en forsvarlig håndtering av deres data – de har imidlertid ikke forutsetninger for å vurdere den totale risikoen ved å gi fra seg kontrollen på et mer strategisk nivå. Videre har de kommersielle leverandørene små incentiver til å levere tjenester det ikke er etterspørsel etter. Fragmenterte innkjøp, lav bevissthet hos innkjøper og høyt kostnadspress blant statlige virksomheter, vil derfor kunne føre til at mye av de beskyttelsesverdige dataene flyttes ut i skyløsninger utenfor norsk kontroll. Det vil øke risikoen for bortfall og forringelse av sentrale offentlige tjenester i fred, krise og krig.

Mål

Basert på identifiserte problemer og behov har vi formulert følgende samfunns mål:

«Sikker og effektiv lagring og behandling av beskyttelsesverdige data og systemer i statlige virksomheter»

Sikkerhetsaspektet i samfunns målet er rettet inn mot å ivareta behovet for nasjonal kontroll og et tilstrekkelig digitalt sikkerhetsnivå for å sikre samfunnskritiske verdier og funksjoner i hele krisespekteret.

Å sørge for at statsforvaltningen har tilgang til effektive skyløsninger vil fremme den videre digitaliseringen av statlig sektor og bygge opp under deres evne til å levere relevante tjenester av høy kvalitet til en tilfredsstillende kostnad.

Effektmålene er knyttet opp til de forventede nyttevirkningene av tiltaket og gjenspeiles i de samfunnsøkonomiske virkningene i alternativanalysen. For å oppfylle samfunns målet må følgende effektmål være oppfylt:

Tabell 0-1 Oversikt over effektmål

Effektmål
E1: Sikkerhet: Tilgjengelighet, integritet og konfidensialitet ivaretas for beskyttelsesverdige data og systemer i fred, krise og krig.
E2: Effektivitet: Statsforvaltningen får tilgang til kostnadseffektive skytjenester med relevant funksjonalitet og tjenestenivå.
E3: Fleksibilitet: Statsforvaltningens skytjenester kan skaleres og tilpasses virksomhetenes kapasitets-, ytelses- og tjenestebehov og gi muligheter for utnyttelse av ny teknologi.

Effektmålene spesifisert ovenfor er ikke binære, men kan oppnås i ulik grad. Det vil si at det ikke er satt konkrete terskelverdier for nødvendig måloppnåelse konseptene må oppfylle.

Det er heller ikke gjort en prioritering mellom de ulike effektmålene. Hva som er den mest hensiktsmessige graden av måloppnåelse av hvert effektmål vil styres av hva som gir høyest oppnåelse av samfunnsmålet, vurdert ut ifra konseptenes samfunnsøkonomiske lønnsomhet. Det innebærer en avveining mellom behovet for kontroll/sikkerhet (E1), og behovet for funksjonalitet, kostnadseffektivitet (E2) og fleksibilitet (E3). I denne avveiningen kan det ligge mulige målkonflikter. Høy grad av nasjonal kontroll og sikkerhet kan for eksempel gå utover målsetningene om effektivitet og fleksibilitet, og vise versa. Hvilke av disse hensynene som bør prioriteres høyest vil være avhengig av hvilke virkninger ulike grader av måloppnåelse gir.

Rammebetingelser

Siden det ikke er satt eksplisitte krav eller terskelverdier for nødvendig måloppnåelse konseptene må oppfylle, følger det heller ikke konkrete rammebetingelser som kan utledes direkte fra de strategiske målene. Det er imidlertid en rekke lover og regler som setter rammer for hvilke konsepter som er relevante og hvilke egenskaper de kan ha. Flere av disse rammebetingelsene er knyttet opp mot nasjonal kontroll og har derfor en klar tilknytning til samfunnsmålet og effektmål E1.

Skytjenesteleverandører eller datasentre er per i dag ikke underlagt egne lovkrav i Norge.² Det er i hovedsak vanlige krav til forvaltningens virksomhet, sektorlovgivning, generelle krav til personvern og informasjonssikkerhet og kundens kontraktsfestede krav som regulerer tjenestene og aktørene.

Det eksisterer en rekke regelverk som vil kunne påvirke etablering og drift av en nasjonal skytjeneste, blant annet knyttet til offentlige anskaffelser, personvern og krav til statsforvaltningens virksomhet. Flere lover inneholder også krav til for eksempel sikkerhet, beredskap, konfidensialitet, integritet og tilgjengelighet som har implikasjoner for bruk og utforming av skytjenester.

De viktigste rammebetingelsene er:

- Rammebetingelser knyttet til leverandører og behandling av data
 - o Begrensninger for bruk og valg av leverandører
 - o Begrensninger for hvor data lagres og behandles
- Rammebetingelser knyttet til regelverk om offentlige anskaffelser og statsstøtte

Disse rammebetingelsene er hensyntatt og vurdert for hvert enkelt konsept i mulighetsstudien.

Konseptuelle muligheter

For å identifisere et tilstrekkelig bredt spekter av relevante alternativer, har vi identifisert konsepter med forskjellige ambisjonsnivå og med ulike vektning av forskjellige behov. Konseptene vi har vurdert har derfor forskjellige egenskaper og utløser ulike virkninger. Hvilket ambisjonsnivå det er hensiktsmessig å legge til grunn vil påvirkes av avveiningen

² Kommunal- og distriktsdepartementet har sendt på høring forslag til regulering av datasentre i ny ekomlov og -forskrift.

mellom kostnader, effektivitetsgevinster og verdien av nasjonal kontroll. Vi har derfor utformet konsepter med ulik oppnåelse av de forskjellige effektmålene, slik at vi legger best mulig til rette for en nærmere vurdering av innretning og ambisjonsnivå i alternativanalysen. På den måten har vi fått frem konsepter som er tilstrekkelig forskjellige, og som utfordrer potensielle målkonflikter, samtidig som de alle er rettet inn mot å løse de samme problemene.

Følgende konsepter ble tatt med til videre utforming og detaljering i alternativanalysen:

K0: Nullalternativet innebærer en videreføring av dagens situasjon der virksomhetene står fritt til å selv vurdere hvilke skyløsninger de ønsker å benytte. Virksomhetene velger hvilke tjenester de skal etablere som skytjenester og hva slags leveransemodell som skal benyttes. Konseptet viderefører virksomhetenes opplevde usikkerhet om bruk av skytjenester og innebærer en mangelfull nasjonal kontroll av beskyttelsesverdige data og systemer.

K1: Reguleringskonseptet innebærer å samle, klargjøre og eventuelt styrke dagens regelverk. Det etableres eller styrkes en statlig tilsynsmyndighet og rådgivningstjeneste, med mulighet for en sertifiseringsordning. Konseptet vil redusere uklarheter knyttet til hvor beskyttelsesverdige data kan lagres og hvem som kan drifte løsninger som inneholder slike data. Det legges til rette for at det vil bli enklere for virksomhetene å planlegge og beslutte overgangen til skyløsninger. Det forventes at dette vil gi en bedre nasjonal kontroll enn i dag.

K2: Statlig skymegler medfører at det tilbys flere parallelle statlige skytjenester levert av et fåtall eksisterende statlig eide tjenesteleverandører, administrert av en liten sentralenhet som inngår rammeavtaler med disse. Tjenesteleverandørene må parallelt tilpasse og utvikle skytjenester som både kan overlappe med og utfylle hverandre. Sentralenheten vil operere som en skymegler mellom virksomhetene og tjenesteleverandørene.

K3: Lukket statlig sky innebærer at staten etablerer en ny eller gir ansvar til en eksisterende virksomhet, som eier og drifter skyløsningen på norsk jord underlagt norsk jurisdiksjon. Denne virksomheten bygger opp en egen drifts- og forvaltningsorganisasjon som anskaffer, drifter, forvalter og eier egen maskin- og programvare, men benytter nødvendig eksisterende datasenterkapasitet. Konseptet innebærer sterk statlig styring og høy grad av nasjonal kontroll.

K4: Lukket kommersiell sky innebærer at staten inngår en avtale med et fåtall kommersielle aktører som eier, leverer, videreutvikler og drifter skyløsningene. Det stilles spesifikke krav knyttet til nasjonal kontroll av skytjenestene som leverandøren(e) må tilfredsstille og gi garantier for. Den statlige enheten som får ansvar for avtalen(e), bygger opp en organisasjon for å styre og videreutvikle skytjenestene.

K7: Kombinasjonskonseptet innebærer at staten både har en virksomhet som eier og drifter en skyløsning på norsk jord underlagt norsk jurisdiksjon (som K3), og samtidig inngår en avtale med en eller et fåtall kommersielle aktører som eier, leverer, videreutvikler og drifter skyløsningene (som K4). Beskyttelsesverdige data med behov for høy grad av nasjonal kontroll, lagres og behandles i en lukket statlig sky, mens andre beskyttelsesverdige data kan virksomhetene velge å lagre og behandle i en lukket kommersiell sky med middels grad av nasjonal kontroll, ut fra en konkret vurdering av deres behov for sikkerhet og funksjonalitet. Kombinasjonen innebærer at man, avhengig av type data som håndteres, både får et høyt nivå av nasjonal kontroll og en høy funksjonalitet.

Alle konseptene er dimensjonert likt med hensyn til hvilken mengde beskyttelsesverdige data de skal ha kapasitet til å håndtere. Det er stor usikkerhet rundt mengden beskyttelsesverdige data som bør ligge i en nasjonal skyløsning, og dimensjoneringen med hensyn til datavolumer har liten betydning for hvilket konsept som er det mest hensiktsmessige. Alle konseptene som er tatt videre til alternativanalysen er utformet på en måte som legger til rette for at omfanget kan justeres vesentlig på et senere tidspunkt, uten at det er behov for å endre på den konseptuelle løsningen.

Alternativanalyse

I alternativanalysen er det gitt en samlet vurdering av de samfunnsøkonomiske kostnads- og nyttevirkningene som følger av konseptene. Resultatene som kommer frem i tabellen under oppsummerer de prissatte og de ikke-prissatte virkningene for de fem konseptene (intern rangering for hver virkning er oppgitt i parentes), samt usikkerheten.

Tabell 0-2 - Oppsummering av prissatte og ikke-prissatte virkninger relativt til nullalternativet med rangering i parentes. De ikke-prissatte virkningene vurderes på en fem-delt skala (svært liten, liten, middels, stor, svært stor)

Virkning	Konsept 1	Konsept 2	Konsept 3	Konsept 4	Konsept 7
Prissatte virkninger, MNOK i 2022-kroner, ekskl. mva.					
Ikke-prissatte virkninger					
Virkninger av økt nasjonal kontroll	Liten positiv virkning (5)	Middels positiv virkning (3)	Svært stor positiv virkning (1)	Middels positiv virkning (3)	Stor positiv virkning (2)
Virkninger av endret funksjonalitet / fleksibilitet	Middels negativ virkning (5)	Liten negativ virkning (3)	Liten negativ virkning (3)	Svært liten negativ virkning (1)	Svært liten negativ virkning (2)
Usikkerhet knyttet til ikke-prissatte virkninger					
Risiko knyttet til etterlevelse av krav	(5)	(4)	(1)	(3)	(2)
Gjennomføringsrisiko knyttet til organisering	(1)	(5)	(2)	(2)	(2)

Virkning	Konsept 1	Konsept 2	Konsept 3	Konsept 4	Konsept 7
<i>Mulighet knyttet til større overgang til sky</i>	(3)	(3)	(3)	(1)	(2)
Samlet rangering etter prissatte og ikke-prissatte virkninger	(4)	(5)	(2)	(2)	(1)

Samlet vurdering og anbefaling

Den samfunnsøkonomiske analysen viser at kostnadene som følger av økt grad av nasjonal kontroll for hele statsforvaltningen er relativt store. Manglende nasjonal kontroll kan imidlertid medføre store konsekvenser, særlig i en krise eller væpnet konflikt. Verdien av økt nasjonal kontroll og forskjeller i funksjonalitet og fleksibilitet er svært vanskelig å anslå og det er derfor krevende å vurdere den samlede samfunnsøkonomiske lønnsomheten av de ulike konseptene. Basert på prissatte virkninger alene er det konsept 4 som medfører de laveste samfunnsøkonomiske kostnadene utover nullalternativet. For de ikke-prissatte virkningene av nasjonal kontroll er det konsept 3 som kommer best ut. For virkningene knyttet til endret funksjonalitet og fleksibilitet er det konsept 4 som er nærmest nullalternativet.

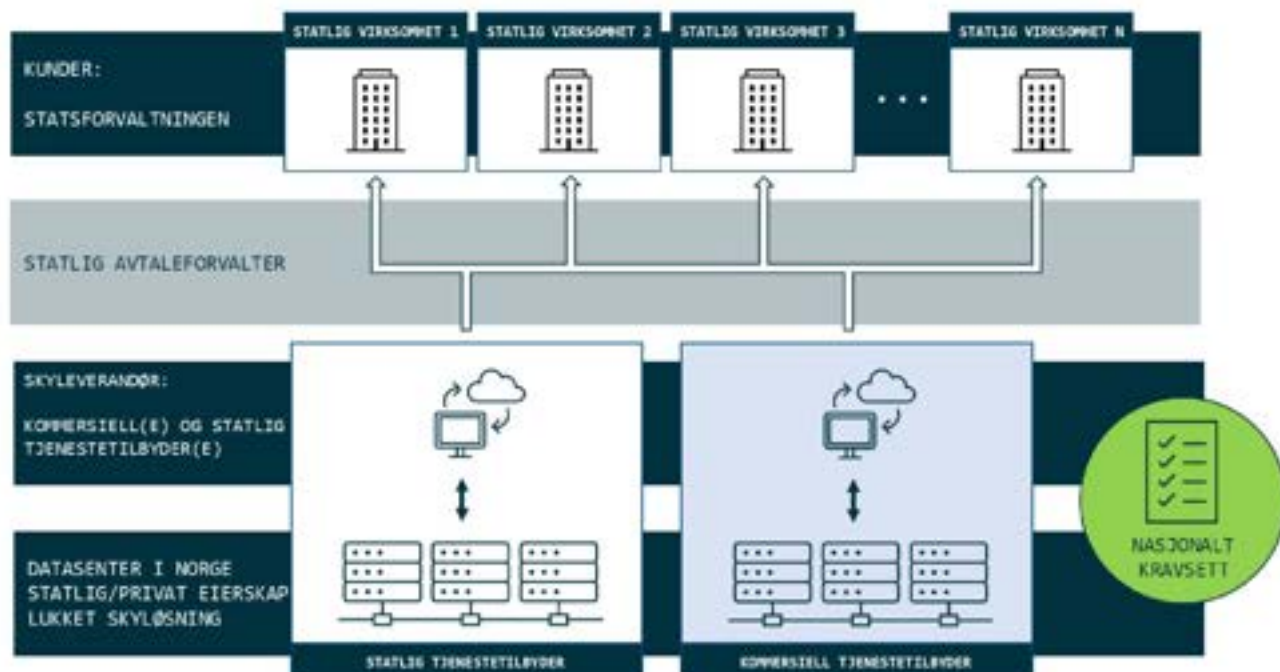
Hvilket konsept som bør gjennomføres blir derfor i all hovedsak et spørsmål om hvilken risiko for tap eller forringelse av sentrale tjenester man er villig til å akseptere. Med manglende grunnlag for å vurdere hvor stor denne risikoen er, er dette mer et spørsmål om politiske prioriteringer enn samfunnsøkonomifaglige vurderinger. Dersom hensynet til kostnader veier tyngre enn hensynet til nasjonal kontroll bør nullalternativet videreføres. Hvis hensynet til nasjonal kontroll vektlegges tyngst, bør konsept 3 velges. Aksepterer man noe høyere risiko (ved middels grad av nasjonal kontroll) i bytte mot reduserte kostnader og økt funksjonalitet, framstår konsept 4 som det mest egnede konseptet. Konsept 3 og konsept 4 er imidlertid ikke nødvendigvis å anse som rene alternativer til hverandre. De kan også kombineres, slik det er gjort i kombinasjonskonseptet K7, som er det konseptet som gir størst fleksibilitet til å balansere hensynene til nasjonal kontroll, kostnadseffektivitet og funksjonalitet.

En slik kombinasjonsløsning vil kunne legge til rette for at graden av nasjonal kontroll er tilpasset behovet for beskyttelse. Det kan gi en løsning som sikrer nasjonale sikkerhetsinteresser samtidig som kostnadene begrenses og behovet for funksjonalitet ivaretas.

Som en minimumstilnærming anbefaler vi at det gjøres et arbeid med å samle og klargjøre regelverket som må følges ved bruk av skytjenester i staten allerede i dag. Det vil gjøre det enklere for statlige virksomheter å velge riktige og trygge løsninger. Dette vil imidlertid ikke være tilstrekkelig til å sikre nasjonal kontroll over sentrale beskyttelsesverdige data og systemer.

Ut ifra en totalvurdering anbefaler utredningen derfor at kombinasjonskonseptet K7 tas med til videre planlegging. Selv om det ikke er tilstrekkelig grunnlag per nå til å fastslå at dette alternativet er det mest samfunnsøkonomisk lønnsomme, gir konsept 7 tilstrekkelig

fleksibilitet til å finne en hensiktsmessig balansegang mellom nasjonale sikkerhetsinteresser og behovet for kostnadseffektive og funksjonelle løsninger. Hvilke krav til nasjonal kontroll som stilles til de ulike deløsningene og hvilke data og systemer som bør plasseres hvor, kan vurderes nærmere når mer detaljert informasjon om de relevante dataene og systemene foreligger. Figuren under illustrerer K7.



Figur 0-3 Illustrasjon av kombinasjonskonseptet K7

Vi anbefaler at følgende tiltak gjennomføres før og under forprosjektet:

- Vurdere hvor eierskapet til det videre arbeid med tiltaket bør plasseres, og at det bør ivareta at det er ulike krav til eierrollen i forbindelse med planlegging og forberedelse frem til endelig beslutning om iverksettelse, og gjennomføringsfasen.
- Legge en plan for det videre arbeidet med tydeliggjøring av dagens regelverk knyttet til bruk av skyløsninger i statsforvaltningen.
- Videreføre arbeidet med å estimere hvilke datavolum og omfang man i startfasen skal dimensjonere skyløsningene for, basert på virksomhetenes oversikt over egne skjermingsverdige og øvrige beskyttelsesverdige data.
- Videreføre arbeidet med godkjenning av skjermingsverdige systemer i henhold til kravene i sikkerhetsloven.
- For å sikre en komplett innføring i hele statsforvaltningen som styrker kontrollen over beskyttelsesverdige data, bør det være en stor grad av forpliktelse om deltakelse fra virksomhetene før et såpass stort tiltak som en nasjonal sky kan igangsettes. Vi anbefaler at det inngås en bindende avtale med virksomhetene i forprosjektfasen, når finansieringsmodell og øvrige forutsetninger er på plass.
- Gjennomføre tiltaket organisert som et program med underliggende prosjekter hvor det utarbeides et sentralt styringsdokument (SSD) både for programmet og prosjektene, da dette vil være ulike styringsobjekter hvor det stilles ulike krav til gjennomføringen.

- Følge opp nasjonale og internasjonale prosjekter som kan ha innvirkning på realiseringen av en nasjonal skyløsning for å sikre nødvendig dialog og iverksettelse av relevante tiltak basert på dette.
- Gjennomføre en markedsdialog i forbindelse med utarbeidelse av konkurransegrunnlaget for blant annet å evaluere om kravene som stilles harmonerer med utviklingstrender i leverandørmarkedet.

1 Om utredningen

Staten forvalter betydelig mengder ugraderte data og systemer som krever særskilt beskyttelse. Dette er data og systemer som er avgjørende for at staten skal kunne levere nødvendige tjenester av tilstrekkelig kvalitet i både fred, krise og krig, og i et eventuelt gjenopprettings-scenario. Det er derfor sentralt at disse dataene og systemenes konfidensialitet, tilgjengelighet og integritet er tilstrekkelig ivaretatt og under nasjonal kontroll. Dette kan være særskilt utfordrende ved bruk av enkelte skytjenester.

Bruk av skytjenester er en tydelig trend på tvers av både virksomheter og sektorer. Bedre kostnadskontroll, mer fleksibilitet og tilgang til moderne teknologi trekkes ofte fram som viktige årsaker til at statlige virksomheter velger skyløsninger når de skal utvikle digitale tjenester og IKT-infrastruktur. Selv om det er mange gode grunner til å benytte skytjenester, er det viktig at virksomhetene er bevisste på hvilke tjenester som settes ut og til hvem. I 2020 løftet NSM fram flere problemstillinger rundt bruk av sky i *Helhetlig digitalt risikobilde 2020*. I rapporten uttrykte NSM bekymring for den samlede nasjonale avhengigheten til utenlandske skytjenesteleverandører og konsekvensene dette kan medføre i de ulike delene av krisespekteret. NSM er også bekymret for at samfunnskritiske IKT-funksjoner tjenesteutsettes uten tilstrekkelige risikovurderinger og sikringstiltak, og at data flyttes til utlandet uten tilstrekkelige sikkerhetsfaglige vurderinger. Jurisdiksjon, ressursprioritering, tilgjengelighet og sikkerhetspolitikk må tas hensyn til i arbeidet med den samlede nasjonale beredskapen.

Justis- og beredskapsdepartementet (JD) har i denne sammenhengen gitt Nasjonal sikkerhetsmyndighet (NSM) i oppdrag å gjennomføre en konseptvalgutredning (Kvu) for etablering av en nasjonal skytjeneste for ugradert, skjermingsverdig informasjon og andre beskyttelsesverdige ugraderte data.

1.1 Bakgrunn og mandat

Siden 2016 har NSM og Digitaliseringsdirektoratet (Digdir) vurdert ulike problemstillinger knyttet til etablering av en sikker skytjeneste. Dette arbeidet danner mye av grunnlaget for igangsettingen og mandatet for denne utredningen.

1.1.1 Tidligere utredninger

I 2016 ble «Nasjonal strategi for bruk av skytjenester» lansert. I den forbindelse fikk Justisdepartementet (JD), i samråd med Kommunal- og moderniseringsdepartementet (KMD) og Forsvarsdepartementet (FD), i oppdrag å «igangsette et arbeid for å vurdere etablering av en statlig driftet skytjeneste med høyt sikkerhetsnivå, slik at også sentrale myndigheter med særskilte sikkerhetsbehov kan utnytte mulighetene til effektivisering som skytjenester gir». Dette oppdraget ble svart ut i rapporten *Sikker sky* i 2016 der NSM vurderte handlingsrom for og innretningen av en sikker skytjeneste på et overordnet nivå. Basert på usikkerheter rundt hva som mentes med «sky» samt hvilke tjenester, funksjoner og applikasjoner som skulle inngå i skytjenesten, anbefalte NSM at det ble utført en behovskartlegging.

Arbeidet ble fulgt opp i 2017 med vurderinger av hvilken type informasjon som bør omfattes av en slik løsning, potensielt kundegrunnlag og aktuelle markedsaktører, samt handlingsrom i henhold til anskaffelsesregelverket. Dette arbeidet resulterte i rapporten *Sikker sky fase 2*.

Siden 2019 har NSM også undersøkt mulighetene for å etablere en «cyber-arkitektur» til neste generasjons samfunnskritiske IT-plattformer. I prosjektet *Muligheter for en moderne IT-plattform* er sky en sentral del av det pågående arbeidet.³

Problemstillingene rundt bruk av skytjenester er altså ikke nye og har blitt diskutert og vurdert over flere år. Diskusjonene om bruk av sky fikk igjen plass på den offentlige agendaen etter publiseringen av *Helhetlig digitalt risikobilde 2020* og gjennom Hurdals-plattformen i 2021. Her tydeliggjorde regjeringen sin prioritering av digital beredskap og ønsket om en ny utredning av mulighetene for en statlig skyløsning.

Stortingets vedtak nr. 735/2021⁴: «Stortinget ber regjeringen utrede behov for og etablering av en felles skytjeneste for forvaltningen», la grunnlaget for at JD, i samarbeid med Kommunal- og distriktsdepartementet (KDD) og FD, høsten 2021 igangsatte en KVV for etablering av en nasjonal skytjeneste for ugradert, skjermingsverdig informasjon.⁵

1.1.2 Mandat for konseptvalgutredningen (KVV)

I mandatet spesifiseres det at KVVen skal vurdere og rangere statsforvaltningens reelle behov for en nasjonal skytjeneste for behandling og lagring av ugradert, skjermingsverdig informasjon. Hvilken type informasjon som anses ugradert, skjermingsverdig skal være en del av KVV-arbeidet. Det skal også vurderes om det er annen ugradert, beskyttelsesverdig informasjon som bør inngå i en nasjonal skytjeneste. Virksomheter som allerede er omfattet av FDs tonivå-plattform⁶, eller som er besluttet at skal benytte plattformen, omfattes ikke av denne utredningen.

Utredningen skal vurdere konseptuelle alternativer for hvordan ugradert, skjermingsverdig informasjon bør behandles og lagres gjennom en nasjonal skytjeneste. Det skal legges til grunn ulike ambisjonsnivåer for de konseptuelle alternativene, inkludert en minimumsløsning hvor bare absolutte krav tilfredsstilles. Det skal også vurderes om det finnes eksisterende løsninger eller løsninger som er under planlegging og etablering som vil kunne dekke behovene for en nasjonal skytjeneste. Utredningen skal beskrive, drøfte og foreslå hvem som skal ha hvilke roller i de ulike konseptuelle alternativene. Minst ett av alternativene skal være en skytjeneste som eies og driftes av staten selv, men der kompetanse og innovasjonskraft fra kommersielle benyttes.

De konseptuelle alternativene skal ta utgangspunkt i nasjonal behandling og lagring av ugradert, skjermingsverdig informasjon. Vurderinger av sikkerhetsutfordringer som kan oppstå om en leverandør er underlagt utenlandske staters jurisdiksjon skal være en del av utredningen.

1.2 Avgrensninger

I henhold til mandatet skal denne konseptvalgutredningen vurdere og rangere statsforvaltningens reelle behov for en nasjonal skytjeneste for «behandling og lagring av ugradert, skjermingsverdig informasjon». Det skal også vurderes om det er «annen ugradert, beskyttelsesverdig informasjon» som bør inngå i en nasjonal skytjeneste. I avsnittene

³ Se Vedlegg E Mulighetsstudien

⁴ Kommunal- og Moderniseringsdepartementet. Vedtak nr. 735, 11. mars 2021

⁵ Se kapittel 1.2.1 samt veileder i ugradert, skjermingsverdig informasjon utgitt av NSM.

⁶ Se for kapittel 1.3 samt Vedlegg B for en omtale av dette prosjektet.

nedenfor gis en kort forklaring om hvordan disse avgrensningene er tolket og brukt i utredningsarbeidet.

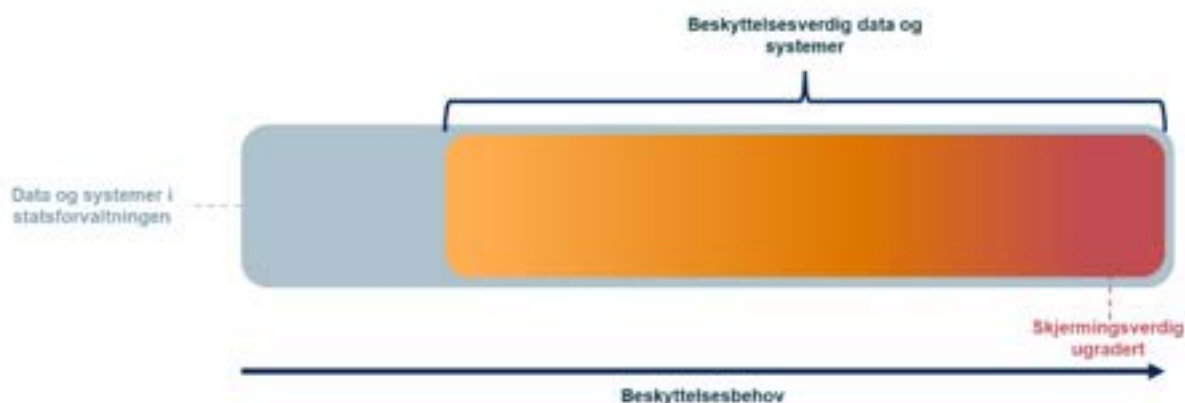
1.2.1 Hvilke data og systemer som omfattes av utredningen

Informasjon betegnes som skjermingsverdig i sikkerhetsloven dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig, jf. sikkerhetsloven § 5-1. Dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen *blir kjent for uvedkommende* (konfidensialitet), skal informasjonen sikkerhetsgraderes, jf. sikkerhetsloven § 5-3. Som spesifisert i mandatet omfatter ikke denne utredningen sikkerhetsgradert informasjon. Dersom kravet til konfidensialitet ikke er til stede, men det kan skade nasjonale sikkerhetsinteresser at informasjonen *går tapt, blir endret eller blir utilgjengelig* (integritet og tilgjengelighet), er informasjonen skjermingsverdig, men skal ikke sikkerhetsgraderes. Denne kategorien betegnes som skjermingsverdig ugradert informasjon. For en nærmere redegjørelse av hva som anses som skjermingsverdig ugradert, vises det til NSMs veileder i skjermingsverdig ugradert informasjon og informasjonssystem.⁷

Mandatet legger også opp til at utredningen skal omfatte *andre* beskyttelsesverdige data. I denne utredningen legger vi til grunn at andre beskyttelsesverdige data er data som skal beskyttes av andre hensyn enn nasjonale sikkerhetsinteresser, for eksempel for å sikre statsforvaltningens evne til å ivareta viktige offentlige tjenester og innfri krav til informasjonssikkerhet. Dette kan blant annet omfatte behandling og beskyttelse av personopplysninger, helseopplysninger og annen informasjon som er unntatt offentlighet eller underlagt taushetsplikt.

Intervjuer med flere virksomheter i statsforvaltningen indikerer at beskyttelsesverdige data vil være av et betydelig større omfang enn det som eventuelt vil kunne klassifiseres som skjermingsverdig ugradert informasjon. I utredningen er begrepet «beskyttelsesverdige data og systemer» benyttet som en *samlebetegnelse* for data og systemer som er skjermingsverdig ugradert informasjon etter sikkerhetsloven, og andre data og systemer som skal beskyttes av andre hensyn. Dette er illustrert i figuren nedenfor.

⁷ Se [Veileder ugradert skjermingsverdig informasjon og informasjonssystem - Nasjonal sikkerhetsmyndighet \(nsm.no\)](#).



Figur 1-1 Beskyttelsesverdige data og systemer og skjermingsverdig ugradert informasjon.

Figuren illustrerer at begrepet beskyttelsesverdige data og systemer favner videre enn sikkerhetslovens virkeområde og at ulike typer data og systemer kan ha behov for forskjellig grader av beskyttelse. Hvor stort dette beskyttelsesbehovet er, vil være avhengig av blant annet hvilke data de ulike systemene behandler. Slike vurderinger krever inngående innsikt i hvert enkelt system og datasett og er en del av virksomhetens forebyggende sikkerhetsarbeid. Ved å ta utgangspunkt i en bred definisjon av beskyttelsesverdige data sikrer vi at utredningen ikke blir for snever i sin tilnærming.

1.2.2 Hva innebærer det at alternativene skal ta utgangspunkt i nasjonal behandling og lagring?

Utredningens forståelse av mandatet er at utredningen må omfatte konsepter som sikrer tilstrekkelig grad av *nasjonal kontroll* over beskyttelsesverdige data og systemer. Dette innebærer konsepter som ivaretar tilstrekkelig kontroll over hvor og hvordan data lagres og behandles, og hvem som har tilgang til slike data og systemer, i hele verdikjeden.

Vi vurderer ikke nasjonal kontroll som et binært spørsmål, men noe som kan oppnås i ulik grad basert på en rekke faktorer. Et krav om nasjonal kontroll må bygge på en avveining mellom hensyn til sikkerhet og kontroll på den ene siden, og andre viktige samfunnshensyn på den andre siden, som hensynet til et fritt og åpent samfunn, behovet for å dra nytte av innovasjon, teknologiutvikling og effektiv ressursutnyttelse, og behovet for å gi forutsigbare rammebetingelser for næringsaktører. Nasjonal kontroll som begrep er nærmere redegjort for i vedlegg J.

Hva som utgjør en hensiktsmessig eller akseptabel grad av nasjonal kontroll kommer an på hvordan ulike hensyn vektlegges, og er et av de mest sentrale spørsmålene denne utredningen forsøker å gi svar på. Dette spørsmålet er derfor nærmere vurdert i vedlegg J om nasjonal kontroll, i mulighetsstudien og i alternativanalysen. Det gir rom for å utrede flere konsepter med ulike innretninger og ambisjonsnivåer. På denne måten åpner også mulighetsrommet for å inkludere en minimumsløsning, slik det blir spesifisert i mandatet.

1.2.3 Hvilke forvaltningsorganer som omfattes av utredningen

Ifølge mandatet skal utredningen omfatte statsforvaltningen, men ikke Statsministerens kontor, departementene, utenriksstasjonene og Departementenes sikkerhets- og serviceorganisasjon (DSS). Dette er begrunnet med at disse virksomhetene allerede

omfattes av Forsvarsdepartementets tonivå-plattform og programmet «Felles IKT-plattform».⁸

Statsforvaltningen inkluderer forvaltningsorganer som direktorater, statlige tilsyn og statsforvaltere, men ikke kommuner og fylkeskommuner. Statsforvaltningen omfatter også forvaltningsorganer med særskilte fullmakter som universiteter og forskningsinstitusjoner, forvaltningsbedrifter, samt statlige fond og statlige finansinstitusjoner.⁹ Mandatet for KVVU-arbeidet legger opp til at det er statsforvaltningens behov for en nasjonal sky som skal vurderes. Samtidig utelukker ikke det at andre målgrupper enn statsforvaltningen kan ta i bruk en eventuell nasjonal sky dersom det viser seg å være hensiktsmessig i fremtiden.

Selv om statseide selskaper ikke regnes som en del av statsforvaltningen, er særlovsselskap som helseforetak inkludert i utredningen i samråd med oppdragsgiver. For øvrig utelukkes ikke statseide selskaper i den utstrekning disse utfører tjenester eller oppgaver på vegne av staten, for eksempel forvaltning av infrastruktur og leveranser av varer og tjenester. Statlig eide selskaper med utelukkende kommersielle formål faller utenfor.

1.3 Grensesnitt mot andre prosjekter

Flere planlagte og pågående prosjekter for etablering av skytjenester har grenseflater mot denne utredningen, både nasjonalt og internasjonalt. Det kan også være eksisterende løsninger som kan ha grenseflater mot en fremtidig etablering av en nasjonal sky. Dette kan være prosjekter som enten kan påvirkes av en eventuell etablering av en nasjonal skytjeneste, eller kan ha en rolle i realiseringen av denne. For eksempel kan det være eksisterende eller planlagte prosjekter som kan imøtekomme deler av de utfordringene en nasjonal sky har som formål å løse. Det vil kunne påvirke behovet for og dimensjoneringen av begge prosjekter. Eksisterende eller planlagte prosjekter kan også være en del av en større, nasjonal skyløsning. Det kan også tenkes at tilsvarende prosjekter i EU kan ha en påvirkning på eller en rolle i en nasjonal skyløsning.

I forbindelse med KVVU-arbeidet har vi kartlagt en rekke ulike prosjekter med mulige grenseflater mot en nasjonal sky. Informasjonen fra kartleggingen brukes i ulike deler av rapporten, men er særlig relevant for mulighetsstudien. Resultatene fra kartleggingen er presentert i Vedlegg A og Vedlegg I til rapporten.

1.4 Metodisk tilnærming til utredningen

En KVVU skal besvare de seks grunnleggende spørsmålene fra utredningsinstruksen. KVVU-arbeidet er gjennomført i tråd med Finansdepartementets kvalitetssikringsordning og Rundskriv R-108/19 av 8. mars 2019¹⁰. Denne utredningen følger en tredelt arbeidsprosess der resultatet fra hver fase ble forankret med Justis- og beredskapsdepartementet. Arbeidsprosessen er illustrert i figuren under.

⁸ Se vedlegg A for nærmere beskrivelse av tilgrensende prosjekter.

⁹ <https://www.regjeringen.no/no/tema/statlig-forvaltning/forvaltningsutvikling/hva-er-statsforvaltningen/id2397949/>

¹⁰ R-108/19: *Statens prosjektmodell - Krav til utredning, planlegging og kvalitetssikring av store investeringsprosjekter i staten*



Figur 1-2 - Arbeidsprosess som følger statens prosjektmodell, med tre delleveranser

1.5 Innhold i KVV-rapporten

Kapittel 2 er prosjektets problembeskrivelse og gir en beskrivelse av den relevante problemstillingens omfang og alvorlighet og forventet utvikling over tid. I Kapittel 3 presenteres behovsanalysen, mens kapittel 4 presenterer de strategiske målene som er angitt for prosjektet. Kapittel 5 redegjør for rammebetingelsene konseptvalget må møte. I kapittel 6 presenteres mulighetsstudien med en beskrivelse av hvilke konsepter som er inkludert og hvilke alternativer som er tatt med videre til alternativanalysen. Kapittel 7 er alternativanalysen og omfatter prosjektets kostnadsusikkerhetsanalyse og den samfunnsøkonomiske analysen. Alternativanalysen avsluttes med en rangering av konseptene, og en anbefaling av konsept på bakgrunn av samfunnsøkonomisk lønnsomhet. I kapittel 8 føringer for forprosjekt, beskrives forutsetninger for en vellykket gjennomføring av prosjektet, med en gjennomføringsstrategi for den etterfølgende forprosjektfasen.

2 Problembeskrivelse

Manglende kontroll over beskyttelsesverdige data og systemer i skyen kan øke faren for tap av tilgang til korrekte data og systemer Norge trenger for å sikre sentrale tjenester i fred, krise og væpnet konflikt. Det gir også reduserte muligheter til å utnytte de fordelene bruk av skytjenester gir. Problemet forventes å øke i tiden som kommer på grunn av virksomhetenes behov for å modernisere sine IKT-systemer og fordi mengden beskyttelsesverdige data forventes å øke.

Statsforvaltningen bruker skytjenester i stadig større omfang for å modernisere og effektivisere den offentlige tjenesteproduksjonen. Bruk av skytjenester gir tilgang på moderne teknologi med stor fleksibilitet som det er vanskelig å oppnå med IKT-løsninger utviklet og driftet på egen plattform. Med bruk av skytjenester gir imidlertid virksomhetene fra seg en del av kontrollen over infrastruktur, systemer og data som lagres og behandles i skyen. Det svekker statens evne til å sikre dataenes konfidensialitet, integritet og tilgjengelighet. Virksomheter i statsforvaltningen forvalter betydelige mengder data og systemer som har et større behov for beskyttelse. Det kan dreie seg om å beskytte personopplysninger, helsedata, finansielle data, eller informasjon om infrastruktur og transportsystemer i Norge. Manglende kontroll over slike data og systemer kan svekke statens evne til å sikre leveranser av helt sentrale offentlige tjenester i fred, krise og krig.

Alternativet til å ta i bruk skytjenester er å anskaffe og drifte nødvendige systemer og infrastruktur selv. Utvikling og drift på egne plattformer gir stor kontroll, men gir ikke de samme mulighetene til å utnytte stordriftsfordeler knyttet til infrastruktur, driftsressurser og store kompetansemiljøer som skyløsninger gir. For mange virksomheter i statsforvaltningen kan det være vanskelig å etablere og vedlikeholde gode løsninger i egenregi fordi det krever vesentlige investeringer, og tilstrekkelig kompetanse og ressurser til å drifte og oppdatere systemer for å opprettholde nødvendig tjenestekvalitet og et forsvarlig sikkerhetsnivå. Det kan føre til økte kostnader, mindre effektiv tjenesteproduksjon og lavere kvalitet på statlige tjenester.

Forenklet sett står statsforvaltningen derfor overfor valget mellom to hovedretninger når de skal videreutvikle sin IKT-infrastruktur med beskyttelsesverdige data og systemer:

- IKT-løsninger utviklet og driftet på egen plattform. Dette kan gjøre det krevende å utnytte den teknologiske utviklingen og ivareta tilstrekkelig informasjonssikkerhet over tid.
- Skyløsninger som gir tilgang på ny teknologi med høy funksjonalitet, men med lavere kontroll over hvor dataene lagres og behandles og hvem som har tilgang til det.

En forenklet årsak-virkningskjede som viser sammenhengene i problembeskrivelsen, er skissert under.



Figur 2-1 – Illustrasjon av sentrale årsak-virkningsmekanismer

Valgene beskrevet ovenfor er en forenkling. Mellom disse to ytterpunktene finnes det flere kombinasjonsmuligheter, med ulike varianter av lukkede og hybride skyløsninger. Det grunnleggende dilemmaet mellom behovet for å sikre tilstrekkelig kontroll over beskyttelsesverdige data og systemer, og samtidig kunne utnytte de fordelene skyteknologi gir, er likevel det samme:

«Manglende kontroll over beskyttelsesverdige data og systemer i sky»

Problemet vil bli mer presserende over tid. Mange virksomheter har allerede tatt steget ut i skyen, mens andre har systemer med betydelig teknisk gjeld og behov for å videreutvikle og fornye sine IKT-løsninger. Mengden data som produseres og behandles på verdensbasis øker kraftig, og det er ingen grunn til å tro at datavolumene i statsforvaltningen følger en annen utvikling¹¹. Når mengden beskyttelsesverdig data som forvaltes digitalt av statsforvaltningen øker, øker også den samlede verdien av det som kan utsettes for digitale angrep. For en stadig mer digitalisert statsforvaltningen, vil konsekvensene av digitale angrep for statens evne til å levere samfunnskritiske tjenester øke. Dette øker igjen behovet for økt nasjonal kontroll over lagring og behandling av beskyttelsesverdige data og systemer.

I delkapitlene under gir vi først en kort beskrivelse av hvilke mengder og type beskyttelsesverdige data og systemer statsforvaltningen besitter i dag, hvorfor de må beskyttes, og mot hva. I tillegg gir vi en beskrivelse av hvordan disse dataene og systemene forvaltes i dag og hvordan dette forventes å utvikle seg framover. Deretter gir vi en nærmere beskrivelse av hvilke konsekvenser manglende kontroll over disse dataene kan føre til, og hvilke ulemper som kan oppstå hvis muligheten til å bruke skytjenester begrenses.

2.1 Beskyttelsesverdige data og systemer i statsforvaltningen

Det er den enkelte virksomhets ansvar å vurdere og ivareta beskyttelsen av de dataene og systemene de besitter. Som et ledd i denne utredningen har NSM derfor gjennomført en kartlegging blant virksomheter i statsforvaltningen for å fremskaffe en overordnet oversikt

¹¹ IDCs DataSphere and StorageSphere reports 2022
<https://www.idc.com/getdoc.jsp?containerId=US49051122> og
<https://www.idc.com/getdoc.jsp?containerId=US49018922>

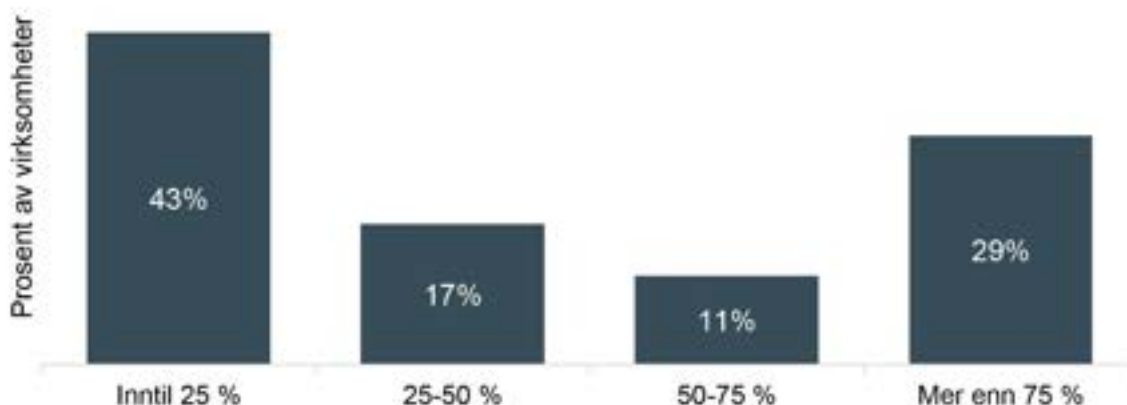
over ulike beskyttelsesverdige data virksomhetene behandler, hvor stort lagringsbehovet for slike data er, og hvilke systemer virksomhetene benytter for å behandle slike data. Virksomhetene ble også bedt om å vurdere hvilke data de anser som mest kritiske for å ivareta egne leveranser gjennom hele krisespekteret. Kartleggingen er avgrenset til ugradert informasjon, da denne utredningen ikke omfatter sikkerhetsgradert informasjon.

2.1.1 Mengde og type beskyttelsesverdige data i statsforvaltningen

Basert på svarene fra undersøkelsen anslår vi at de relevante virksomhetene i statsforvaltningen til sammen lagrer og behandler rundt [REDACTED] data. Det er stor variasjon i hvor store datamengder den enkelte virksomhet behandler. Av de som har svart på utredningens spørreundersøkelse er det virksomheter under [REDACTED]

[REDACTED] som besitter de største datamengdene.

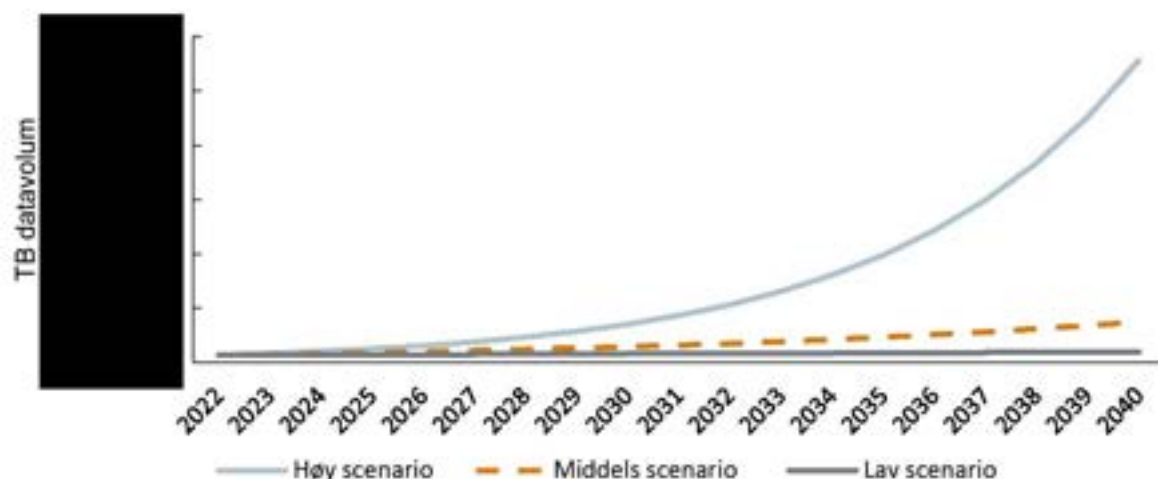
Hvor stor andel av disse dataene som (basert på virksomhetenes egne vurderinger) er å anse som beskyttelsesverdige varierer også mye mellom de ulike virksomhetene. Virksomhetene som forvalter større datavolumer, forvalter i all hovedsak også mer beskyttelsesverdige data. Blant virksomhetene som forvalter mer enn [REDACTED] data, svarte halvparten at mer enn 75 prosent av deres data kan anses som beskyttelsesverdige.



Figur 2-2 – Oppgitt andel beskyttelsesverdige data

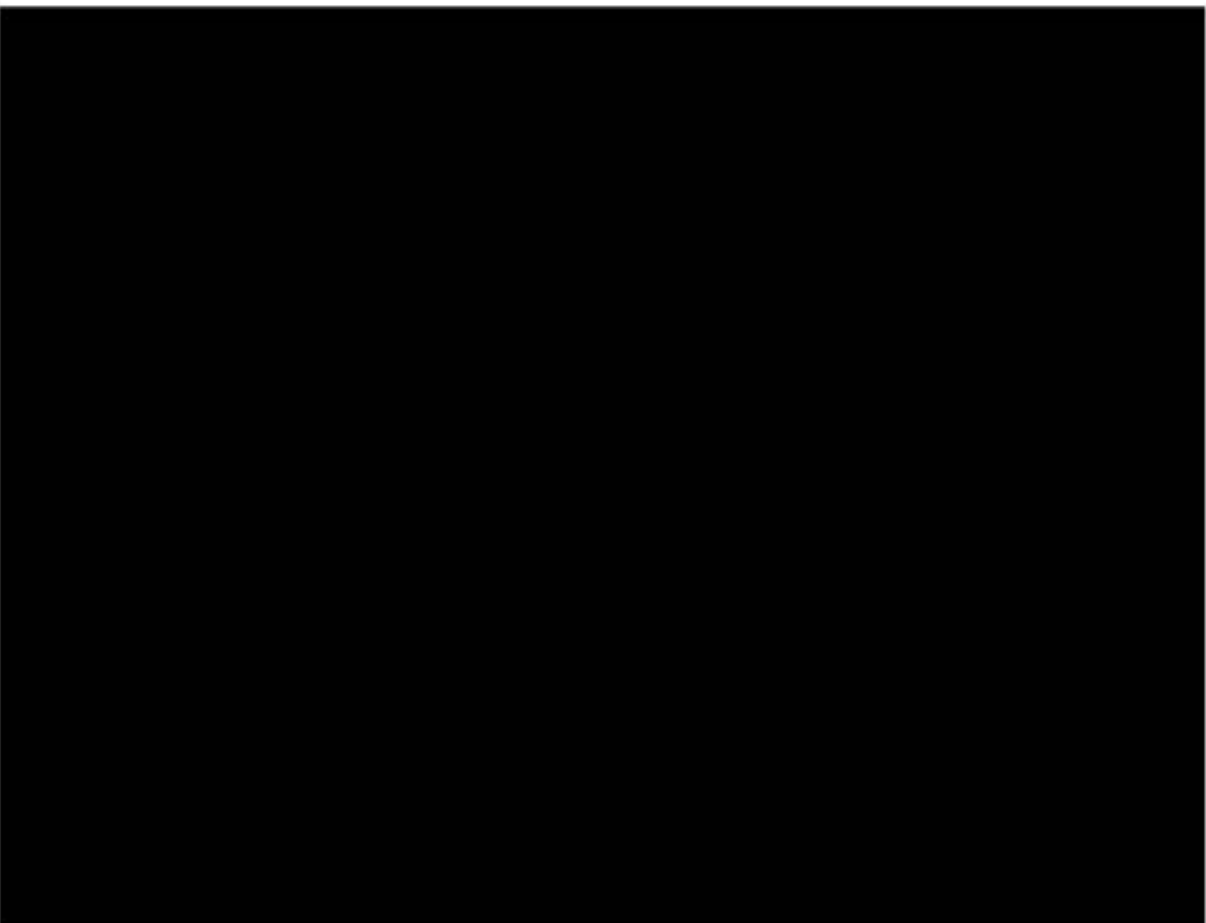
Av statsforvaltningens 185 virksomheter som mottok undersøkelsen er det kun 112 virksomheter som har svar og som derfor har oppgitt hvor mye beskyttelsesverdige data de besitter. Som beskrevet i kapittel 1.2.1 omfatter dette både skjermingsverdig ugradert informasjon og andre beskyttelsesverdige data. For å få en totaloversikt over de samlede mengdene beskyttelsesverdige data har vi derfor brukt informasjonen fra de som har svart på spørreundersøkelsen til å estimere beskyttelsesverdige datavolumer for øvrige virksomheter. Estimeringen er basert på blant annet virksomhetens størrelse, sektor og andre relevante kjennetegn og er nærmere beskrevet i Vedlegg G – Estimering av konsepter. Basert på disse estimatene anslår vi at det samlede volumet beskyttelsesverdige data i statsforvaltningen per i dag er på mellom [REDACTED]. Dette indikerer at andelen beskyttelsesverdig data av total mengde data er på mellom [REDACTED] prosent.

Videre er det også forventet en vesentlig vekst i datavolumer fremover. Ulike rapporter og analyser legger til grunn en forventet årlig vekst i samlede datavolumer på mellom 2 prosent og 23 prosent på verdensbasis. Dette er nærmere forklart i vedlegg G. Hvordan veksten i beskyttelsesverdige data vil utvikle seg relativt til annen type data har utredningen begrenset med grunnlag for å vurdere. Med utgangspunkt i de kildene utredningen har tilgjengelig er det utarbeidet en framskrivning av forventede volumer av beskyttelsesverdige data fram mot 2040. Utredningen tar utgangspunkt i at beskyttelsesverdige data er på rundt [REDACTED] 2022, [REDACTED] av total datamengde. Vi har estimert tre scenarier, et høyt scenario med 23 prosent årlig vekst, et middels scenario med 10 prosent årlig vekst og et lavt scenario med 3 prosent årlig vekst. I høyt scenario vokser datavolumet med 4000 prosent til 2040, mens det i middels scenarioet vokser med 450 prosent og i lavt scenario med 43 prosent. Utredningen tar utgangspunkt i middels scenario i analysene, men er bevisste på at den potensielle veksten i datavolum kan være betraktelig høyere. Dette er vist i figuren under.



Figur 2-3 - Vekst i datavolum for beskyttelsesverdige data frem mot 2040.

Som figuren over viser, vil mengden beskyttelsesverdige data kunne øke betraktelig i årene som kommer. Respondentene i spørreundersøkelsen oppgir at disse dataene kan være personopplysninger, helseopplysninger, ulike typer arkivverdige informasjon, geografiske data eller kartdata, statistiske data, forskningsdata, opplysninger om eierskap, forretningssensitive og børssensitive opplysninger, og annen informasjon som er unntatt offentlighet eller underlagt taushetsplikt. Figuren nedenfor gir en oppsummering av hvordan mengden beskyttelsesverdige data fordeler seg på ulike kategorier basert på de svarene utredningen har mottatt i spørreundersøkelsen. En nærmere beskrivelse av hvilke typer data virksomhetene anser som beskyttelsesverdige foreligger i vedlegg A - Behovskartlegging.



Som figuren over viser er det stor variasjon i hvilke typer data de ulike virksomhetene anser som beskyttelsesverdige. Det er også stor variasjon i hvor stort beskyttelsesbehovet er. Noen data er kritiske for å kunne levere sentrale offentlige tjenester og det er derfor avgjørende at de er tilgjengelige og korrekte til enhver tid. Andre data må beskyttes i henhold til for eksempel personvernlovgivning.

 Det pågår fortsatt prosesser på tvers av sektorer for å identifisere grunnleggende nasjonale funksjoner, gjennomføre skadevurderinger i virksomhetene og klassifisere skjermingsverdige infrastrukturer. Det er knyttet usikkerhet til hvordan omfanget av skjermingsverdig ugradert informasjon vil endre seg over tid etter hvert som disse prosessene går fremover.

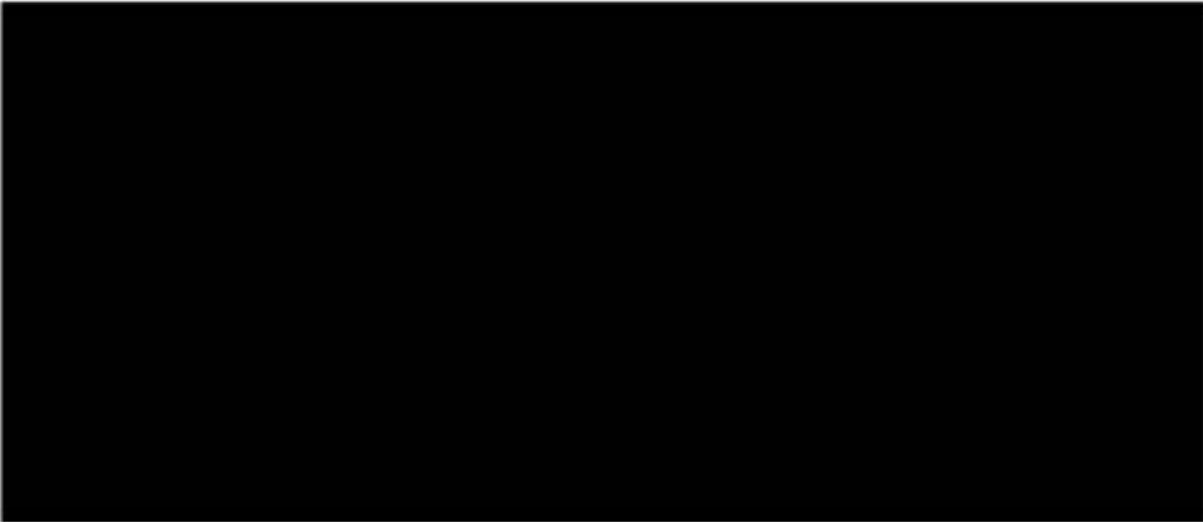
Uavhengig av om de beskyttelsesverdige dataene er å anse som skjermingsverdig ugradert eller ikke, er mye av informasjonen og systemene de ligger i avgjørende for at statsforvaltningen skal kunne levere en rekke sentrale tjenester til offentligheten. Noen eksempler på dette er:





Tilgang til disse dataene og systemene er nødvendig for at statsforvaltningen skal kunne yte tjenester på et høyt nivå og må derfor være tilgjengelige og beskyttes mot uautoriserte endringer. I tillegg vil noen systemer være særskilt viktige for å kunne håndtere situasjoner som oppstår i krise eller væpnet konflikt.

I forbindelse med kartleggingen av de beskyttelsesverdige dataene og systemene, ble virksomhetene bedt om å vurdere hvor stor andel av de beskyttelsesverdige dataene som er særskilt viktige i en krise eller væpnet konflikt. Samlet viser svarene at virksomhetene vurderer at  av den totale datamengden er å anse som særskilt viktig i en krise eller væpnet konflikt. Resultatene er vist i figuren under.



Flere av interessentene påpeker at det er utfordrende å konkretisere hvilke av dataene og systemene de forvalter som er særlig viktige i en krise- eller krigssituasjon. En del av disse systemene vil utgjøre viktige innsatsfaktorer i en krise eller væpnet konflikt, for å yte et minimumsnivå av offentlige tjenester og sørge for en grad av tjenestekontinuitet. Noen typer data og systemer er særlig viktige sett i lys av enkelte virksomheters rolle i Totalforsvaret der de understøtter Forsvaret. Bortfall av slike data og systemers tilgjengelighet og integritet kan derfor få vesentlige konsekvenser for nasjonens styringsevne og handlefrihet, eller påvirke nasjonens evne til å levere kritiske samfunnsfunksjoner gjennom hele krisespekteret.

De mest kritiske av disse dataene og systemene vil kunne bli vurdert som ugradert skjermingsverdig informasjon eller ugraderte skjermingsverdige informasjonssystemer etter sikkerhetsloven. Skjermingsverdig ugradert informasjon understøtter funksjoner som samfunnet er avhengig av. Dette fordrer at de underliggende informasjonssystemene er sikret på et forsvarlig nivå gjennom hele krisespekteret. Sikkerhetslovens krav skal sikre at skjermingsverdig, ugradert informasjon ikke går tapt, blir endret eller blir utilgjengelig, slik at nasjonale sikkerhetsinteresser ikke påvirkes. Krav som følger av sikkerhetsloven, er nærmere redegjort for i vedlegg B.

I en krisesituasjon er det overordnede formålet å sikre tilgang til sentrale tjenester som er nødvendige for å håndtere situasjonen som er oppstått. Det innebærer at aktører som er sentrale i krisehåndteringen skal kunne fortsette å levere viktige tjenester, og at offentlige tjenester påvirkes i minst mulig grad.

I væpnet konflikt vil formålet være å sikre statens styringsevne og handlefrihet i størst mulig grad, og ivareta et akseptabelt minimumsnivå av offentlig tjenesteproduksjon. I en krigssituasjon skal staten fortsatt ha kontroll over beskyttelsesverdige data og systemer for å minimere konsekvensene for grunnleggende tjenester.

2.1.2 Forvaltning og drift av beskyttelsesverdige data og systemer

Basert på tall fra Statsregnskapet brukte de statlige virksomhetene totalt 12,7 milliarder på drift av data og systemer i 2021¹². Disse kostnadene inkluderer blant annet leie av datasystemer og servere, kjøp av konsulenttjenester til utvikling og anskaffelse av programvare, men tar ikke høyde for bruk av interne IKT-ressurser. Med anslaget på at mengden beskyttelsesverdig data er på rundt 60 prosent av total datamengde og en antagelse om at drift og forvaltning av disse har tilsvarende kostnader som øvrige data og systemer, kan vi anslå at virksomhetene årlig bruker rundt 7,6 milliarder kroner på drift av beskyttelsesverdige data og systemer i 2021-kroner.

De beskyttelsesverdige dataene behandles i en rekke forskjellige registre og fagsystemer. En del av systemene benyttes kun av en enkelt virksomhet, mens andre benyttes av flere virksomheter eller av hele statsforvaltningen. De beskyttelsesverdige dataene og systemene i statsforvaltningen er fordelt på både standardløsninger¹³ og spesialutviklede løsninger¹⁴. En del av de beskyttelsesverdige dataene behandles også i hyllevare- og kontorstøtteløsninger¹⁵.

Beskyttelsesverdige data er ikke nødvendigvis skilt ut i egne løsninger, men ofte integrert i virksomhetens øvrige systemer og kan være plassert både i skyløsninger og i mer tradisjonelle IKT-systemer. Analyser basert på resultater fra spørreundersøkelsen vi har sendt ut i forbindelse med denne KVUen og en spørreundersøkelse av A-2 Norge som kartla drift og forvaltning av IKT-løsninger i staten gjennomført høsten 2021,¹⁶ indikerer at omtrent

¹² Kun 70 prosent av de 185 statlige virksomheten er en del av statsregnskapet, noe som tilsvarer kun [redacted] av datamengden. Vi har dermed estimert IKT-kostnader for disse for å få totale IKT-kostnader. Se flere detaljer i vedlegg G.

¹³ Standardløsninger er systemer som er kommersielt utviklet for en større kundegruppe, men som kan tilpasses enkeltkunder gjennom konfigurering og oppsett. Eksempler på standardløsninger er saks- og arkivsystem (for eksempel ePhorte, Public 360, DocuLive), økonomi- og lønssystemer (for eksempel SAP, Agresso/Unit4, Visma), ERP-løsninger (for eksempel SAP, Microsoft, Oracle) og pasientjournalsystemer (EPJ).

¹⁴ Spesialutviklede løsninger er laget for å dekke enkelte spesielle behov til en virksomhet. Spesialutviklede løsninger er aktuelle når virksomhetenes behov ikke dekkes av hyllevare- eller standardløsninger. Mange fagsystemer i offentlig forvaltning er spesialutviklede løsninger, som understøtter ett eller flere fagområder. Eksempler på dette er det statlige barnevernet (BiRK), statsbudsjettets samhandlingsverktøy for budsjettdata (Budmod), utlendingsmyndighetenes datasystem for utlendings- og flyktningsaker (DUF).

¹⁵ Hyllevare- og kontorstøtteløsninger er ferdige systemer som kjøpes og brukes uten tilpasninger. Eksempler er Office-pakken til Microsoft med Excel, Word, Outlook og PowerPoint, og prosjektstyringsverktøy som MS Project.

¹⁶ Kartlegging av drift og forvaltning av IKT-løsninger i statlige virksomheter, A-2 Norge, 2021

██████████ dag befinner seg på egendriftet plattform. Resterende beskyttelsesverdige data og systemer ligger i ulike skyløsninger¹⁷.

Gjennom analyser vi har gjennomført basert på spørreundersøkelsen om drift og forvaltning av IKT-løsninger i staten estimerer vi at i underkant av ██████████ av datamengden som er i sky ligger i lukkede skytjenester, mens øvrige ligger i allmenne skytjenester¹⁸. Videre viser undersøkelsen at de amerikanske selskapene Microsoft (Azure), Amazon (AWS) og Google (Google Cloud) dominerer markedet for offentlige skytjenester levert til statsforvaltningen, med Microsoft som den klart største aktøren i Norge. Markedet for de kommersielle aktørene som tilbyr lukkede skyløsninger er mye mer fragmentert med mange forskjellige leverandører.

Hvor beskyttelsesverdige data er lagret varierer ut fra hvilke typer systemer som brukes. Nær 70 prosent av de virksomhetene som benytter spesialutviklede løsninger oppgir at deres data er lagret i Norge. For de som benytter standardløsninger eller hylleware- og kontorstøtteløsninger er andelen som oppgir at dataene er lagret i Norge henholdsvis 60 og 40 prosent.

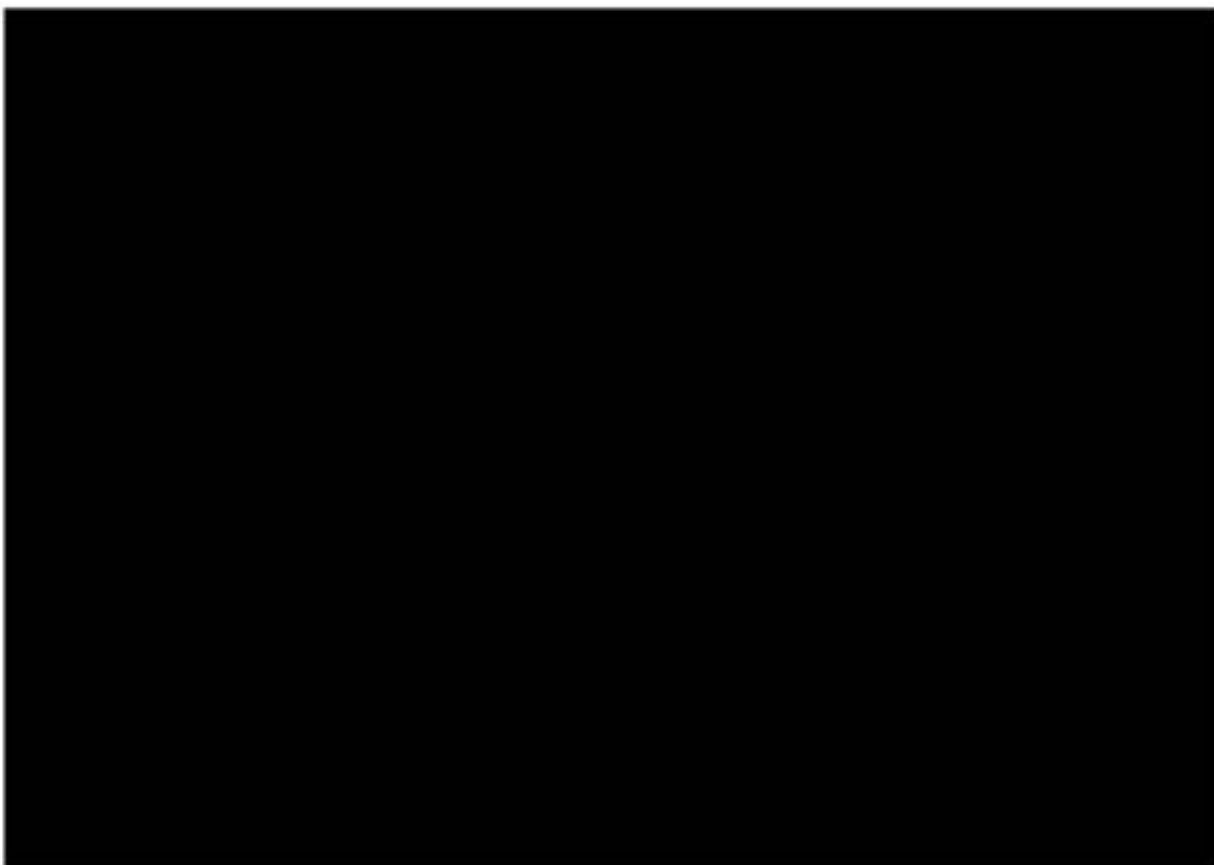
Kartleggingen fra høsten 2021 om drift og forvaltning av IKT-løsninger i statlige virksomheter viser videre at statsforvaltningen forventer en stor vekst i bruk av skyløsninger framover. Det er bruk av allmenne skytjenester som forventes å vokse mest. Bruken av lukkede skyløsninger forventes også å øke framover. Samlet forventer nær halvparten av virksomhetene i stor eller svært stor grad økt bruk av offentlige skyløsninger for egne systemer. Basert på utredningens analyser av resultatene, er det anslått en årlig vekst på 2,5 prosentpoeng i det allmenne skymarkedet, og en årlig vekst på rundt 2 prosentpoeng for lukkede skytjenester for statsforvaltningen.

Ettersom mange av virksomhetene allerede i dag benytter skytjenester for hylleware-, kontorstøtte- og standardløsninger, er det sannsynlig at det i større grad vil være mer spesialutviklede fagsystemer som vil flyttes ut i sky framover. Noen av disse systemene vil imidlertid fortsette å ligge på egendriftede plattformer. En del av disse løsningene er eldre systemer som i liten grad er tilpasset sky. I spørreundersøkelsen vi har gjennomført oppgir også enkelte virksomheter at de er tilbakeholdne med å flytte enkelte data og systemer ut i sky fordi det oppleves som krevende å sikre tilstrekkelig ivaretagelse av alle lover og regler. Likevel oppgir rett i underkant av 60 prosent av de statlige virksomhetene som har svart på spørreundersøkelsen at de planlegger å flytte beskyttelsesverdige data og systemer helt eller delvis ut i sky i årene som kommer.

Basert på fordeling av beskyttelsesverdig data mellom egendriftede plattformer, lukket sky og allmenn sky, veksten i bruk av skyløsninger og veksten i datamengde som er beskrevet i avsnittene over estimerer vi en forventet utvikling i bruk av ulike leveransemodeller for lagring og behandling av beskyttelsesverdige data og systemer fram mot 2040. Veksten i datamengden baserer seg på middels scenario på 10 prosent årlig vekst beskrevet i kapittel 2.1.1 Mengde og type beskyttelsesverdige data i statsforvaltningen. Denne utviklingen er vist i figuren under.

¹⁷ Beskrivelse av analysene finnes i vedlegg G Estimering og usikkerhetsanalyse

¹⁸ Beskrivelse av analysene finnes i vedlegg G Estimering og usikkerhetsanalyse. Vi har sett bort ifra hybride skyløsninger.



2.2 utfordringer ved bruk av skytjenester

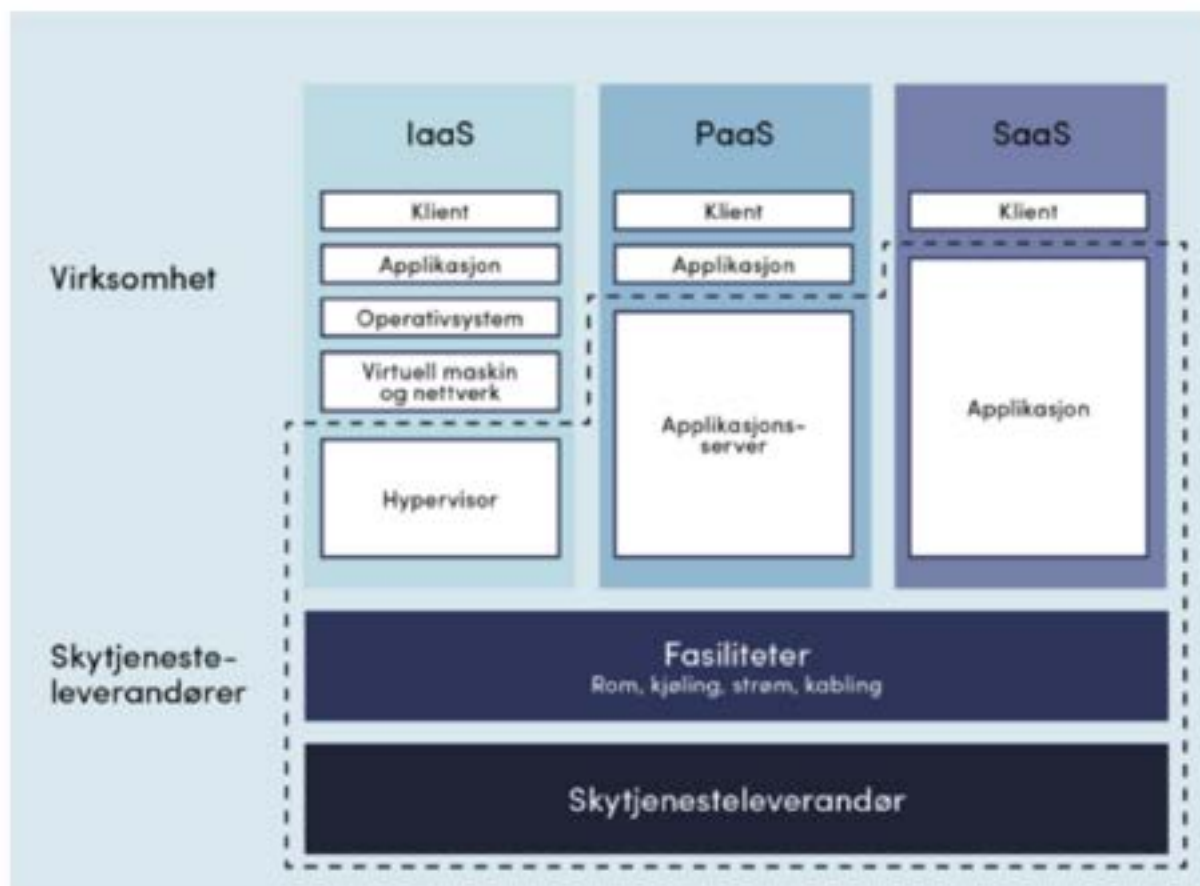
Skytjenester, og særlig allmenne skytjenester, skal blant annet utnytte stordriftsfordeler som legger til rette for kostnadseffektive løsninger og stor innovasjonskraft. De store skyleverandørene har store og effektive drifts-, sikkerhets- og utviklingsmiljøer. I tillegg vil dynamisk fordeling av datasenterressursene mellom kundene, gjøre at prosessering og data kan flyttes mellom datasentre ut fra tilgjengelig kapasitet.²⁰ Det gir stor fleksibilitet og mulighet til å skalere tjenester. Skyleverandørenes digitale verdikjeder på tvers av landegrenser gjør det imidlertid vanskelig å kontrollere hvor dataene til enhver tid er lagret og hvem som har tilgang til dem.

2.2.1 Bruk av skytjenester utfordrer virksomheters kontroll over data og systemer

Figuren under illustrerer hvordan forskjellige grader av tjenesteutsetting gjennom bruk av sky kan resultere i ulik grad av kontroll. Området innenfor de stiplede linjene viser hva leverandøren har ansvar for. Alt utenfor den stiplede linjen må virksomheten selv sikre.

¹⁹ Utviklingen over tid for IKT-tjenester på egendriftet plattform; frem til 2031 vil datamengden i denne leveransemodellen synke grunnet at flere går over til skybaserte tjenester. Etter 2031 vil datamengden å vokse som følge av generell vekst i datamengde frem mot 2040.

²⁰ Bruk av skytjenester i Forsvaret – muligheter og utfordringer, FFI, 2021



Figur 2-7 - Illustrasjon av sikkerhetsansvar i ulike skymodeller. Se også ordlisten for forklaring av IaaS, PaaS og SaaS.

Som figuren viser, vil man selv med begrenset bruk av skytjenester gi fra seg en viss grad av kontroll. Dette følger i stor grad av hvordan skytjenester er innrettet. For å i størst mulig grad kunne utnytte stordriftsfordeler benytter mange skyleverandører ressurser og komponenter i flere land, hvilket innebærer at data og metadata i en skytjeneste kan være underlagt ulike lands jurisdiksjon og kontroll.

Figuren under viser en forenklet illustrasjon av hvordan data og systemer kan være underlagt flere lands jurisdiksjon gjennom lange digitale verdikjeder, selv om datasenteret er plassert i Norge.



Figur 22-8 - Illustrasjon av hvordan data og metadata kan være underlagt flere lands lover, selv om datasenteret ligger i Norge. Piler indikerer teknisk tilgang til data og metadata. Kilde: NSM, Colourbox.com

Hvilken jurisdiksjon de ulike dataene og systemene i en skytjeneste er underlagt påvirkes blant annet av hvor datasentre er plassert, hvor funksjoner knyttet til drift, support eller sikkerhetskopi befinner seg, og i hvilke land leverandørene har hovedkontor.

Basert på svarene fra en markedsundersøkelse (RFI) gjennomført i forbindelse med denne utredningen, finnes det enkelte kommersielle leverandører i Norge som kan tilby skytjenester som anses å ha en høyere grad av nasjonal kontroll, men til en høyere kostnad. Grunnen til dette kan være av både teknisk og administrativ art. For eksempel kan hovedkontoret ligge i Norge eller at drift og support i hovedsak blir utført av personell i Norge. Det er verdt å nevne at prisene varierer en del fra leverandør til leverandør, men vi ser at gjennomsnittsprisen for et produksjonsmiljø (PaaS-nivå) kan øke i betydelig grad dersom man stiller strenge krav til nasjonal kontroll. Selv om det er noe usikkerhet knyttet til tallene, viser det at kostnadsnivået øker dersom man ønsker en høyere grad av nasjonal kontroll.

Ved bruk av kommersielle leverandører følger det også usikkerhet knyttet til eierskap. Mulighet for oppkjøp og fusjoner i verdikjeden gjør det utfordrende å beholde kontroll og oversikt over tid. Det gjelder ikke bare de internasjonale leverandørene. Også eierskapsstrukturer i det norske markedet er sårbare for strategiske oppkjøp fra utenlandske aktører, blant annet gjennom trusselaktørers strategiske fremgangsmåter for å skape komplekse og uoversiktlige eierstrukturer.²¹

Markedskonsentrasjonen gir også en risiko for at store mengder beskyttelsesverdige data og systemer samles hos én eller få leverandører. At store mengder beskyttelsesverdige data er konsentrert hos en eller noen få aktører utenfor norsk kontroll øker også sårbarheten for ytre politisk press. Dette kan potensielt føre til redusert styringsevne og handlefrihet i en krise eller ved væpnet konflikt. Dette kan skje enten ved at norske virksomheter aktivt utestenges

²¹ Risiko 2020, "Strategiske investeringer og oppkjøp", NSM, 2020

fra systemene, slik tilfellet har vært for Russland i kjølvannet av invasjonen i Ukraina, eller ved at norske virksomheter nedprioriteres i en internasjonal krise.²²

2.2.2 Økt risiko for tap av konfidensialitet, integritet og tilgjengelighet

Summen av manglende kontroll over enkeltvirksomheters data og systemer, og tap av strategisk kontroll som følge av konsentrasjonsrisiko gir økt risiko for tap av konfidensialitet, tilgjengelighet og integritet til beskyttelsesverdige data og systemer.

Virkemidler innen det digitale domenet benyttes av både statlige og ikke-statlige aktører. Statlige aktører disponerer avanserte verktøy og betydelige ressurser. Metodene de benytter tyder på en målrettet og langsiktig satsning innen digitale kapabiliteter. Samtidig ser vi at digital kriminalitet blir stadig mer profesjonalisert. En konsekvens av dette er blant annet at digital utpressing øker i både omfang og antall. I flere tilfeller har slike hendelser ført til store systemutfall som medfører at funksjoner og tjenester blir utilgjengelige, og at sensitiv informasjon blir kjent for uvedkommende.

Tap av konfidensialitet for beskyttelsesverdige data vil typisk få konsekvenser for enkeltpersoner eller virksomheter. Det kan for eksempel være knyttet til brudd på personvern eller taushetsplikt, eller fare for spredning av forretningssensitiv informasjon. Manglende tilgjengelighet og integritet kan føre til at virksomhetene ikke får tak i eller kan stole på den informasjonen de trenger for å levere tjenester. I fredstid vil det kunne føre til forsinkelser, feil eller annen forringelse av kvaliteten på tjenestene, som igjen vil kunne påføre både virksomheter og brukere vesentlige kostnader og medføre alvorlige konsekvenser.

I en krise eller væpnet konflikt vil tilgjengelighets- og integritetsbrudd få større konsekvenser. Hvilke konsekvenser som vil kunne oppstå er avhengig av hvilke data og systemer som blir påvirket og hvilke tjenester de understøtter. I tabellen under viser vi noen eksempler på mulige konsekvenser som kan oppstå dersom ulike data eller systemer blir kompromittert eller utilgjengelig.

Tabell 2-1 - Eksempler på hva som kan tenkes å være vurdert som beskyttelsesverdig data og systemer.

Departement	System	Tjenester som støttes	Mulige konsekvenser
Helse- og omsorgsdepartementet			

²² Microsoft suspends new sales in Russia, Microsoft, mars 2022

Departement	System	Tjenester som støttes	Mulige konsekvenser
Justis- og beredskaps-departementet			
Kommunal- og distrikts-departementet			

Departement	System	Tjenester som støttes	Mulige konsekvenser
Samferdsels-departementet			
Alle departementer			

Det finnes flere reelle eksempler på at tap av konfidensialitet for beskyttelsesverdige data kan inntreffe. I mai 2022 ble det for eksempel kjent at en database hos Norkart var kompromittert og en kopi av Matrikkelen ble lastet ned av en ukjent aktør.²⁸ Persondata som

[Redacted text]

²⁸ Nasjonalt digitalt risikobilde 2022, NSM, 2022

navn, adresser, fødselsnummer og informasjon om hva man eier kom på avveie. Selv om dette er ugraderte data, er det særlig bekymringsfullt dersom denne type datasett kan settes i sammenheng med annen tilgjengelig informasjon. Det kan for eksempel brukes til å utnytte eller eksponere både enkeltpersoner og virksomheter og kan være første ledd i en større cyberoperasjon. Legitime brukeropplysninger kan benyttes som inngangsmetode inn i virksomhetens systemer og viser at informasjon som innhentes i kartleggingsøyemed av ondsinnede aktører faktisk omsettes og utnyttes.

Et annet eksempel på konsekvenser er løsepengeangrepet på Østre Toten kommune i 2021.²⁹ Angrepet førte til at alle kommunens IT-systemer var nede over en lengre periode. I perioden IT-systemene var utilgjengelig hadde ikke barnevernet eller hjemmesykepleierne tilgang til sine systemer. Gjenopprettingen etter angrepet er anslått å koste om lag 20 millioner kroner. I tillegg vil det reduserte tilbudet til innbyggerne, og slitasjen på ansatte i kommunen også ha en samfunnsmessig kostnad. Dersom slike angrep rammer nasjonale tjenester, vil konsekvensene være langt mer omfattende.

Informasjonens verdi og kritikalitet vil variere i de ulike delene av krisespekteret. Helsedata fikk for eksempel en høyere verdi under utbruddet av Covid-19 grunnet økt behov for behandling av smittede og gjennom fokuset på forskning og utvikling av en vaksine.

2.3 utfordringer ved utvikling på egne plattformer

Løsninger som utvikles og driftes på egen plattform gir stor grad av kontroll, ettersom man kan sikre lokal lagring og behandling av data og systemer og mulighet til å styre hvem som har tilgang til dem. Som enkeltstående virksomhet får en imidlertid ikke utnyttet stordriftsfordelene knyttet til infrastruktur, driftsressurser og innovasjonskraften i kompetansemiljøene til leverandørene av kommersielle skyløsninger. Det kan gjøre det krevende å holde kostnadene nede og følge den teknologiske utviklingen.

Å bygge sikker IKT-infrastruktur som ivaretar både nasjonal kontroll og behov for bedre funksjonalitet over tid, kan være krevende. Virksomheter som ønsker å utvikle IKT-infrastruktur på egen plattform må gjøre vesentlige investeringer og ha kompetanse og ressurser som kan drifte, oppdatere og jevnlig forbedre løsningene dersom de ønsker å opprettholde tjenestekvaliteten. Det kreves et høyt kompetansenivå for å holde løsningene sikre og tilgjengelige i tråd med sikkerhets- og driftskrav og å holde tritt med et omskiftelig trusselbilde.

2.3.1 Økte kostnader til investering, drift og vedlikehold

Utvikling av IKT-systemer og -infrastruktur krever investeringer som følge av at blant annet alt av maskinvare, lisenser til programvare, nettverksutstyr og fysiske lokasjoner må anskaffes. Etter installasjon krever alle IKT-løsninger kontinuerlig vedlikehold. Dette krever ressurser og kompetansemiljøer som kan være kostbart og vanskelig å bygge opp og beholde, særlig for mindre virksomheter.

Statsforvaltningen må fortløpende investere for å sikre at deres IKT-løsninger holder et akseptabelt sikkerhetsnivå med egnet funksjonalitet. En betydelig andel av statsforvaltningen har store utfordringer med å klare dette. En kartlegging av

²⁹ Temaside: Dataangrep i 2021 mot Østre Toten kommune, NRK, januar 2023

statsforvaltningens eksisterende IKT-systemer og infrastruktur fra 2019³⁰ viser at virksomhetene som deltok i undersøkelsen disponerte opp mot 6 800 systemer, og at mellom 500 - 600 av disse ble vurdert som meget viktige og/eller kritiske for virksomhetene. Det ble estimert at det samlede etterslepet for IKT-systemene var mellom 5,2 – 5,8 mrd. kroner, hvor ca. [REDAKERT] kan knyttes til de viktigste og/eller kritiske systemene. Etterslepet er i like stor grad knyttet til systemer under 10 år som til eldre og komplekse systemer. For IKT-infrastruktur ble etterslepet estimert til å ligge mellom 1,3 – 1,5 mrd. kroner, men funnene gir likevel en tydelig indikasjon på behovet for oppgradering og modernisering av viktige og kritiske IKT-systemer i statsforvaltningen og at kostnadene som følger av dette vil være betydelige.

Kartleggingen viste også at etterslepet knyttet til de eldste IKT-systemene bare unntaksvis var høyt. Dette innebærer at man fortsatt kan forvente en lang levetid for de eldste IKT-systemene. De representerer trolig et «grunnfjell» som det er viktig å vedlikeholde på en god måte fremover, og at nye skybaserte systemer i mange tilfeller vil bygges rundt disse.

Alternativet til å disponere egne ressurser og bygge opp egen kompetanse er å tjenesteutsette deler av arbeidet, samtidig som virksomheten selv må ivareta sitt ansvar for forebyggende sikkerhet. Så lenge statsforvaltningen ikke opptre koordinert, vil muligheten til å utnytte stordriftsfordeler og forhandlingsmakt reduseres, noe som vil kunne medføre høyere kostnader.

2.3.2 Risiko for redusert informasjonssikkerhet

NSM har over tid observert at mange virksomheter mangler grunnleggende risikoreduserende tiltak, og at den generelle IKT-sikkerheten hos mange virksomheter er svak.³¹ Inntrengingstester har blant annet avdekket tilfeller hvor virksomhetens servere mangler kritiske sikkerhetsoppdateringer, og hvor eldre operativsystemer mangler viktig sikkerhetsfunksjonalitet. Noen virksomheter benytter datamaskiner med operativsystemer som er så gamle at leverandøren ikke lenger leverer sikkerhetsoppdateringer. Nye systemer legges på eldre systemer som i kombinasjon kan introdusere sårbarheter som det er vanskelig å ha kontroll og oversikt over. Disse sikkerhetsutfordringene kan være en konsekvens av manglende ressurser, kompetanse og forståelse av risikobildet knyttet til verdiene virksomhetene forvalter.

Intervjuer med virksomheter i statsforvaltningen har avdekket at det er store forskjeller i IKT-kompetanse mellom virksomheter. Enkelte virksomheter har store IT-avdelinger med høy kompetanse, som også etablerer egne skyløsninger, mens andre virksomheter oppgir at de ikke har tilstrekkelig kompetanse og kapasitet til å gjøre nødvendige vurderinger. Dette gjelder også data og systemer som kan være av interesse for trusselaktører. IKT-utvikling på egne plattformer er utfordrende for virksomheter med manglende tilgang til nødvendige ressurser og kompetanse. Mangelfulle verddivurderinger av virksomhetens data kan føre til at informasjon ikke sikres tilstrekkelig i tråd med gjeldende regelverk, og åpner for en rekke sårbarheter som kan utnyttes.

Profesjonelle tjenestetilbydere kan ha tilgang til ressurser og kompetanse som virksomheten selv mangler, og som er nødvendige for å opprettholde et høyt sikkerhetsnivå over tid.

³⁰ Evaluering av IT-tilstanden i statlige virksomheter, A-2 Norge, 2019

³¹ Nasjonalt digitale risikobilde 2020 og 2021, NSM

Tjenesteutsetting kan således bidra til kvalitetssikring og økt sikkerhet så lenge virksomheten får tilstrekkelig støtte i bruken av tjenesten og har god tilgang til egne logger og informasjon ved hendelseshåndtering. Samtidig er det viktig å understreke at virksomheter ikke kan basere sitt forebyggende sikkerhetsarbeid på tjenesteutsetting. Virksomhetens ledelse har selv det overordnede ansvaret for sikkerheten i egen virksomhet, herunder å sørge for at virksomheten og brukerne i virksomheten tilføres nødvendig kompetanse.

2.3.3 Tapt produktivitet og redusert kvalitet på tjenester

For å sikre tilstrekkelig utnyttelse av den kontinuerlige teknologiske utviklingen er det behov for sterke kompetansemiljøer. Dette vil være særlig krevende for mindre virksomheter å oppnå på egenhånd, noe som vil kunne føre til tap av funksjonalitet over tid. Det vil også kunne innebære redusert kapasitet og ytelse, redusert bredde og nivå på tjenester og en manglende evne til å tilpasse løsninger til behovsendringer.

En betydelig andel av dagens innovasjon og teknologisk utvikling innen IKT skjer nå i tilknytning til skyteknologi og -tjenester, og en vellykket digitalisering av offentlig sektor avhenger av at statlige virksomheter har tilgang til moderne skyfunksjonalitet. Dersom man ikke kan utnytte innovasjonsmulighetene som denne funksjonaliteten innebærer kan det resultere i særskilt to negative konsekvenser. For det første kan det medføre at statlige virksomheter går glipp av muligheter til å effektivt samhandle internt og eksternt, forbedre interne saksbehandlingsprosesser og tilby moderne tjenester. Dette utgjør tapte produktivitetsgevinster som kunne bidratt til en effektivisering av offentlig sektor. For det andre kan det medføre redusert kvalitet på tjenestetilbudet. Statsforvaltningens muligheter til tjenesteinnovasjon svekkes som følge av redusert funksjonalitet. Det medfører tapte gevinster for innbyggere og andre virksomheter som ville dra nytte av bedre tjenester.

Beskyttelsesverdige data og systemer understøtter en rekke tjenester. Noen av disse tjenestene er beskrevet i tabellen under. Flere av disse tjenestene benyttes direkte eller indirekte av store deler av befolkningen. Redusert kvalitet på tjenestene som understøttes av beskyttelsesverdige data og systemer kan derfor medføre store negative konsekvenser for hele befolkningen.

Tabell 2-2 - Oversikt over eksempler på mulige tjenester med beskyttelsesverdige data og systemer³²

Department	Funksjon	Konsekvenser	Virksomheter	Sluttbrukere
Helse- og omsorgs-departementet				
Justis- og beredskaps-departementet				

³² Samfunnets kritiske funksjoner ver. 1, Direktoratet for samfunnssikkerhet og beredskap, 2016

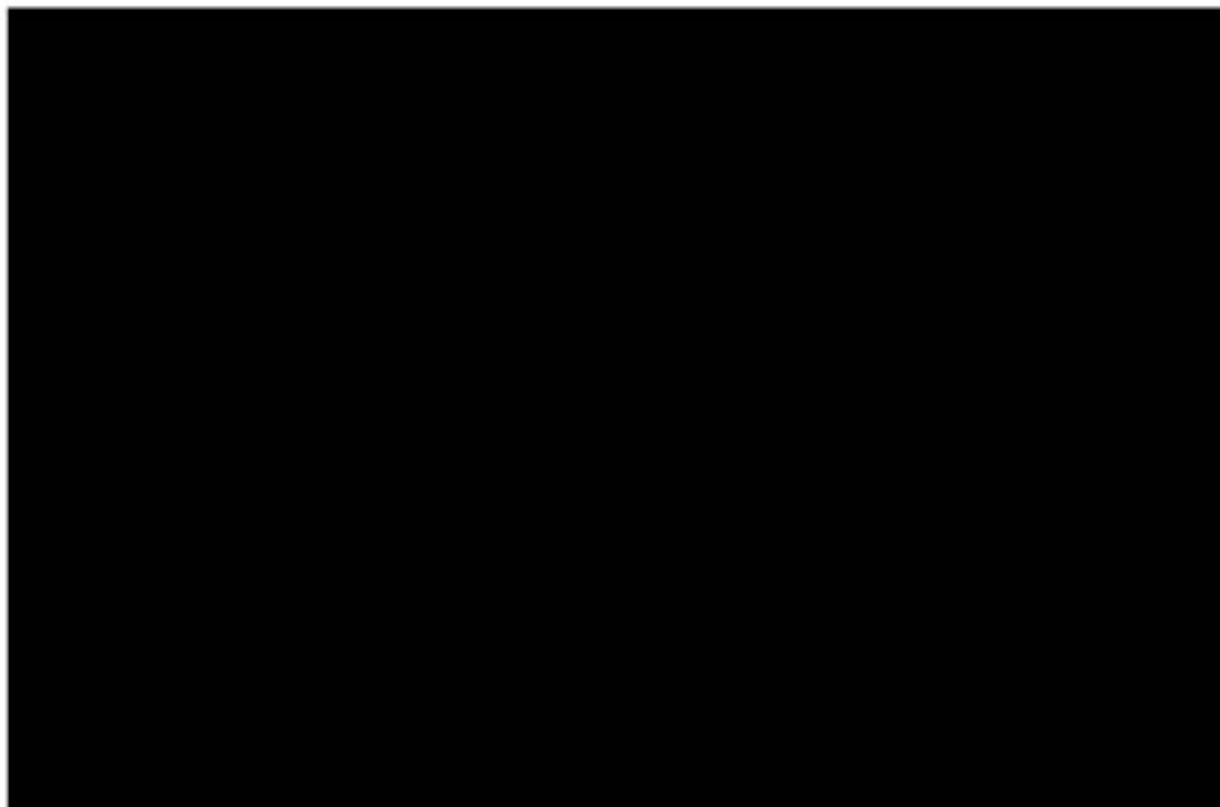
Department	Funksjon	Konsekvenser	Virksomheter	Sluttbrukere
Olje- og energi-departementet				
Samferdsels-departementet				
Finans-departementet				
Kommunal- og distrikts-departementet				
Alle departementer				

3 Behovsanalyse

Statsforvaltningen har behov for funksjonelle og kostnadseffektive skytjenester som sikrer tilstrekkelig grad av nasjonal kontroll over beskyttelsesverdige data og systemer. Det vil legge til rette for videre digitalisering og effektivisering av statlig sektor innenfor sikre rammer. Det innebærer et behov for å kunne styre fysisk og logisk tilgang til infrastruktur og systemer som lagrer og behandler beskyttelsesverdige data. Videre er det behov for en bredde av digitale tjenester med tilstrekkelig fleksibilitet og kapasitet som kan understøtte de statlige virksomhetenes evne til å levere offentlige tjenester av høy kvalitet på en effektiv måte.

Norge har behov for funksjonelle og kostnadseffektive skytjenester som gir tilstrekkelig grad av nasjonal kontroll over beskyttelsesverdige data og systemer, samtidig som det legges til rette for videre digitalisering og effektivisering av statlig sektor. Etterspørselen etter skytjenester er stor, både fra kommersielle og offentlige virksomheter. Utredningens analyse viser at det også er stor etterspørsel etter å kunne bruke skytjenester til lagring og behandling av beskyttelsesverdige data og systemer. Dersom dagens utviklingstrender fortsetter, vil om lag [REDACTED] av beskyttelsesverdige data og systemer ligge i skybaserte løsninger fra 2032 og ut analyseperioden.

Det er spesielt beskyttelsesverdige data og systemer som er særskilt viktige i krise og væpnet konfliktsom det er størst behov for å ha nasjonal kontroll over. Dette skyldes at et bortfall av eller integritetsbrudd i disse dataene og systemene potensielt kan få vesentlige konsekvenser for statens styringsevne og handlefrihet, eller påvirke statens evne til å levere viktige tjenester gjennom hele krisespekteret. Basert på spørreundersøkelsen vist til i problembeskrivelsen er dette estimert til å utgjøre om lag [REDACTED] av statsforvaltningens samlede dataomfang. Veksten i datamengden baserer seg på middels scenario på 10 prosent årlig vekst beskrevet i kapittel 2.1.1. Denne forventede framtidige utviklingen er vist i figuren nedenfor og fordeler seg mellom allmenne skytjenester, lukkede skytjenester og IKT-tjenester på egendriftet plattform.



Som figuren over viser, forventer vi en sterk vekst i bruk av skytjenester for beskyttelsesverdige data og systemer fram mot 2040. Behov for flere, bedre og mer digitaliserte offentlige tjenester øker statsforvaltningens etterspørsel etter mer kapasitet, ytelse og tjenesteutvikling. Omfanget av informasjon som behandles, lagres og deles internt i og på tvers av statsforvaltningen blir stadig større. Det øker virksomhetenes behov for fleksible og kostnadseffektive IKT-løsninger med høy funksjonalitet som skytjenester kan tilby.

Med økt bruk av enkelte skytjenester vil imidlertid den nasjonale kontrollen over disse dataene og systemene bli kraftig svekket. Det kan få store konsekvenser. Enkelte tjenester som behandler beskyttelsesverdige data, er så kritiske for samfunnet at de må være tilgjengelige og inneholde korrekt informasjon gjennom hele krisespekteret. Dersom disse tjenestene faller bort eller innholdet i data er endret uten autorisasjon, vil det påvirke statens evne til å levere sentrale tjenester. Det er derfor et behov for å sikre de beskyttelsesverdige dataene og systemene i hele krisespekteret. For å sikre beskyttelsesverdige data i statsforvaltningen, må staten ha kontroll over hvor data lagres og behandles, og hvem som har tilgang til slike data.

De statlige virksomhetene står derfor overfor et dilemma der de må veie behovet for å kjøpe inn tjenester med høy funksjonalitet, til lavest mulig kostnad, mot behovet for nasjonal kontroll over beskyttelsesverdige data. Dette dilemmaet vil ikke uten videre løses av seg selv. Hver enkelt virksomhet har selv ansvar for å vurdere hva som er en forsvarlig håndtering av deres data – de har imidlertid ikke forutsetninger for å vurdere den totale risikoen ved å gi fra seg kontrollen på et nasjonalt nivå. Videre har de kommersielle leverandørene få incentiver til å levere tjenester det ikke er etterspørsel etter. Fragmenterte innkjøp, begrenset bestillerkompetanse og høyt kostnadspress blant statlige virksomheter vil

derfor kunne føre til at beskyttelsesverdige data flyttes ut i løsninger utenfor nasjonal kontroll. Det vil øke risikoen for bortfall og forringelse av sentrale offentlige tjenester i fred, krise og væpnet konflikt.

I delkapitlene under gir vi en nærmere beskrivelse av disse overordnede behovene og hvilke operasjonelle behov for ulike funksjoner og egenskaper de medfører. Behovene er identifisert gjennom informasjon og analyser basert på både normative, etterspørselsbaserte og interessentbaserte metoder, nærmere beskrevet i vedlegg A - Behovsanalyse.

3.1 Behov for å sikre beskyttelsesverdige data og systemer i hele krisespekteret

Norske virksomheter står overfor et komplekst risikobilde der fremmede stater og andre aktører forsøker å utnytte sårbarheter for å få tilgang til verdier. Både Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) vurderer at utenlandsk etterretnings- og påvirkningsaktivitet rettet mot både offentlige og private virksomheter forblir en betydelig trussel mot norske interesser.^{34, 35}

Trusselaktører kan utnytte politiske og økonomiske forhold og juridiske gråsoner og kombinere virkemidler som cyberoperasjoner, påvirkningsoperasjoner, investeringer og oppkjøp for å oppnå strategiske mål. Trusselaktører har med andre ord et bredt utvalg av virkemidler til rådighet.

Cyberoperasjoner og påvirkningsoperasjoner ved hjelp av ukonvensjonelle virkemidler er blitt en del av militære operasjoner. En hensikt med slik irregulær krigføring kan være å undergrave befolkningens tillit til myndighetene og ramme myndighetenes styringsevne og handlefrihet ved hjelp av ukonvensjonelle virkemidler, inkludert cyberoperasjoner rettet mot sivile mål. Dette medfører et behov for å sikre sivil infrastruktur også med hensyn til de mest avanserte trusselaktørene. Irregulær krigføring innebærer også at de tradisjonelle skillene mellom fred, krise og krig utfordres. Det er derfor behov for tiltak for å sikre viktig sivil infrastruktur gjennom hele krisespekteret.

Etter hvert som man beveger seg gjennom krisespekteret, fra fred til krise og væpnet konflikt, vil trusselaktører kunne benytte ulike virkemidler. I en fredssituasjon vil innhenting av informasjon og kartleggingsaktivitet kunne legge til rette for større operasjoner ved en eventuell fremtidig eskalering. I en krisesituasjon vil man for eksempel kunne se et økt antall cyber- og påvirkningsoperasjoner, slik man har sett i opptakten til Russlands invasjon av Ukraina i 2022.³⁶ I en væpnet konflikt vil man kunne oppleve fysiske anslag på norsk jord i tillegg til digitale angrep. Høyere oppe i krisespekteret vil den samfunnsmessige kostnaden være svært betydelig dersom virksomheter i statsforvaltningen rammes av flere samtidige hendelser i ulike domener, og særlig dersom hendelsene rammer viktige samfunnsfunksjoner.

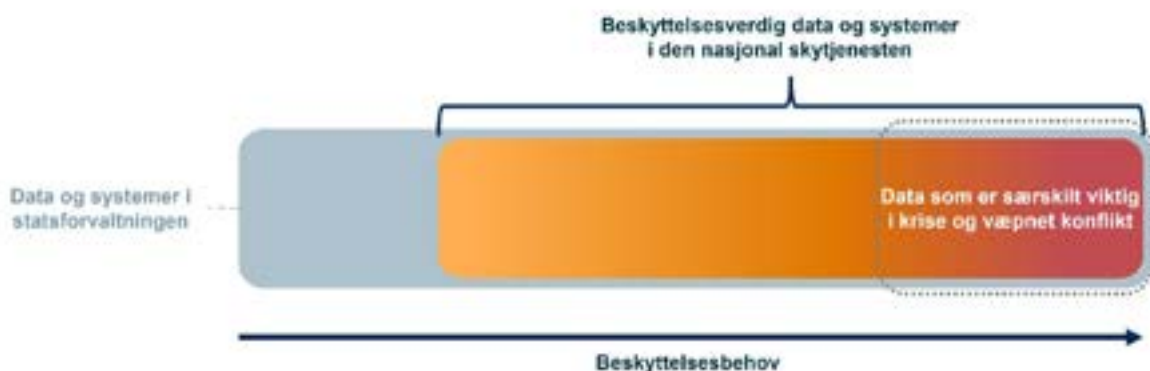
I spørreundersøkelsen ble virksomheter i statsforvaltningen spurt om hvor stor andel av deres egne beskyttelsesverdige data og systemer som de anser som *særs viktig i en krise eller krig*. På denne måten fikk virksomhetene anledning til å oppgi andelen av de

³⁴ Politiets sikkerhetstjeneste (2022), *Nasjonal trusselvurdering 2022*, s. 6-7.

³⁵ Etterretningstjenesten (2022), *Fokus 2022*, s. 19.

³⁶ [EU-erklæring om russiske cyberangrep mot Ukraina, Regjeringen.no, 12.05.2022](#)

beskyttelsesverdige dataene og systemene som de selv vurderer som særskilt viktige gjennom hele krisespekteret. Svarene på dette spørsmålet gir den beste indikasjonen på virksomhetenes verdivurderinger av egne data og systemer ut fra hvilke data som har størst betydning for samfunnsviktige tjenester. Utredningens vurdering er at denne kategorien - beskyttelsesverdige data og systemer som er særskilt viktige i krise og væpnet konflikt – innehar det største behovet for nasjonal kontroll, illustrert i figuren under. Dette skyldes at et bortfall av eller integritetsbrudd i disse dataene og systemene potensielt kan få vesentlige konsekvenser for statens styringsevne og handlefrihet, eller påvirke statens evne til å levere viktige tjenester gjennom hele krisespekteret. Basert på dette er det derfor utredningens vurdering at den mengden data virksomhetene har oppgitt som særskilt viktig i en krise eller væpnet konflikt per nå gir den beste indikasjonen på mengden data som bør inngå i en nasjonal sky.



Figur 3-2 Illustrasjon av hvilke data og systemer som er særskilt viktig i krise og væpnet konflikt og som danner utgangspunktet for videre analyse i utredningen.

Behov for nasjonal kontroll over IKT-infrastruktur og -tjenester kan komme til uttrykk iblant annet lover og forskrifter. Eksempler på dette kan være utførselsforbudet i arkivloven § 9b³⁷ og eierskapskontrollbestemmelsene i sikkerhetsloven kapittel 10.³⁸ Andre lover inneholder krav til for eksempel sikkerhet, beredskap, konfidensialitet, integritet og tilgjengelighet, ansvarlighet, dokumentasjon, risikovurderinger, internkontroll, informasjonssikkerhet mv. som kan sette grenser for bruken og innretningen av skytjenester. De siste årene er det også publisert en rekke offentlige utredninger, strategier og stortingsmeldinger som beskriver behovet for kontroll over data og IKT-infrastrukturer, blant annet Meld. St. 9 (2022-2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet* og NOU 2015: 13 *Digital sårbarhet – sikkert samfunn og Nasjonal strategi for bruk av skytjenester* (2016). I tillegg har NSM løftet frem behovet for nasjonal kontroll i rapporter om tjenesteutsetting og bruk av skytjenester, som det også vises til i mandatet for denne utredningen. En vurdering av behov ut fra normative metoder og føringer knyttet til nasjonal kontroll finnes i behovskartleggingen i del 1 i vedlegg A.

Nasjonal kontroll er ikke et entydig definert begrep, men forstås i denne sammenhengen som et sett med virkemidler for å ivareta sikkerhet i lys av et skjerpet trussel- og risikobilde, ved å redusere risiko knyttet til lagring og behandling av data ved statsforvaltningens bruk av skytjenester. Virkemidlene skal redusere fremmede statlige aktørers mulighet til å påvirke norske interesser og redusere risiko for verdi-/leverandørkjedeangrep. Virkemidlene knyttet

³⁷ NOU 2019:9 *Fra kalveskinn til datasjø*, Kulturdepartementet, 2019

³⁸ Vedlegg B Rammebetingelser etter sikkerhetsloven og Vedlegg C Notat skytjenester Haavind

til nasjonal kontroll er nærmere redegjort for i vedlegg J og drøftet i mulighetsstudien og alternativanalysen.

FRED	KRISE	VÆPNET KONFLIKT
Sikre innbyggernes personvern og effektiv produksjon av offentlige tjenester med høy kvalitet.	Sikre tilgang til sentrale tjenester som er nødvendig for å håndtere situasjonen som har oppstått.	Sikre styringsdyktighet og et akseptabelt minimumsnivå av offentlig tjenesteproduksjon.
Eksempel Tilgang til korrekt informasjon for å effektivt levere sentrale tjenester som f.eks. strøm og vann.	Eksempel Tilgang på korrekt helsedata i en pandemi for å kunne prioritere vaksiner og korrekt behandling av alvorlig syke personer.	Eksempel Tilgang til systemer som sikrer at sivile samfunnsfunksjoner får understøttet forsvarsinnsatsen, samtidig som sivilbefolkningens sikkerhet og basisbehov dekkes.

Figur 3-3 – Eksempler på behov i ulike deler av krisespekteret

I fredstid har man et nasjonalt behov for å levere tjenester av høy kvalitet. Da er det avgjørende at de data og systemer som understøtter statens produksjon av tjenester er sikret slik at de er tilgjengelige og inneholder riktig informasjon til enhver tid. Ettersom stadig flere samfunnskritiske funksjoner, for eksempel leveranse av vann og strøm, i stor grad styres av IKT-systemer, er det et økende behov for å sikre disse systemenes tilgjengelighet og integritet.

I en krisesituasjon har man behov for å håndtere krisen, samtidig som andre tjenester i så liten grad som mulig påvirkes av dette. Innbyggerne har et behov for å kunne få tilgang til den informasjon de behøver, og at denne informasjonen er riktig. I en krisesituasjon er det i tillegg en risiko for at sentrale leverandører utsettes for økt press, fra politisk hold, men også fra hybride trusler. I en krisesituasjon kan også konsekvensene ved bortfall eller redusert kvalitet på sentrale tjenester øke. Det er derfor et særskilt behov for at leverandører som er sentrale i krisehåndteringen er i stand til levere tjenester med god kvalitet.

I væpnet konflikt har statsforvaltningen behov for å sikre styringsevne og handlefrihet, og ivareta et akseptabelt minimumsnivå av offentlig tjenesteproduksjon. En krig gjennomføres med både konvensjonelle og ukonvensjonelle midler, og cyberdomenet er en sentral arena.

Konsekvensene av at offentlige tjenester reduseres eller bortfaller, vil kunne være langt større i en krigssituasjon enn i en fredssituasjon. Det er derfor et sentralt behov for å ivareta kritiske systemer i en krigssituasjon. Det vil også være behov for å kunne gjenopprette data og systemer i fasen etter en væpnet konflikt.

Det overordnede behovet for å sikre beskyttelsesverdige data og systemer i hele krisespekteret medfører en rekke operasjonelle behov for å kunne ivareta en grad av nasjonal kontroll. Disse operasjonelle behovene er nærmere drøftet under.

3.1.1 Behov for kontroll over hvor data lagres og behandles

For å kunne sikre beskyttelsesverdige data og systemer i statsforvaltningen, har staten et behov for kontroll over hvor data lagres og behandles. For å kunne ivareta en høyere grad av nasjonal kontroll, er det nødvendig å stille krav om at beskyttelsesverdige data lagres og behandles på datasentre i Norge, for å sikre at data og systemer, og virksomhetene som

forvalter dem, er underlagt norsk jurisdiksjon. Jurisdiksjonsspørsmålet er helt sentralt med hensyn til nasjonal kontroll, fordi det er avgjørende for virkemidlene staten har til rådighet overfor leverandører. Dette fordrer at staten utnytter kapasitet på eksisterende datasentre i Norge, eller selv etablerer datasentre.

3.1.2 Behov for kontroll over hvem som har tilgang til data og systemer

Nasjonal kontroll over infrastruktur, data og systemer fordrer streng tilgangsstyring til en skytjeneste både i det fysiske og logiske domenet. Med styrt tilgang innen det fysiske domenet menes kontroll over hvem som har tilgang til den fysiske infrastrukturen, mens det logiske domenet handler om hvilket personell som har tilgang (eller fjerntilgang) til skytjenesten gjennom digitale verktøy (for eksempel via Internett). Logisk tilgang kan tilegnes gjennom arbeid med for eksempel programvareutvikling, driftsfunksjoner eller kundestøttefunksjoner.

Virksomheter i statsforvaltningen ble som en del av utredningen spurt om hvilke tjenester eller egenskaper de mener en nasjonal skytjeneste må kunne tilby. «Sikker drift og forvaltning av autorisert personell» var det alternativet som ble trukket frem som viktigst av respondentene. Over 90 prosent av virksomhetene fremhevet dette som nødvendig i "stor" eller "svært stor" grad.

For å sikre nasjonal kontroll må tilgangsstyringen sikre at personell med berettiget behov, som skal oppdatere og rette feil i systemer/programvare, eller utføre endringer på datasentrene, ikke får tilgang til mer enn nødvendig eller i en lengre tidsperiode enn det er behov for. For å kunne kontrollere tilganger og endringer kreves det overvåkings- og loggfunksjonalitet som registrerer aktivitet, samt at denne informasjonen er korrekt.

3.1.3 Behov for kontroll med leverandører og avhengigheter til utlandet

Digitale verdikjeder er ofte lange, komplekse og uoversiktlige, og omfatter mange ledd med leveranser av programvare, maskinvare og ulike digitale tjenester. Disse leveransene omfatter som regel oppdateringer og vedlikehold gjennom hele levetiden til produktet eller tjenesten og fører derfor til et avhengighetsforhold mellom leverandør og kunde. Tjenesteleverandører er attraktive mål for trusselaktører, både fordi skadepotensialet og ringvirkningene er store, og fordi det kan være lettere å kompromittere tjenesteleverandører lenger ute i verdikjeden enn å direkte angripe virksomheter som har iverksatt ulike sikkerhetstiltak for å beskytte sine verdier.³⁰

Dette medfører et behov for å ivareta kontroll med leverandører. Valg av leverandører må bygge på en risikobasert tilnærming som tar hensyn til eierskapsstrukturer og nasjonale/utenlandske tilknytninger i hele verdikjeden.

3.1.4 Behov for kontroll med maskinvare og programvare

Det vil være gjenstående avhengigheter til leverandører av grunnleggende IKT-produkter (maskinvare og programvare) som inngår i skytjenesten. For å ivareta en høyere grad av nasjonal kontroll er det som et minimum nødvendig å velge leverandører ut fra en risikobasert tilnærming som også tar hensyn til nasjonal tilknytning eller opprinnelsesland.

Det er videre behov for å oppnå tillit til og sikre integriteten i programvare og systemer slik at uautorisert tilgang ikke oppstår tilsiktet eller utilsiktet. Det betyr for eksempel at en oppdatering til en nyere programvareversjon ikke gir uautorisert personell tilgang til

systemer. Integritet i programvare og systemer kan undersøkes og verifiseres gjennom tekniske tiltak, men dette fordrer betydelig IKT-teknisk kompetanse og ressurser. I forlengelse av dette vil det være behov for å sikre at utregninger, beregninger eller forslag som disse programmene eller systemene gir, er riktige og ikke påvirket av bevisste eller ubevisste feil i underliggende algoritmer.

3.1.5 Behov for et høyt nivå av generell IKT-sikkerhet

Kravene til tilgjengelighet og integritet for de beskyttelsesverdige dataene og systemene fordrer et høyt nivå av generell IKT-sikkerhet. Et høyt nivå av generell IKT-sikkerhet er en nødvendig, men ikke tilstrekkelig betingelse for en høyere grad av nasjonal kontroll. Det er et behov for at sikkerhetsbrudd raskt blir oppdaget og korrigert, og for at tjenestene raskt kan gjenopprettes.

For å sikre dette er det nødvendig å finne gode tekniske og administrative løsninger som bidrar til å redusere nedetid og som opprettholder tilgangen og integriteten til tjenestene. Dette vil igjen kunne medføre særegne krav til funksjoner eller tiltak som redundans, sikkerhetskopi og gjenoppretting, autentisering, deteksjon, robustheten til tjenestene og ikke-forstyrrende vedlikehold eller liknende.

For å etablere og opprettholde et høyt sikkerhetsnivå er man avhengig av personell med god sikkerhetsfaglig kompetanse innen digital sikkerhet. Dette inkluderer fagområder som IT/IKT-drift og overvåking, nettverkssikkerhet, inntrengningstesting, kryptografi og autentisering samt kommunikasjonsteknologi og protokoller. I tillegg kommer fagområdene beredskap, administrasjon og virksomhetsstyring (Governance, Risk and Compliance - GRC) og anskaffelser som alle understøtter et høyt sikkerhetsnivå.

3.1.6 Behov for beredskapstiltak knyttet til beskyttelsesverdige data

Uavhengig av konsept vil det være behov for å etablere beredskapstiltak for å ivareta evnen til å flytte beskyttelsesverdige data til andre datasentre og om nødvendig ut av landet i en krise eller væpnet konflikt. Samtidig vil det være behov for å ivareta evnen til å gjenopprette en nasjonal skytjeneste også etter en væpnet konflikt eller okkupasjon, hvor tidligere datasentre og infrastruktur har blitt ødelagt - enten som en konsekvens av fiendtlige ødeleggelser eller på grunn av nødmakulering.

For å kunne flytte og gjenopprette funksjoner ved en eskalering i krisespekteret har man behov for oversikt over hvor beskyttelsesverdige data lagres, behandles og driftes fra. Det vil også være behov for å inngå avtaler med utvalgte samarbeidspartnere i andre land for å kunne gjennomføre en slik flytting og gjenoppretting.

3.2 Behov for å utnytte mulighetene som ligger i moderne skytjenester

I statens digitaliseringsstrategi for offentlig sektor er det uttalt:

«Digitalisering av offentlig sektor skal gi en enklere hverdag for innbyggere, næringsliv og frivillig sektor gjennom bedre tjenester, mer effektiv ressursbruk i offentlige virksomheter og legge til rette for produktivitetsøkning i samfunnet.

Hensikten med strategien er å understøtte digital transformasjon i hver enkelt virksomhet, og i offentlig sektor som helhet.»³⁹

Strategien skaper en klar forventning om at offentlig sektor skal tilby gode digitale tjenester og at disse fortløpende skal utvikles i tråd med mulighetene som åpnes gjennom den teknologiske utviklingen. Selv om statsforvaltningen har investert mye i digitalisering, er det fortsatt store muligheter for å forbedre tjenester og effektivisere daglig drift.

Koronapandemien er et eksempel på en hendelse som bidro til økt digitalisering som følge av at mange virksomheter ble tvunget til å utvikle og ta i bruk digitale verktøy meget raskt for å kunne samhandle bedre. En undersøkelse gjennomført av Statistisk sentralbyrå⁴⁰ viser at cirka 75 prosent av statsforvaltningen og kommuner sier de har hatt en økning i satsningen på å utvikle digitale tjenester under koronapandemien.

Som et ledd i denne utviklingen forventer statsforvaltningen økt bruk av skytjenester framover.⁴¹ Behov for flere, bedre og mer digitaliserte offentlige tjenester øker statsforvaltningens etterspørsel etter mer kapasitet, ytelse og tjenesteutvikling. Omfanget av informasjon som behandles, lagres og deles internt i og på tvers av statsforvaltningen blir stadig større, noe som øker virksomhetenes behov for fleksible og kostnadseffektive IKT-løsninger. Skalerbarheten ved skytjenester gir fleksibilitet til virksomheter med voksende eller varierende behov for lagringsplass, prosesseringskraft, eller for eksempel ved håndtering av et stort antall samtidige brukere. Samtidig har mange av disse virksomhetene teknisk gjeld⁴² og begrenset med kompetanse og kapasitet til å videreutvikle eksisterende IKT-infrastruktur og -systemer. Mange virksomheter opplever derfor at skyleverandørene har bedre løsninger enn de selv kan tilby. For å imøtekomme behovet for modernisering oppfordrer dessuten Digitaliseringsrundskrivet virksomhetene til å benytte skyteknologi der det er mulig.⁴³

Disse behovene treffer også beskyttelsesverdige data og systemer. Både fordi det er et selvstendig behov for å modernisere de systemene som innehar og bruker beskyttelsesverdige data, men også fordi det ofte er store avhengigheter på tvers av de ulike systemene i virksomheten. To tredeler av de statlige virksomhetene som svarte på spørreundersøkelsen oppga at det var middels eller stor grad av avhengigheter og integrasjoner mellom de beskyttelsesverdige systemene og andre IKT-systemer. Det inkluderer også skytjenester. Over tid kan vi derfor forvente at en betydelig del av de beskyttelsesverdige dataene og systemene i statsforvaltningen, vil flyttes ut i skyen i sin helhet eller være tilknyttet andre skybaserte systemer.

Det brukes allerede i dag store ressurser på skytjenester i statsforvaltningen. Dette er en måte å effektivisere drift og samtidig skape mer forutsigbarhet. Med antakelse om at 40 prosent av de statlige virksomhetenes data og systemer allerede er i sky i dag⁴⁴, kan vi grovt

³⁹ En digital offentlig sektor (2019)

⁴⁰ <https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/okt-digitalisering-i-offentlig-sektor-som-folge-av-koronapandemien>

⁴¹ Kartlegging av drift og forvaltning av IKT-løsninger i Staten, Kommunal- og distriktsdepartementet (A-2 Norge), jan 2022

⁴² A-2 Norge (2019): *Evalueringsrapport av IT-tilstanden i statlige virksomheter*

⁴³ Digitaliseringsrundskrivet (ver. 2022), [Regjeringen.no](https://regjeringen.no)

⁴⁴ Beskrivelse av analysene finnes i vedlegg G.

anslå at 40 prosent av de totale IKT-kostnadene er knyttet til data og systemer som er i lukkede eller allmenne skyløsninger. Dette vil si omtrent 5 milliarder kroner.⁴⁵

Virksomhetene i statsforvaltningen kan oppnå en rekke positive effekter ved å flytte data og tjenester ut i en skyløsning. En årlig undersøkelse rettet mot europeiske virksomheter viser at økt fleksibilitet, kostnadsreduksjon, optimalisert drift, modernisering av IKT-porteføljen, og raskere utvikling er viktige kriterier når man vurderer om en virksomhet skal ta i bruk skytjenester.⁴⁶ Svarene på spørreundersøkelsen viser at de statlige virksomhetene er opptatt av de samme virkningene. Dette er sterke drivere for å videreføre overgangen fra IKT-tjenester på egendriftet plattform til skybaserte tjenester. Behovet for et bredt spenn av skytjenester og løsninger som ivaretar behovet for fleksibilitet og kapasitet, er stort. Dette presenteres nærmere i de neste to kapitlene.

3.2.1 Behov for et bredt tjenestetilbud

Statsforvaltningen har ulike samfunnsoppdrag og leverer et bredt spenn av tjenester. De 1855 statlige virksomhetene som i utgangspunktet er målgruppen for en nasjonal skyløsning, spenner fra små tilsynsmyndigheter til store operative etater. Både virksomhetens størrelse, digital modenhet og type tjenester virksomheten leverer, kan påvirke hvilket behov de har for å ta i bruk ulike skytjenester. Alle virksomheter som behandler beskyttelsesverdige data, vil ha behov for å lagre og behandle disse på en rasjonell og trygg måte.

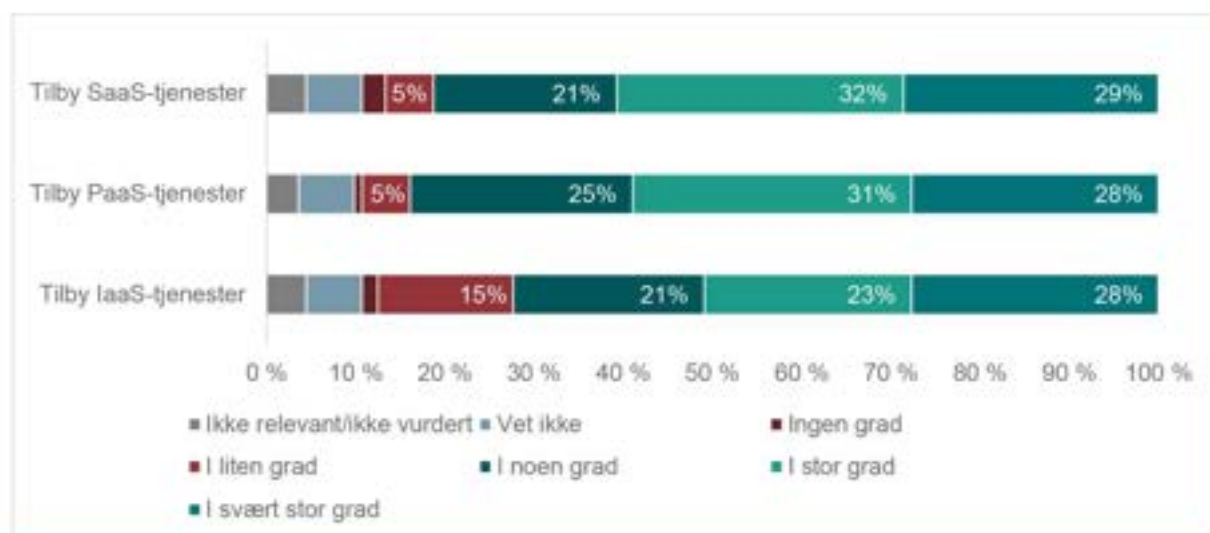
Det er et (grunnleggende) behov knyttet til informasjonssikkerhet, tjenestekvalitet og konkurransedyktige kostnader. Behovet går igjen hos mange, men det er i tillegg et betydelig spekter av øvrige tjenestebehov. Dette spennet av tjenester kan dekke alt fra kjøp av lagringsplass, via ulike plattformtjenester, til bruk av standard hyllevare.

Det er videre et behov for å kunne ha tilgang til og benytte både enkle og avanserte skybaserte tjenester. Enkelte har kun behov for standardtjenester, som for eksempel videokonferanse eller samhandlingsplattformer. Andre kan ha et behov for mer avanserte løsninger, som for eksempel krever tilgang til en utviklingsplattform med ledende verktøy og kodebiblioteker for AI-applikasjoner. Flertallet av virksomhetene benytter spesialutviklede fagsystemer som er aktuelle å legge på en skyplattform, og mange av disse inneholder beskyttelsesverdige data. Det er derfor viktig at det er mulig for hver enkelt virksomhet å ha et tilstrekkelig bredt spekter av tjenester å velge fra, og at disse er satt sammen på en slik måte at det dekker deres behov i forbindelse med egen tjenesteproduksjon.

For å få bedre innsikt i hvor hovedvekten av tjenestebehovene knyttet til beskyttelsesverdige data og systemer ligger, spurte vi i spørreundersøkelsen hvilke tjenester og egenskaper virksomhetene mener en nasjonal sky må kunne tilby. Svarene bekrefter at virksomhetene har behov for ulike skytjenester på ulike tjenestenivåer. Figuren under viser at over halvparten av virksomhetene svarte at de mente en nasjonal sky i stor eller svært stor grad må kunne tilby SaaS-, PaaS- og IaaS-tjenester.

⁴⁵ Tallene er hentet fra Statsregnskapet for 2021. Disse kostnadene inkluderer blant annet leie av datasystemer og servere, kjøp av konsulenttjenester til utvikling og anskaffelse av programvare, men tar ikke høyde for bruk av interne IKT-ressurser. Kun 70 prosent av de 185 statlige virksomhetene er en del av statsregnskapet, vi har dermed oppjustert IKT-kostnadene for å dekke de resterende virksomhetene. Se flere detaljer i vedlegg G.

⁴⁶ Basefarm Cloud Report 2021



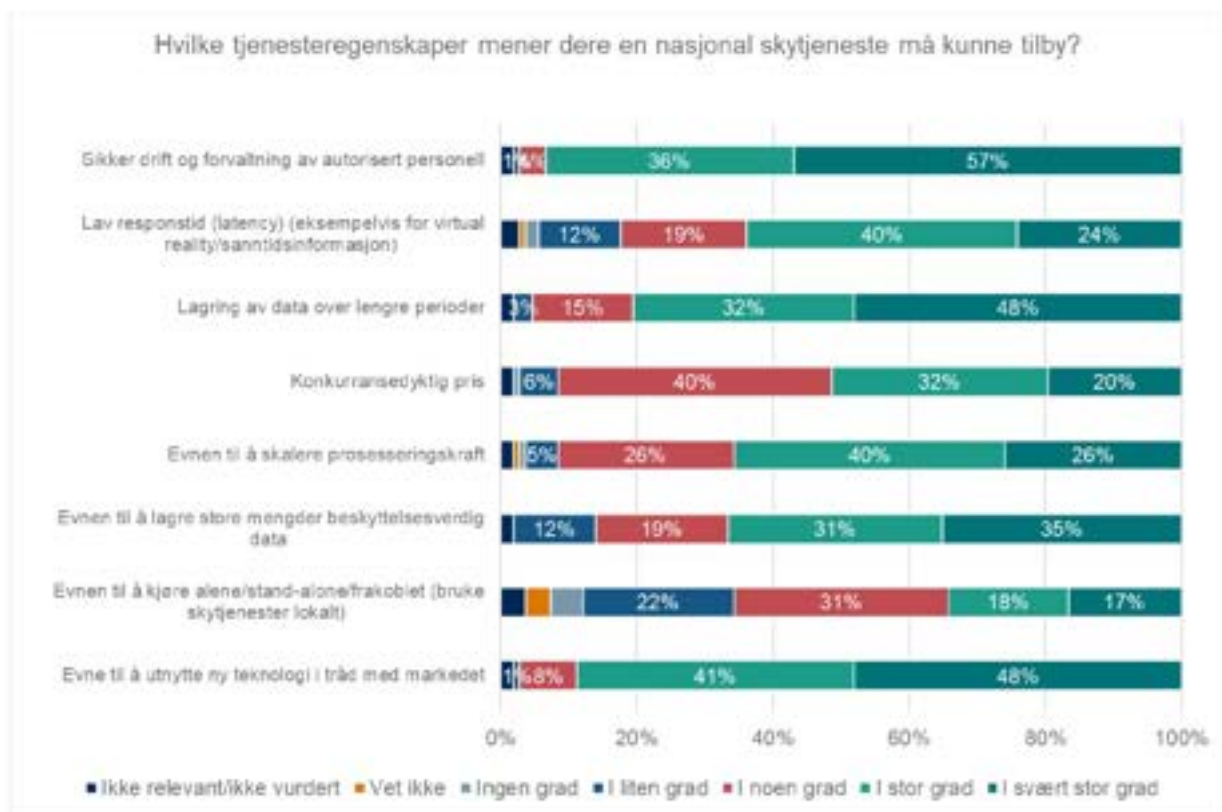
Figur 3-4 - Utdrag av svaralternativer fra spørsmålet "Hvilke typer tjenester mener dere en nasjonal skytjeneste må kunne tilby? (kryss av for alle rader)

Spørreundersøkelsen ba også om mer konkrete vurderinger av hvilke tjenesteegenskaper virksomheten hadde størst behov for.

Svarene viser at de viktigste behovene virksomhetene må ha dekket i en nasjonal skyløsning, hvor de svarer stor eller svært stor grad av relevans, er:

- Sikker drift og forvaltning (93 prosent)
- Lagring av data over lengre perioder (80 prosent)
- Evne til å utnytte ny teknologi (89 prosent)
- Evne til å skalere prosesseringskraft (64 prosent)

Svarene gjengitt i figuren nedenfor, viser at egenskapene har stor eller svært stor betydning for mer enn halvparten av virksomhetene, og underbygger behovet for å ha et allsidig tjenestetilbud og konkurransedyktige egenskaper.



Figur 3-5 Utdrag av svaralternativer fra spørsmålet "Hvilke tjenester/egenskaper mener dere en nasjonal skytjeneste må kunne tilby?"

3.2.2 Behov for funksjonelle og fleksible egenskaper

På samme måte som det er et behov for et bredt tjenestetilbud, har virksomhetene også behov for at disse tjenestene besitter funksjonelle og fleksible egenskaper som kan tilpasses den situasjon virksomhetene til enhver tid befinner seg i. Eksempler på slike egenskaper er robusthet, utviklingsmulighet, ytelse og kapasitet. Dette er egenskaper som gjelder både for beskyttelsesverdige og ikke-beskyttelsesverdige data. Virksomhetene oppgir selv at rundt 60 prosent av deres data kan kategoriseres som beskyttelsesverdig, men behovet for beskyttelse varierer og usikkerheten er stor, både knyttet til volumer og beskyttelsesbehov. Av den grunn er det et stort behov for løsninger med fleksible egenskaper.

Behovet for robusthet kan omfatte en rekke forhold. Det kan innebære redundante løsninger som gjør at nedetiden for løsningene i praksis blir null, men også økt mulighet for å gjenopprette systemer. Robuste løsninger har stor motstandsdyktighet ved ondsinnede angrep, og må være meget fleksible for å kunne tilpasse seg nye trusler og angrepsmåter.

Behovet for å kunne følge teknologiutviklingen innebærer at virksomhetene drar nytte av de mulighetene som oppstår. Den teknologiske utviklingen går raskt og de store skyaktørene har stor innovasjons- og utviklingskraft. Det krever en betydelig fleksibilitet for raskt å kunne utvikle og ta i bruk nye skytjenester.

Behovet for større ytelse, økt kapasitet eller dynamisk skalering av en tjeneste, er en annen form for utvikling. Statsforvaltningen har ulike behov for ytelse og kapasitet avhengig av mengden data de besitter og hvilken type data det er. Behovet for kapasitet vil variere

både mellom virksomhetene og over tid. Behovet for ulike typer av ytelser og kapasiteter er ofte knyttet til lagringstjenester, prosesseringskraft og nettverkskapasitet.

Behovet for fleksible lagringstjenester er stort, og behovet forventes å øke betydelig i årene som kommer. Mange virksomheter har utfordringer med å håndtere store datavolumer, og uten et godt og effektivt regime for datalagring blir det vanskelig å utnytte det fulle potensialet av verdien til de store datamengdene. I tillegg er det en utvikling mot at dataelementer blir mer fingranulerte og dette øker behovet for lagringskapasitet. For eksempel har geografiske data et stadig økende detaljnivå, bilder har høyere kvalitet og bruken av sensorer og satellitter produserer en kontinuerlig strøm av enorme mengder med data.

I spørreundersøkelsen trekker 85 prosent av virksomhetene frem «evnen til å lagre store mengder beskyttelsesverdig data» som en viktig egenskap i en nasjonal skytjeneste. Åtte av ti virksomheter svarte at lagring av data over lengre perioder var noe en nasjonal skytjeneste måtte tilby i «svært stor grad» eller «stor grad» (ref. figur over).

Behovet for fleksibel prosesseringskraft oppstår gjerne når mange samtidige brukere benytter applikasjoner som trekker på samme infrastruktur. Da er det avgjørende at serverparken kan håndtere denne belastningen. Dersom prosesseringskapasiteten ikke møter behovet, vil brukerne oppleve treghet, forsinkelser, avbrudd og produktivitetstap.

Flere statlige virksomheter har behov for å gjøre analyser av store datavolumer. Virksomhetene deler mye data seg imellom og data kan komme fra en rekke ulike datakilder, både nasjonale og internasjonale. Slike analyser gir virksomhetene mulighet til å finne nye sammenhenger som tidligere ikke har vært mulig å kartlegge. I intervjuer har virksomhetene indikert at dette behovet vil øke fremover. Enkelte av slike analyser krever betydelig prosesseringskraft. Slike løsninger kan være svært kostbare å anskaffe, drifte og forvalte. En utfordring er at slike løsninger tidvis kan ha lav utnyttelsesgrad. Det vil derfor være et behov for at virksomhetene kan samarbeide og dele tilgangen på slike ressurser, så ikke hver enkelt virksomhet trenger å anskaffe, drifte og forvalte slike løsninger selv.

Behovet for tilstrekkelig og fleksibel nettverkskapasitet innebærer at datanettverk kan håndtere økte trafikkvolumer, både som en konsekvens av mange samtidige brukere og når datavolum må kunne transporteres raskt over nettverket. Mange virksomheter opplever forskjellige bruksmønstre på sine tjenester. Noen har jevn trafikk mot sine tjenester og nettsider, mens andre vekselvis har perioder med svært høy trafikk og lange perioder med lite trafikk. Dersom nettverkskapasiteten ikke møter dette behovet, vil virksomhetene oppleve treghet, forsinkelser, avbrudd, nedsatt brukeropplevelse og produktivitetstap. Flere virksomheter bruker data eller leverer data til systemer som er avhengige av å gjøre beregninger i sanntid. I slike systemer er det ikke bare viktig at beregningene er riktige, men at de også kan gjøres raskt.

Behov for skalering av kapasiteter. Behovet for å kunne tilpasse lagrings-, prosesserings- og nettverkskapasiteten til varierende trafikk kan oppsummeres som et behov for en fleksibel skalering. Dersom virksomheten dimensjonerer sin kapasitet for å kunne håndtere tjenestekvalitet i perioder med høyest trafikk, kan dette innebære unødvendig stor ressursbruk og høye kostnader. For å kunne drive kostnadseffektivt har de derfor et behov for kunne skalere kapasitet både ned og opp i slike perioder.

Virksomhetene ønsker en skyløsning som innebærer en automatisk og dynamisk skalering uten at de må iverksette tiltak i sine egne løsninger. Behovet understøttes av svarene i spørreundersøkelsen, både direkte ved at en majoritet mener skalering av kapasitet er en sentral egenskap ved en eventuell nasjonal skytjeneste, men også indirekte ved at det er en forutsetning for å kunne levere tjenester med den kvalitet som forventes.

Behov for å definere infrastruktur som kode. For å utnytte egenskapene beskrevet over på en hensiktsmessig og effektiv måte vil også virksomhetene ønske å ta i bruk moderne skyløsninger sin evne til å administrere infrastruktur og ressurser i skyen ved å beskrive disse i kode.⁴⁷ Dette muliggjør automatisering og effektivisering av konfigurasjon og etablering av nye miljøer og ressurser i skyen og kan dermed redusere tidsbruk og ledetid for digitalisering av tjenester.

Behov for å ta i bruk moderne arbeidsmetodikk. Å ta i bruk skytjenester er mer enn bare teknologi. Enkelte aktører viser til at potensialet som ligger i å ta i bruk denne teknologien først maksimeres når man også klarer å ta i bruk smidige og transformativ leveranse- og arbeidsmetoder (Agile og DevOps/DevSecOps). I dette ligger det at tidligere operasjonsmodeller forbedres eller erstattes av mer moderne måter å utvikle, drifte og kvalitetssjekke tjenester på. Det vil også være et behov å kunne utvikle tjenester som ansees å være *cloud native*. Altså tjenester som, allerede fra starten av, er designet for bruk i sky.

⁴⁷ 12 Ways Cloud Upended IT Security (And What You Can Do About It), CSA, mars 2019

4 Strategiske mål

Samfunnsmålet for utredningen er «Sikker og effektiv lagring og behandling av beskyttelsesverdige data og systemer i statlige virksomheter». Det er også utformet tre effektmål: E1 – Tilgjengelighet, integritet og konfidensialitet ivaretas for beskyttelsesverdige data og systemer i fred, krise og krig. E2 – Statsforvaltningen får tilgang til kostnadseffektive skytjenester med relevant funksjonalitet og tjenestenivå. E3 – Statsforvaltningens skytjenester kan skaleres og tilpasses virksomhetenes kapasitets-, ytelses- og tjenestebehov og gi muligheter for utnyttelse av ny teknologi.

De strategiske målene i KVUen skal gi en klar retning for mulighetsstudien ved å tydeliggjøre det overordnede formålet med prosjektet og spesifisere hvilke virkninger som ønskes utløst.

4.1 Samfunnsmål

Samfunnsmålet skal reflektere hvilken samfunnsutvikling prosjektet skal bygge opp under og er knyttet til tiltakets virkninger for samfunnet som helhet. Basert på identifiserte problem og behov har vi formulert følgende samfunnsmål for utredningen:

«Sikker og effektiv lagring og behandling av beskyttelsesverdige data og systemer i statlige virksomheter»

Sikkerhetsaspektet i samfunnsmålet er rettet inn mot å ivareta behovet for nasjonal kontroll og et tilstrekkelig digitalt sikkerhetsnivå for å sikre samfunnskritiske verdier og funksjoner i hele krisespekteret. Det innebærer at løsningene tilbyr sikker databehandling og -lagring både i fred, krise og krig. Å sikre dataenes tilgjengelighet, integritet og konfidensialitet der det er nødvendig vil bidra til å trygge samfunnskritiske funksjoner for norske borgere.

Å sørge for at statsforvaltningen har tilgang til effektive skyløsninger vil fremme den videre digitaliseringen av statlig sektor og bygge opp under deres evne til å levere relevante tjenester av høy kvalitet til en tilfredsstillende kostnad. Effektivitetsaspektet ved samfunnsmålet omfatter derfor en målsetning om både kostnadseffektive løsninger og tilstrekkelig funksjonalitet til å understøtte en effektiv tjenesteproduksjon.

Samfunnsmålet er rettet mot beskyttelsesverdige data og systemer i statsforvaltningen og gir en tydelig avgrensning av det relevante omfanget for en eventuell løsning. Avgrensningen følger av mandatet, men utelukker ikke at andre deler av offentlig forvaltning kan benytte seg av løsningen dersom det er hensiktsmessig.

4.2 Effektmål

Effektmålene er knyttet opp til de forventede nyttevirkningene av tiltaket og gjenspeiles i de samfunnsøkonomiske virkningene i alternativanalysen. For å oppfylle samfunnsmålet må følgende effektmål være oppfylt:

Effektmål	Indikatorer for måloppnåelse
E1: Sikkerhet: Tilgjengelighet, integritet og konfidensialitet ivaretas for beskyttelsesverdige data og systemer i fred, krise og væpnet konflikt (omfatter ikke sikkerhetsgradert informasjon).	Reflekteres i fravær av avvik fra anerkjente standarder og rammeverk i interne og eksterne sikkerhetsrevisjoner eller tilsyn, og i antall uønskede hendelser knyttet til brudd på tilgjengelighet, integritet og konfidensialitet.
E2: Effektivitet: Statsforvaltningen får tilgang til kostnadseffektive skytjenester med relevant funksjonalitet og tjenestenivå.	Reflekteres i virksomhetenes brukerkostnader i form av tjenestepris, tilpasningskostnader og virkninger på produksjon av tjenester som beskyttelsesverdige data og systemer understøtter (effektivitet og kvalitet).
E3: Fleksibilitet: Statsforvaltningens skytjenester kan skaleres og tilpasses virksomhetenes kapasitets-, ytelses- og tjenestebehov og gi muligheter for utnyttelse av ny teknologi.	Reflekteres i hvor enkelt nye tjenester kan utvikles, forbedres eller legges til og konseptets evne til å skalere (både per bruker og med mengde data).

Det første effektmålet, sikkerhet, reflekterer det overordnede behovet for å ivareta tilstrekkelig nasjonal kontroll over beskyttelsesverdige data og systemer. Det reflekterer også behovet for løsninger basert på en helhetlig tilnærming til digital sikkerhet, med nødvendige sikkerhetstiltak og i tråd med overordnede føringer fra NSM og andre myndigheter. Konkret skal tilgjengelighet, integritet og konfidensialitet for disse dataene og systemene ivaretas i tilstrekkelig grad. Effektmålet spesifiserer at målet skal gjelde i hele krisespekteret, det vil si i fredstid så vel som i en sikkerhetspolitisk krise eller væpnet konflikt. Det presiseres at skjermingsverdig gradert informasjon ikke omfattes av denne utredningen.

Det andre effektmålet, effektivitet, reflekterer behovene for å støtte opp om den videre effektiviseringen og digitaliseringen av offentlig sektor. Det innebærer at statsforvaltningen får tilgang til en tjenestebredde og et tjenestenivå tilpasset den enkelte virksomhets behov for funksjonalitet, og det til en pris som kan konkurrere med eksisterende alternativer. Effektmålet må derfor tolkes som et todelt mål om å både imøtekomme behovet for kostnadseffektivitet i selve løsningene og behovet for løsninger som bidrar til at norsk statlig sektor kan drive en mest mulig effektiv tjenesteproduksjon.

Det tredje effektmålet, fleksibilitet, reflekterer behovet for å ruste statsforvaltningens IKT-infrastruktur for fremtiden, ved å ivareta tilstrekkelig fleksibilitet til å skalere tjenestene etter endrede behov knyttet til kapasitet, ytelse og tjenestenivå – og ikke minst ved å utnytte innovasjonskraften i markedet til å ta i bruk fremtidens teknologiske løsninger. Dette er avgjørende for å sikre at løsningen holder seg relevant og bidrar til økt sikkerhet og effektivitet over tid.

4.3 Mulige målkonflikter og prioritering av effektmål

Effektmålene spesifisert ovenfor er ikke binære, men kan oppnås i ulik grad. Det vil si at det ikke er satt konkrete terskelverdier for nødvendig måloppnåelse konseptene må oppfylle. Det er heller ikke gjort en prioritering mellom de ulike effektmålene. Hva som er den mest hensiktsmessige graden av måloppnåelse av hvert effektmål vil styres av hva som gir høyest oppnåelse av samfunns målet, vurdert ut ifra konseptenes samfunnsøkonomiske

lønnsomhet. Det innebærer en avveining mellom hensynet til behovet for kontroll/sikkerhet (E1), og behovet for funksjonalitet, kostnadseffektivitet (E2) og fleksibilitet (E3). I denne avveiningen kan det ligge mulige målkonflikter mellom de ulike effektmålene. Høy grad av nasjonal kontroll og sikkerhet kan for eksempel gå utover målsetningene om effektivitet og fleksibilitet og vice versa. Hvilke av disse hensynene som bør prioriteres høyest vil være avhengig av hvilke virkninger ulike grader måloppnåelse gir.

At det er mulige «konflikter» mellom de forskjellige effektmålene er ikke et problem i seg selv. Derimot tydeliggjør det sentrale avveininger som vurderes nærmere i mulighetsstudien og alternativanalysen. En viss grad av måloppnåelse av alle de tre effektmålene er imidlertid en forutsetning for å nå samfunns målet og oppnå de ønskede effektene.

Effektmålene er ikke utformet med tanke på en operativ styring av tiltaket. I forprosjektfasen vil resultatmål knyttet til blant annet tid, kost og kvalitet defineres, og det er disse målene som skal benyttes for å sikre en operativ styring. Indikatorene for effektmålene kan imidlertid benyttes for å følge en utvikling i retning av oppnåelse av effektmålene og for å verifisere at konseptets formål er i varetatt.

4.4 Sammenheng med andre overordnede målsetninger

Både den nasjonale strategien for bruk av skytjenester og kravene i Digitaliseringsrundskrivet har de siste 5-6 årene medført føringer og press på at statlige (og kommunale) virksomheter skal øke sin bruk av skytjenester. Det fastslås at bruk av skytjenester kan gi økt fleksibilitet og mer kostnadseffektiv bruk av IKT, men at særlige krav til sikkerhetsvurderinger kan være til hinder for bruk av skytjenester. Det skal videre være en forutsetning at valgt løsning tilfredsstiller virksomhetens krav til informasjonssikkerhet. Føringerne i Digitaliseringsrundskrivet er således rettet mot enkeltvirksomhetene. Målene i denne KVUen er både rettet mot de enkelte virksomhetene, men tar også høyde for en utvikling innen statsforvaltningen som helhet. Dette gjelder spesielt effektmål E1 om nasjonal kontroll. Dette målet må sees i sammenheng med at Norge utsettes for et økende trusselbilde. Dette er omtalt en rekke steder i denne KVUen. Vi legger også innholdet i Meld. St. 9 (2022 – 2023) Nasjonal kontroll og digital motstandskraft, til grunn. Videre er det i Vedlegg A under normative metoder omtalt en rekke dokumenter som gir rammene for gjennomføringen. Det vil si at målene både må møte utfordringene knyttet til nasjonal kontroll, kostnadseffektivitet og fleksibilitet.

I forbindelse med utformingen av målene er disse blitt presentert og drøftet i møter med prosjekteierne (JD og KDD), samt i møter med referansegruppen som er sammensatt av representanter for en rekke offentlige virksomheter.

5 Rammebetingelser for konseptvalg

Det er identifisert en rekke rammebetingelser en nasjonal sky må ivareta. De viktigste av disse er rammebetingelser som legger begrensninger på hvilke leverandører som kan benyttes og hvor data lagres og behandles. Videre er det også rammebetingelser i regelverk om offentlige anskaffelser og statsstøtte.

Rammebetingelser skal tydeliggjøre hvilke betingelser som må oppfylles for valg av konseptuell løsning. De kan enten utledes av samfunns- og effektmålene eller relateres til andre ikke-prosjektspesifikke mål og prinsipielle spørsmål.

Som beskrevet i kapittelet ovenfor er det ikke satt noen eksplisitte krav eller terskelverdier for nødvendig måloppnåelse konseptene må oppfylle. Det innebærer at det heller ikke følger noen konkrete rammebetingelser som kan utledes direkte fra de strategiske målene. Det er imidlertid en rekke lover som setter rammer for hvilke konsepter som er relevante og hvilke egenskaper de kan ha.

For å kartlegge mulige rammebetingelser er det foretatt en gjennomgang av regelverk som kan få betydning for hvordan konseptene utformes og på hvilken måte. Som det fremgår av vedlegg C punkt 1.2 er ikke skytjenesteleverandører eller datasentre underlagt egne lovkrav i Norge. Det er i hovedsak vanlige krav til forvaltningens virksomhet, sektorlovgivning, generelle krav til personvern og informasjonssikkerhet og kundens kontraktsfestede krav som regulerer tjenestene og aktørene. Med unntak for sikkerhetsloven er det heller ikke særskilte krav til sikring, lokalisering eller eierskap.

Gjennomgangen viser likevel at det eksisterer en rekke regelverk som vil kunne påvirke etablering og drift av en nasjonal skytjeneste, blant annet knyttet til offentlige anskaffelser, personvern og krav til forvaltningens virksomhet, se vedlegg C punkt 1.2. Flere lover inneholder også krav til for eksempel sikkerhet, beredskap, konfidensialitet, integritet og tilgjengelighet som har implikasjoner for bruk og utforming av skytjenester. Gjennomgangen tar for seg gjeldende rett, men det vises til enkelte kommende regelverksendringer som kan få betydning for nasjonal skytjeneste.

De identifiserte rammebetingelsene presenteres i vedlegg B og C. De mest relevante gjengis under.

5.1 Rammebetingelser knyttet til leverandører og behandling av data

Skytjenester er i mange tilfeller levert av utenlandske selskaper og driftet helt eller delvis fra andre land enn Norge. Selv om data er lagret innenfor Norges grenser, kan tjenester og tilganger til systemene og dataene være helt eller delvis fra utlandet. Lovgivning kan gjelde både innenfor og utenfor statens territorium og på den måten ha ekstraterritorial virkning, se vedlegg C punkt 3.5. Lovverk kan gi myndighetene rett til tilgang til data i nasjonale selskapers systemer, også dersom behandlingen og lagringen foregår utenfor det aktuelle landet. Leverandøren kan også være underlagt forbud mot å informere den norske kunden om utleveringen. USA har for eksempel slike regler, samt mange europeiske land og Norge. En kontraktsfestet taushets- og konfidensialitetsplikt vil i mange tilfeller ikke være tilstrekkelig for å hindre utlevering av data til utenlandske myndigheter. Spørsmål knyttet til jurisdiksjon

er derfor særlig relevant for bruk av skytjenester, spesielt ved bruk av leverandører fra andre land. Det vises til vedlegg C punkt 3 for redegjørelsen av jurisdiksjonsspørsmålet.

5.1.1 Begrensninger på bruk og valg av leverandører

Statsforvaltningen er underlagt sikkerhetsloven, se § 1-2. Ettersom en nasjonal skyløsning skal inkludere skjermingsverdig informasjon og informasjonssystemer, gjelder lovens bestemmelser om informasjons- og informasjonssystemsikkerhet. Sikkerhetslovens bestemmelser om objekt- og infrastrukturens sikkerhet vil komme til anvendelse på hele eller deler av en nasjonal skyløsning dersom denne utpekes som skjermingsverdig infrastruktur eller objekt. Det skal foretas en vurdering av risiko for å avgjøre hvilke tiltak som er nødvendige for å beskytte objektet eller infrastrukturen og for å opprettholde et forsvarlig sikkerhetsnivå, jf. sikkerhetsloven § 7-3. De konkrete beskyttelsestiltakene som kan utledes av risikovurderingen, vil kunne påvirke hvordan konseptene utformes, herunder medføre begrensninger i bruk av utenlandske leverandører. Se nærmere om sikkerhetsloven i vedlegg B.

Reglene i personopplysningsloven om overføring av personopplysninger til land utenfor EØS (tredjeland) vil i praksis innebære skranker for bruk av skytjenester og leverandører fra utlandet, se vedlegg C punkt 5.1. Selv om personopplysningene lagres og behandles nasjonalt, vil reglene om overføring av personopplysninger til tredjeland blant annet komme til anvendelse dersom leverandøren eller underleverandører til skytjenesten har tilgang til personopplysninger fra et tredjeland og ved pålegg om utlevering fra myndigheter utenfor EØS.

Reglene om forvaltningens taushetsplikt etter forvaltningsloven eller særlovgivning utgjør ikke en direkte rettslig hindring for å benytte skytjenester i statsforvaltningen, men stiller krav til bruk og tiltak som kan ha betydning for nasjonal skyløsning, se vedlegg C punkt 4.4. For eksempel vil taushetsplikten være brutt hvis uvedkommende får innsyn i informasjonen. Forvaltningsloven legger derfor klare begrensninger på hvem som kan ha tilgang til de taushetsbelagte opplysningene.

Taushetspliktregler vil også kunne begrense bruken av leverandør eller underleverandør. En tjenesteleverandør kan i tillegg være underlagt lovgivning i hjemlandet som pålegger vedkommende å utlevere data til egne myndigheter, samt forbud mot å informere den norske kunden. Utlevering av taushetsbelagt informasjon vil derfor kunne skje uten norske kunders og myndigheters kunnskap, og uten at man har fått vurdert lovligheten etter norsk rett.

5.1.2 Begrensninger på hvor data lagres og behandles

Statlige organer er underlagt arkivplikt etter arkivloven. Arkivloven har bestemmelser som innebærer rettslige skranker for bruk av skytjenester, se vedlegg C punkt 5.3. Det mest sentrale er lovens forbud mot å føre arkiv ut av landet, jf. arkivloven § 9b, og som vil innebære en hindring for bruk av skyløsning med lagring på servere i utlandet. Dette gjelder både papirarkiv og lagring av digitalt arkivmateriale.

Innen flere sektorer er det også lovbestemte regler om tilsyn som forutsetter at den statlige tilsynsmyndigheten får tilgang til informasjon, se vedlegg C punkt 4.9. Tilsyn kan være stedlig, se for eksempel arkivloven. Det kan stilles spørsmål om kravene til tilsyn kan

oppfylles hvis forvaltningsorganet benytter skytjenester med lite kontroll over hvor data lagres og behandles, og særlig hvis data lagres i utlandet.

Regnskaps- og bokføringslovgivningen inneholder regler som i praksis innebærer rettslige skranker for bruk av skytjenester, se vedlegg C punkt 5.2. I hovedsak er dette krav om nasjonal (eller nordisk) lagring av regnskapsmateriale etter bokføringsloven.

Regler om forvaltningens taushetsplikt fremgår blant annet av forvaltningsloven. Oppbevaring av taushetsbelagt materiale i en jurisdiksjon hvor den utenlandske staten etter egen lovgivning kan få tilgang til informasjonen kan etter omstendighetene ikke være betryggende, jf. forvaltningsloven § 13c, se vedlegg C punkt 4.4. Det legger også begrensninger på hvor taushetsbelagt data kan lagres og behandles.

5.2 Rammebetingelser knyttet til regelverk om offentlige anskaffelser og statsstøtte

Reglene om offentlig støtte setter krav til hvordan det offentlige gjør innkjøp av varer og tjenester knyttet til etablering og drift av en skytjeneste. Det kan ikke utelukkes at statsstøttereglene kommer til anvendelse i tilfeller hvor skytjenesten leveres gjennom egenregi, se vedlegg C punkt 4.2.2.

Anskaffelsesregelverket inneholder krav som må være oppfylt for at unntakene for offentlig egenregi og samarbeid skal kunne benyttes, se vedlegg C punkt. Dette betyr at anskaffelsesregelverket gir visse føringer for hvordan offentlig samarbeid om nasjonal sky må innrettes. Anskaffelsesregelverket får imidlertid ikke anvendelse på samarbeid som ikke bygger på kontrakt, for eksempel dersom det fastsettes i lov eller forskrift at et bestemt organ skal være ansvarlig for å etablere og drifte en nasjonal løsning for statlige forvaltningsorganer.

Likebehandlingsprinsippet i anskaffelsesloven § 4 vil også medføre visse skranker for hvilke krav som kan stilles til leverandører i en anskaffelse, se vedlegg C punkt 4.1.3. For eksempel vil det ikke være anledning til å uten videre kreve nasjonal lagring og behandling av data i skyløsningen. Anskaffelsesloven § 3 gir også visse rettigheter til leverandører etablert utenfor EU/EØS.

Unntaket fra anskaffelsesregelverket om sikkerhetsmessige forhold mv., jf. forskrift om offentlige anskaffelser § 2-2, kan være anvendelig dersom hele eller deler av nasjonal skyløsning omfattes av sikkerhetsloven, for eksempel dersom løsningen anses som skjermingsverdig infrastruktur.

6 Mulighetsstudie

I mulighetsstudien er det gjort en bred vurdering av mulige konsepter innenfor det definerte mulighetsrommet. Disse konseptene er deretter spisset og slått sammen til helhetlig konsepter. Konsepter med tilstrekkelig grad av måloppnåelse, og som vil kunne imøtekomme rammebetingelsene er tatt videre til alternativanalysen. I tillegg til nullalternativet er fem konsepter tatt med videre: K1 Reguleringskonseptet, K2 Statlig skymegler, K3 Lukket statlig sky, K4 Lukket kommersiell sky, og K7 Kombinasjonskonseptet.

Formålet med mulighetsstudien er å finne et tilstrekkelig bredt spekter av relevante konsepter som sikrer at den beste løsningen identifiseres. For at konseptene skal være relevante må de bidra til å oppnå de målene som er satt og befinne seg innenfor de identifiserte rammebetingelsene. Utredningen har tilstrebet at konseptene som tas med videre til alternativanalysen er konseptuelt forskjellige, noe som innebærer at de innehar forskjellige egenskaper og utløser forskjellige virkninger. For å imøtekomme dette er det identifisert konsepter med forskjellige ambisjonsnivå og med ulik vektning av forskjellige behov. Hvilket ambisjonsnivå det er hensiktsmessig å legge til grunn vil påvirkes av avveining mellom kostnader, effektivitetsgevinster og verdien av nasjonal kontroll. Det er derfor utformet konsepter med ulik oppnåelse av de forskjellige effektmålene, slik at det legges best mulig til rette for en nærmere vurdering av innretning og ambisjonsnivå i alternativanalysen. På den måten har utredningen fått frem konsepter som er tilstrekkelig forskjellige, og som utfordrer potensielle målkonflikter, samtidig som de alle er rettet inn mot å løse de samme problemene identifisert i kapittel 2.

Arbeidet med mulighetsstudien har vært en stegvis prosess som grenser opp mot og gradvis går over i arbeidet med alternativanalysen. Det er benyttet følgende prosess for å identifisere, vurdere og velge konsepter som skal videreføres:

1. Definere mulighetsrommet basert på identifiserte behov, mål og rammebetingelser
2. Utforske mulighetsrommet gjennom bruk av ulike dimensjoner og virkemidler
3. Lage ulike konsepter som gir forskjellige virkninger
4. Justere og grovsile konseptene til mer helhetlige og relevante alternativer
5. Gjennomføre nedvalg av konsepter som tas videre til alternativanalysen

I de kommende kapitlene beskrives det nærmere hvordan mulighetsstudien er gjennomført og hvilke konsepter som tas videre til alternativanalysen og hvorfor.

6.1 Definerings av det relevante mulighetsrommet

Første steg i arbeidet med mulighetsstudien er å definere mulighetsrommet. Det innebærer å finne riktig avgrensning av hva det er relevant å vurdere, og deretter finne hvilke dimensjoner og virkemidler som kan brukes til å identifisere ulike alternativer innenfor disse rammene. Problembeskrivelsen, behovsanalysen, mål og rammebetingelser danner utgangspunktet for å definere det relevante mulighetsrommet. Dette danner grunnlaget for

identifisering og vurdering av mulige konsepter. Disse er beskrevet i kapittel 2-5 ovenfor, men en kort oppsummering er gjengitt i figuren under.



Figur 6-1 - Oppsummerte problem, behov, mål og rammebetingelser

6.1.1 Avgrensninger av mulighetsrommet

De strategiske målene og rammebetingelsene setter de mest sentrale rammene for avgrensningen av mulighetsrommet.

Målene gir tydelige føringer om at aktuelle konsepter må ivareta balanse mellom sikkerhet, effektivitet og fleksibilitet. Det er ikke gjort en rangering av disse målene og det er ikke satt noen absolutte kriterier for måloppnåelse som alle konsepter skal ivareta. Alle konsepter må imidlertid gi en tilstrekkelig grad av måloppnåelse innenfor alle tre effektmål for å være relevante.

Rammebetingelsene gjør det tydelig at alle konsepter må kunne realiseres i tråd med gjeldende regelverk. Dette gjelder blant annet anskaffelsesregler, konkurranselov, sikkerhetsloven, forvaltningsloven og arkivloven. Hvordan dette skal gjøres i praksis vil utredes mer detaljert i senere planleggingsfaser. Konsepter som ikke vil kunne realiseres i tråd med rammebetingelsene, blir valgt vekk før alternativanalysen.

Mandatet inneholder også enkelte føringer som avgrenser mulighetsstudien. Det er blant annet spesifisert at konseptene som vurderes skal rette seg mot ugradert, skjermingsverdig informasjon, men at annen informasjon som ansees beskyttelsesverdig, og er ugradert, også skal vurderes. Videre er det spesifisert at det er statsforvaltningen, utenom departementene, som er den relevante målgruppen, og at det skal utarbeides et minimumsalternativ. Mandatet tar utgangspunkt i at Stortinget har bedt Regjeringen om å «utrede behov for og etablering av en felles skytjeneste for forvaltningen». Dette avgrenser utredningen til å vurdere ulike skyløsninger, mens tradisjonelle IKT-tjenester på egendriftet plattform (som ikke er skybaserte) ikke er inkludert. Selv om mandatet spesifiserer en skytjeneste for statsforvaltningen, har vi inkludert overordnede vurderinger av hvorvidt de ulike konseptene kan utvides til å betjene et bredere spekter av offentlige virksomheter, for eksempel kommunesektoren, i senere faser.

6.1.2 Sentrale mulighetsdimensjoner og virkemidler

Med utgangspunkt i rammene ovenfor er neste steg i mulighetsstudien å identifisere hvilke dimensjoner de ulike konseptene kan utformes langs. Med mulighetsdimensjoner menes sentrale egenskaper som påvirker problemet, imøtekommer behov og har stor betydning for grad av måloppnåelse og hvilke virkninger som utløses. Mulighetsdimensjonene inneholder egenskaper som har en direkte sammenheng med årsak-virkningsforholdene identifisert i problembeskrivelsen og som konsepter kan differensieres langs. På den måten tydeliggjøres både muligheter og forskjeller mellom konseptene. I tillegg er hvilke virkemidler som kan brukes til å realisere løsningene vurdert.

På denne måten er mulighetsrommet spent ut slik at alle relevante konsepter tas med i den tidlige prosessen. Det er lagt vekt på at konseptene som vurderes skal være relevante og gjennomførbare, og at de konseptene som videreføres til alternativanalysen dekker mulighetsrommet på en tilstrekkelig måte.

Det finnes en rekke dimensjoner og virkemidler som kan benyttes ved utarbeidelse av konsepter innen digitalisering. Det er vurdert og forkastet flere mulige overordnede dimensjoner, blant annet mengde data, som i utgangspunktet er viktig både for valg av ambisjonsnivå og hvilket kostnadsnivå konseptet ender på. Mengde data vil imidlertid gi begrenset verdi fordi skytjenester per definisjon er svært skalerbare og det er betydelig usikkerhet knyttet til hvor mye data konseptene i utgangspunktet bør dimensjoneres for. Utredningen har derfor lagt opp til at alle konseptene skal håndtere samme mengde data. Hvis ikke vil det bli uhensiktsmessig krevende å sammenligne og rangere konseptene på en god måte i alternativanalysen. Hvilke og hvor mye data som bør inngå i det valgte konseptet kan med fordel avgjøres på et senere stadium når man har et bedre informasjonsgrunnlag, uten at det får betydning for innretningen av konseptet som er valgt.

Basert på de behovene som er identifisert og målene som er utledet av disse, har to overordnede dimensjoner pekt seg ut som særlig egnede for å utvikle konsepter rundt. Den første overordnede dimensjonen er den samlede *funksjonaliteten* en nasjonal sky kan tilby. Funksjonalitet er særlig styrende for behovstilfredstillelse til brukerne av konseptet og inkluderer underdimensjonene:

- **Egenskaper:** Dekker forhold som ytelse, kapasitet, skalerbarhet, robusthet og utviklingsmulighet.
- **Tjenestetilbud:** Dekker både omfanget av tjenester som tilbys, og hvilke tjenestenivåer (kvalitet) som tilbys.

Den andre hoveddimensjonen i mulighetsrommet er *nasjonal kontroll* (se og vedlegg J). Graden av nasjonal kontroll vil være avgjørende for oppnåelsen av effektmål 1 om sikkerhet og det overordnede behovet for å sikre beskyttelsesverdig informasjon i hele krisespekteret. Hvor mye nasjonal kontroll et konsept vil kunne tilby påvirkes av en rekke faktorer og virkemidler som kan samles i fire underdimensjoner:

- **Statlig styring:** Dekker i hvilken grad staten kan styre eller har direkte kontroll over innsatsfaktorene i løsningen, og hvor sterkt staten kan styre videreutviklingen av løsningen.

- **Avhengigheter:** Dekker i hvilken grad staten er avhengig av tredjeparter for å drifte og levere tjenester, herunder avhengigheter til leverandører som omfattes av andre lands jurisdiksjon.
- **Sikkerhetskrav og kontrollmekanismer:** Dekker hvor omfattende krav til sikkerhet, plassering av datasenter, personell, tilgangsstyring / fjerntilgang osv. er.
- **Sikkerhetsorganisering:** Dekker i hvilken grad ansvaret for å vurdere risiko, stille krav til og følge opp sikkerhetstiltak er koordinert, samordnet eller fordelt på mange virksomheter.

Samlet vil hvilken **funksjonalitet** en nasjonal sky kan tilby og graden av **nasjonal kontroll** definere ambisjonsnivået på konseptet og med det også kostnader og behovstilfredsstillelse. Dette avgjør oppnåelsen av samfunns- og effektmål. Nivået på funksjonalitet spenner fra et minimum av tjenester og egenskaper som en enkel back-up tjeneste med lave tids- og ytelseskrav, til et meget høyt tjeneste- og egenskapsnivå som tilsvarer det de beste globale selskapene som leverer allmenne skytjenester kan tilby. En lav grad av nasjonal kontroll vil innebære en tillitsbasert tilnærming til tjenestekjøp og leverandørvalg, omfattende avhengigheter til underleverandører og sikkerhetskrav og kontrollmekanismer som i all hovedsak styres av ordinære markedsvilkår. I den andre enden av skalaen vil en høy grad av nasjonal kontroll kjennetegnes ved direkte statlig styring av løsningen, minimale avhengigheter til leverandører, omfattende krav til sikkerhet og verifikasjon og enhetlig og samordnet sikkerhetsstyring.

Ulik vektlegging av de to hoveddimensjonene vil også gi konsepter med ulik innretning og grad av måloppnåelse av de forskjellige effektmålene. Totalt sett gir det derfor et godt grunnlag for å sikre relevante konsepter med ulike ambisjonsnivåer, og konsepter som gir forskjellig type virkninger. For en nærmere beskrivelse av hvordan de ulike nivåene på funksjonalitet og nasjonal kontroll er definert, se Vedlegg E Mulighetsstudien og kap. 7 Alternativanalysen.

6.2 Utforming av konsepter

Med utgangspunkt i de valgte mulighetsdimensjonene er det identifisert en rekke konsepter. I utarbeidelsen av en bruttoliste over mulige konsepter ble det blant annet tatt utgangspunkt i andre tilgrensende prosjekter og liknende initiativer fra andre land. Det ble både vurdert enkle løsninger med begrenset funksjonalitet og tjenestetilbud, og mer fullverdige løsninger med et bredt spekter av tjenester og høy ytelse. Det er vurdert løsninger som spenner fra tjenestekjøp utelukkende fra kommersielle aktører, til løsninger som innebærer statlig tjenesteproduksjon i full egenregi. Det er også vurdert løsninger som primært baserer seg på gjenbruk og utnyttelse av eksisterende infrastruktur og organisasjoner, samt løsninger som omfatter etablering av helt nye virksomheter der alt bygges opp fra bunnen. Ulike former for organisering og bruk av regulatoriske virkemidler, rådgivningstjeneste og tilsyn er også tatt med i vurderingene. For en nærmere beskrivelse av de ulike konseptmulighetene som er vurdert, se bruttoliste av alternativer beskrevet i Vedlegg E Mulighetsstudien.

Med utgangspunkt i bruttolisten over relevante konseptmuligheter ble det gjort en første siling av konsepter som ga liten eller ingen måloppnåelse. Konsepter som i stor grad var overlappende, eller som i stor grad er å anse som varianter av samme konsept, ble omstrukturert. I omstruktureringen ble det lagt vekt på å lage helhetlige konsepter som kan

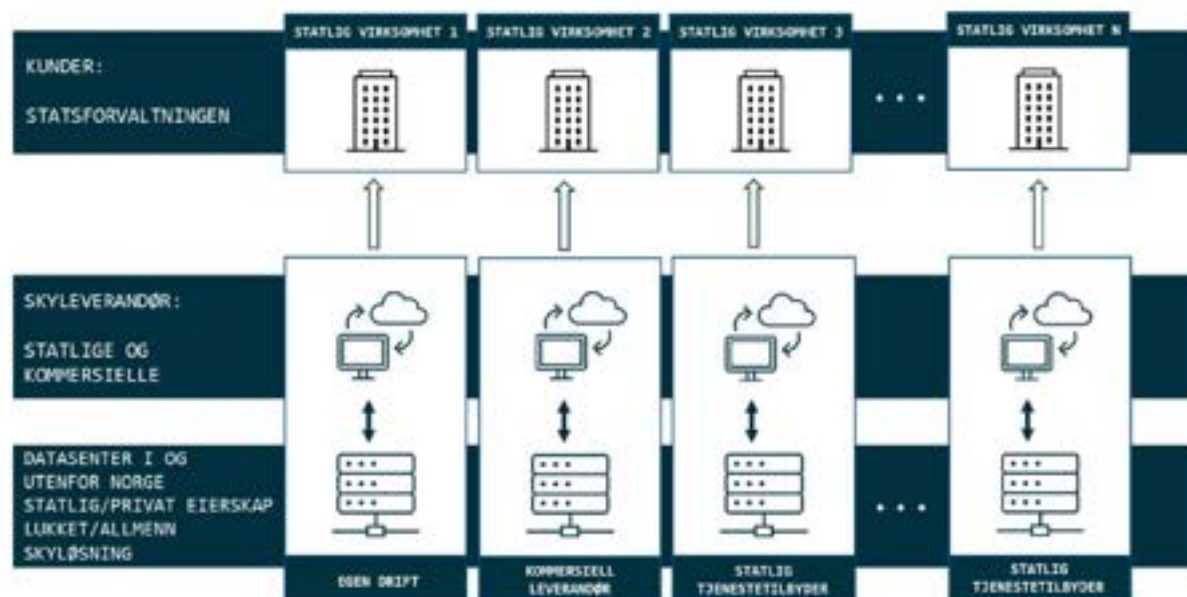
levere både IaaS, PaaS og SaaS-tjenester. Begrunnelsen for dette er det brede spekteret av virksomheter som konseptene skal imøtekomme behovene til. Det er også et bredt spenn i hvilke type beskyttelsesverdige data og systemer de ulike virksomhetene besitter. For at et konsept skal ha mulighet til å oppnå tilstrekkelig grad av måloppnåelse, må det derfor kunne tilby et bredt nok tilbud av basistjenester til at det oppleves relevant for de potensielle brukerne. Videre er grenseflatene mellom IaaS, PaaS og SaaS såpass flytende at det er lite hensiktsmessig å begrense enkelte løsninger til kun ett tjenestelag - både kostnadmessig, funksjonelt og med hensyn til kontrollspørsmålet. Det vil likevel være nok frihetsgrader innenfor hvert konsept til å kunne sikre variasjon i både funksjonalitet, nasjonal kontroll og ambisjonsnivå. Se Vedlegg E for nærmere beskrivelse og illustrasjoner.

Enkelte egenskaper ved konseptene er vurdert til være gjeldende for alle konseptene. Disse er trukket ut av beskrivelsen av de enkelte konseptene. Se Vedlegg E for utdypende beskrivelser av felles egenskaper for, og innholdet i, de enkelte konseptene. Felles egenskaper som må ivaretas på tvers av konseptene er:

- *Nasjonal kontroll* – konseptene må møte grunnleggende krav om nasjonal kontroll knyttet til datasenterlokasjon, driftspersonell, verdikjedekontroll etc.
- *Godkjenning av skjermingsverdige systemer* - dersom et system behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner, skal systemet godkjennes
- *Informasjonssikkerhet* – konseptene må tilfredsstille de nasjonale kravene til grunnleggende informasjonssikkerhet
- *Teknologi* - konseptene må dekke egenskaper som redundans, skalering, universelle kjøremiljøer for å sikre portabilitet, bruk av kontainerbaserte løsninger og moderne virtualiseringsteknologi. En nasjonal sky må baseres på flere, geografisk adskilte datasenter med en redundant interkonnektivitet.
- *Spesielle tjenester* – konseptene må for å møte behovene for et bredt og rikt tjenestespekter og bruk av tidsriktige verktøy, tilby utvalgte tjenester levert som allmenne skytjenester, eksempelvis avanserte analyseverktøy
- *Målgruppe* - konseptene er i utgangspunktet rettet inn mot å løse behov for virksomhetene i statsforvaltningen, men vi anbefaler at det på sikt gjøres en vurdering om dette bør utvides til å dekke større deler av offentlig sektor
- *Samarbeid utenfor Norge* - enkelte tjenester kan dersom det er ønskelig, utføres på tilsvarende nasjonale datasentre i andre land som Norge har et tett partnerskap med

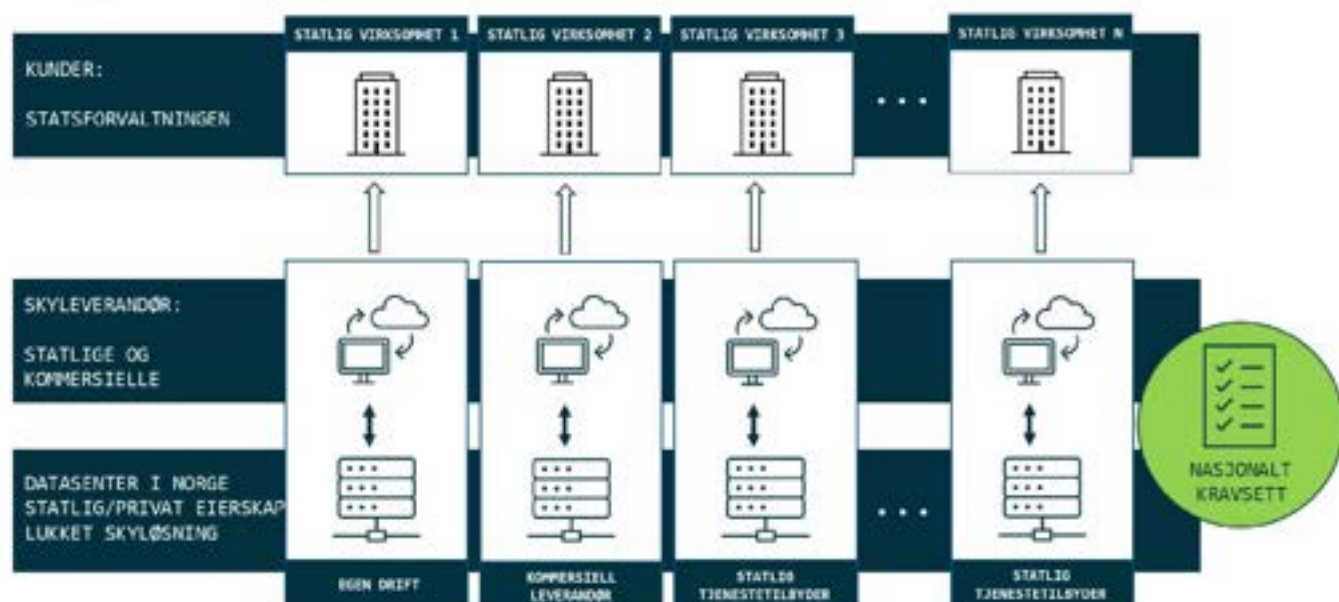
Følgende konsepter ble tatt med til videre utforming og detaljering:

K0: Nullalternativet innebærer en videreføring av dagens situasjon der virksomhetene står fritt til å selv vurdere hvilke skyløsninger de ønsker å benytte. Virksomhetene velger hvilke tjenester de skal etablere som skytjenester og hva slags leveransemodell som skal benyttes. Konseptet viderefører virksomhetenes opplevde usikkerhet om bruk av skytjenester og innebærer en mangelfull nasjonal kontroll av beskyttelsesverdige data og systemer. Konseptet er illustrert i figuren under.



Figur 6-2 Nullalternativet: Mange skyleverandører og sammensatt bruk av sky hos virksomhetene

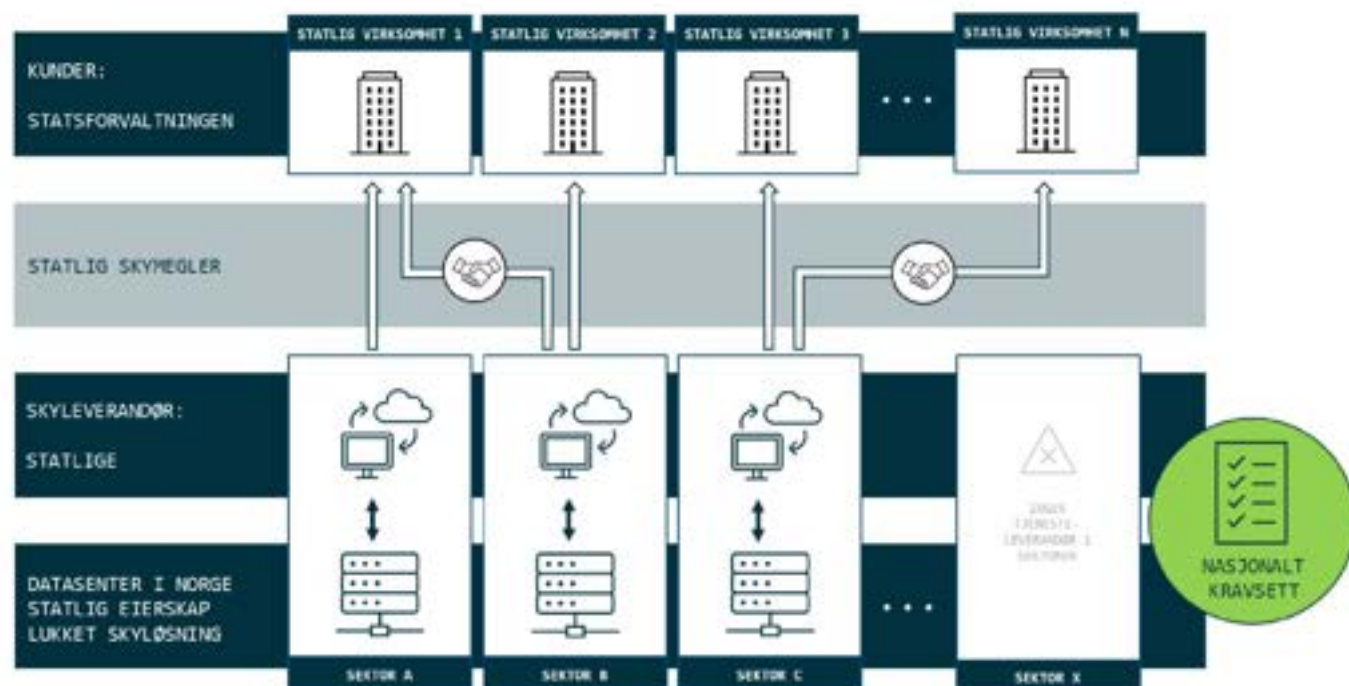
K1: Reguleringskonseptet innebærer å samle, klargjøre og eventuelt styrke dagens regelverk. Det etableres eller styrkes en statlig tilsynsmyndighet og rådgivningstjeneste, med mulighet for en sertifiseringsordning. Konseptet vil redusere uklarheter knyttet til hvor beskyttelsesverdige data kan lagres og hvem som kan drifte løsninger som inneholder slike data. Det legges til rette for at det vil bli enklere for virksomhetene å planlegge og beslutte overgangen til skyløsninger. Det forventes at dette vil gi en bedre nasjonal kontroll enn i dag. Konseptet er illustrert i figuren under.



Figur 6-3 Reguleringskonseptet: Styrte videreføring innen et tydeligere regelverk

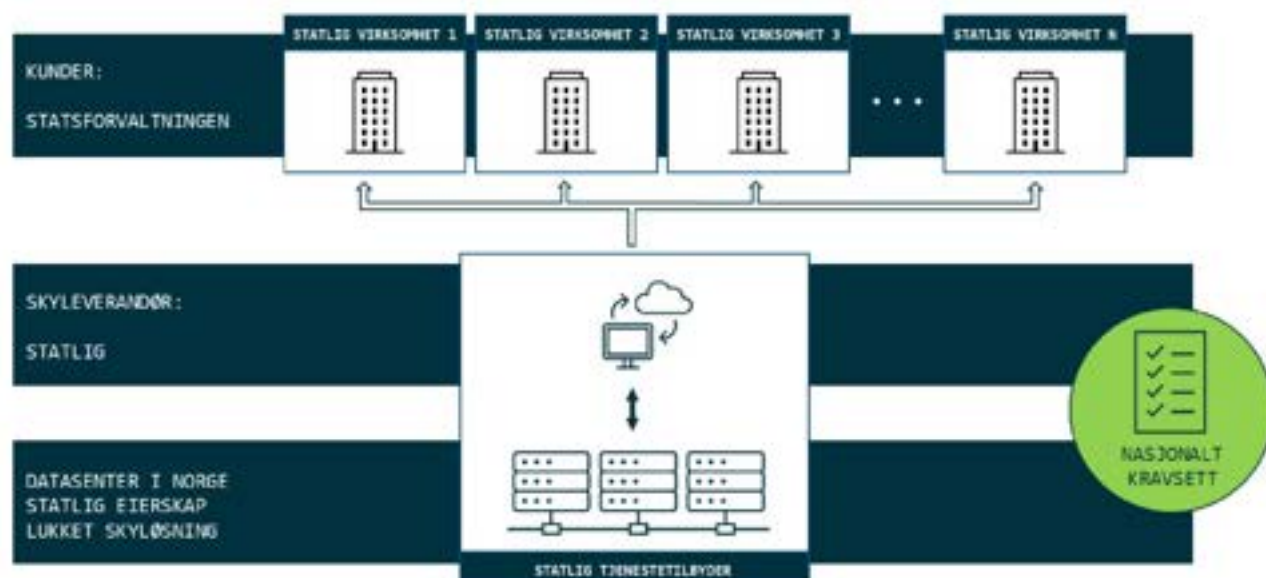
K2: Statlig skymegler medfører at det tilbys flere parallelle statlige skytjenester levert av et fåtall eksisterende statlig eide tjenesteleverandører, administrert av en liten sentralenhet som inngår rammeavtaler med disse. Tjenesteleverandørene må parallelt tilpasse og utvikle skytjenester som både kan overlappes med og utfylle hverandre. Sentralenheten vil operere

som en skymegler mellom virksomhetene og tjenesteleverandørene. Konseptet er illustrert i figuren under.



Figur 6-4 Statlig skymegler: Etablerte statlige tjenesteleverandører leverer skytjenester til statlige virksomheter

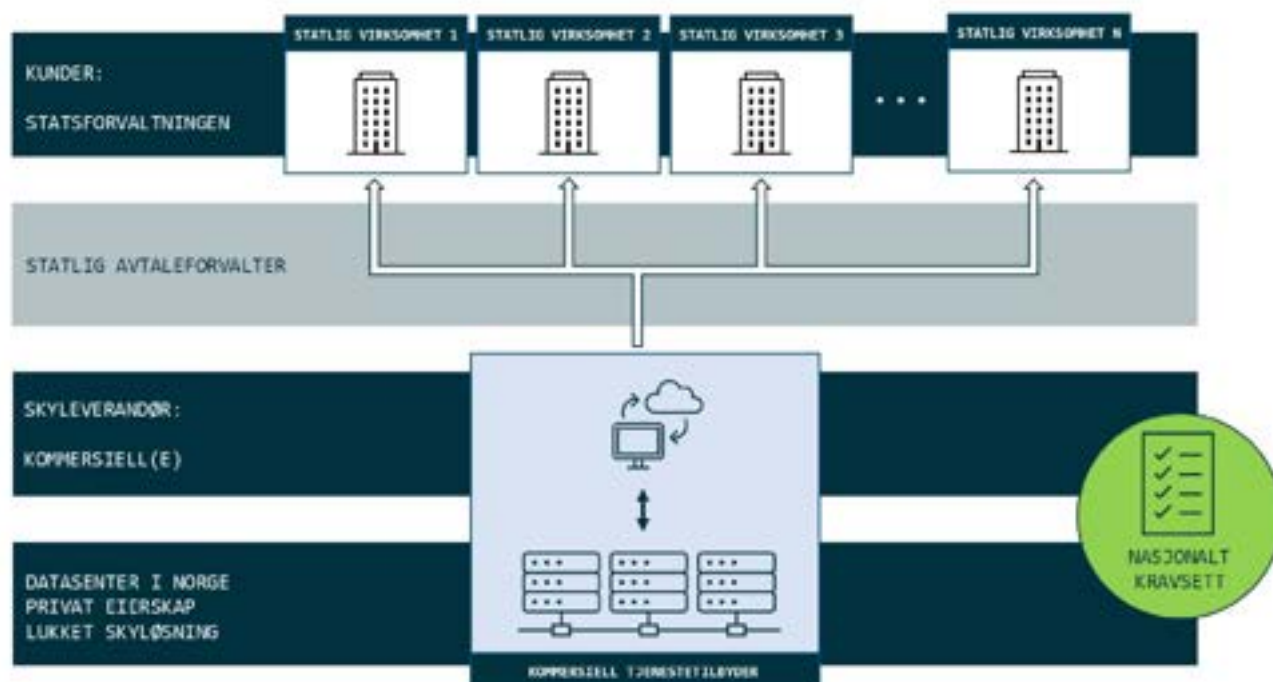
K3: Lukket statlig sky innebærer at staten enten etablerer en ny eller gir ansvar til en eksisterende statlig virksomhet som eier og drifter skyløsningen på norsk jord underlagt norsk jurisdiksjon. Denne virksomheten bygger opp en egen drifts- og forvaltningsorganisasjon og benytter nødvendig eksisterende datasenterkapasitet. Konseptet innebærer sterk statlig styring og høy nasjonal kontroll. Konseptet er illustrert i figuren under.



Figur 6-5 Lukket statlig sky: En felles skyplattform som eies og driftes av staten

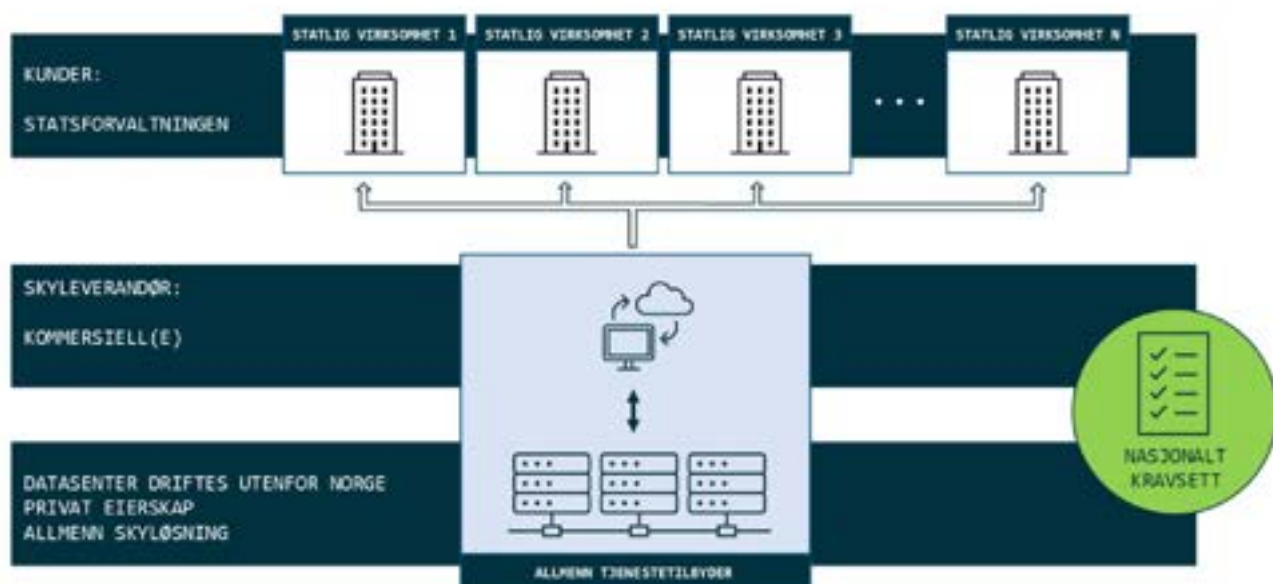
K4: Lukket kommersiell sky innebærer at staten inngår en avtale med et fåtall kommersielle aktører som eier, leverer, videreutvikler og drifter skyløsningene. Det stilles

spesifikke krav knyttet til nasjonal kontroll av skytjenestene som leverandøren(e) må tilfredsstillende og gi garantier for. Den statlige enheten som får ansvar for avtalen(e), bygger opp en organisasjon for å styre og videreutvikle denne. Konseptet er illustrert i figuren under.



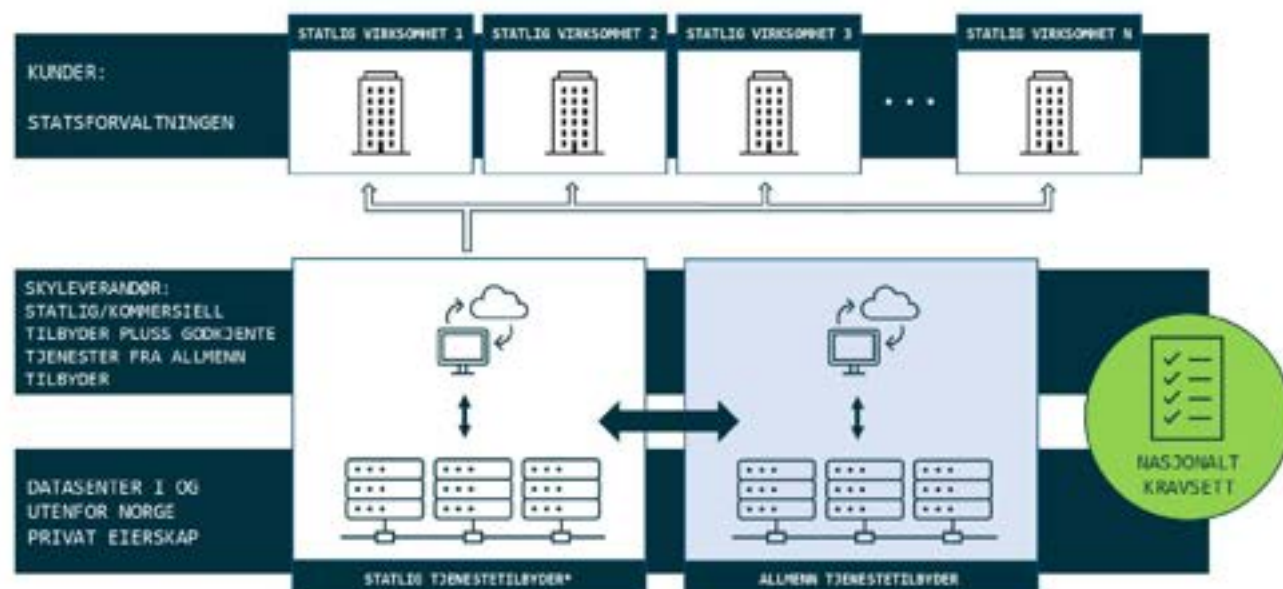
Figur 6-6 Lukket kommersiell sky: Kommersielle aktører drifter en nasjonal skytjeneste

K5: Allmenn sky innebærer at en eksisterende statlig virksomhet får mandat og myndighet til å inngå avtale med en eller flere store, globale kommersielle leverandører for leveranse av allmenne skytjenester. Konseptet innebærer et meget stort tjenestespekter og mulighet for et meget høyt tjenestenivå, men med en lav grad av statlig styring og mulighet for nasjonal kontroll. Konseptet er illustrert i figuren under.



Figur 6-7 Allmenn sky: Staten videreformidler kommersielle allmenne skytjenester

K6: Hybrid nasjonal sky innebærer at staten etablerer en lukket skytjenesteløsning (statlig eller kommersielt eid og driftet) og åpner for at enkelte tjenester kan leveres utenfor den lukkede skyløsningen i en allmenn skyløsning, så lenge dette er i tråd med kravene som stilles om nasjonal kontroll. Konseptet innebærer en til dels meget høy funksjonalitet og kan innebære en høy grad av nasjonal kontroll. Konseptet er illustrert i figuren under.



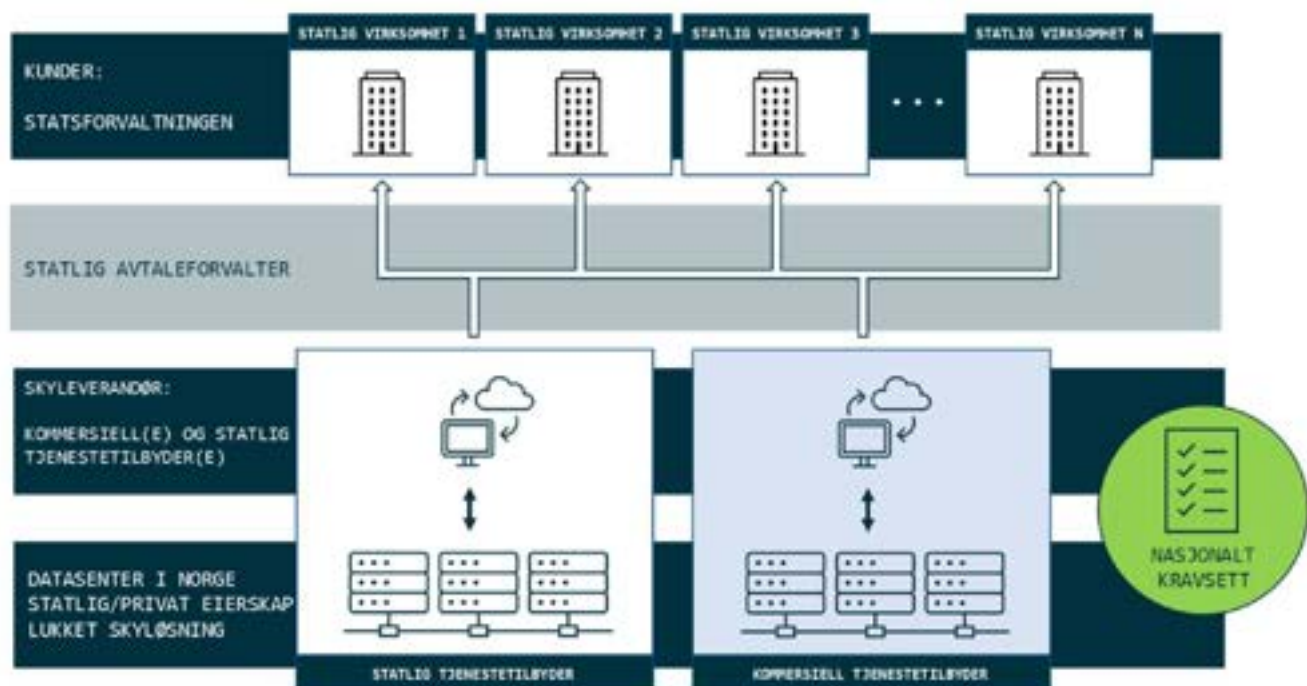
*) Her illustrert med K3, men den allmenne skyløsningen kan kombineres med både K2, K3 og K4

Figur 6-8 Hybrid sky: Sammensetning av lukket og allmenn skytjeneste

K7: Kombinasjonskonseptet innebærer en kombinasjon av K3 og K4, hvor staten sikrer at en statlig virksomhet eier og drifter en skyløsning på norsk jord underlagt norsk jurisdiksjon (som K3), og at denne statlige virksomheten i tillegg inngår avtale med en eller et fåtall kommersielle leverandører som eier, leverer, videreutvikler og drifter skytjenester med middels grad av nasjonal kontroll (som K4).

Beskyttelsesverdige data som må sikres med høy grad av nasjonal kontroll, lagres og behandles i en lukket statlig sky (som K3). Andre beskyttelsesverdige data kan virksomhetene velge å lagre og behandle i en lukket kommersiell sky (som K4) med middels grad av nasjonal kontroll, basert på virksomhetenes vurdering av behov for sikkerhet og funksjonalitet.

Kombinasjonen innebærer at man, avhengig av hvilke data som håndteres, både oppnår et høyt nivå av nasjonal kontroll og en høy funksjonalitet. Konseptet er illustrert i figuren under.



Figur 6-9 Kombinasjonskonseptet: Både statlig og nasjonal lukket sky

6.3 Nedvalg av konsepter

Av de syv konseptene som er beskrevet over er det to konsepter som ikke er tatt med til alternativanalysen; K5 Allmenn sky og K6 Hybrid nasjonal sky.

K5: Allmenn sky ekskluderes fordi det ikke gir tilstrekkelig måloppnåelse (E1: sikkerhet) og møter ikke rammebetingelsene i tilstrekkelig grad. Årsaken er at leveransmodellen for dagens allmenne skytjenester i stor grad baserer seg på best mulig utnyttelse av infrastruktur, kompetansemiljøer og andre ressurser på tvers av landegrensene. Det vil derfor være vanskelig å verifisere hvor beskyttelsesverdige data lagres og behandles, og det vil av den grunn kunne være jurisdiksjonsutfordringer og lav grad av kontroll. At store mengder beskyttelsesverdige data samles hos aktører utenfor norsk kontroll øker også sårbarheten for ytre politisk press som kan redusere norsk nasjonal styringsevne og handlefrihet i en krise eller væpnet konflikt. Dette kan skje enten ved at norske virksomheter aktivt utestenges fra systemene, eller ved at norske virksomheter nedprioriteres i en internasjonal krise.

Konseptet vil også kunne innebære at personopplysninger eller andre beskyttelsesverdige data overføres til land utenfor EØS og kan aksesseres fra tredjeland, selv om de lagres innenfor EØS-området. Alternativet vil derfor trolig innebære betydelige rettslige utfordringer med å ivareta regelverket for lovlig overføring av personopplysninger til tredjeland. Over tid vil dette kunne endre seg og det kan ikke utelukkes at allmenne skytjenester etter hvert kan imøtekomme kravene til nasjonal kontroll. Dersom det blir tilfelle, vil imidlertid slike utvalgte tjenester kunne kombineres med øvrige konsepter i tråd med beskrivelsen av K6.

Et tilleggsmoment i vurderingen av om K5 møter rammebetingelsene er knyttet til krav i sikkerhetsloven, blant annet i forbindelse med nødvendige beskyttelsestiltak, klarering av personell og leverandørklarering. Personell som skal ha tilgang til skjermingsverdig informasjonssystem utpekt som skjermingsverdig objekt eller infrastruktur vil kunne være

omfattet av reglene om adgangsklarering og autorisasjon. Det innebærer at personellet med slik tilgang må være kjent, og at personellet kan klarerers og autoriseres.

Det stilles krav om leverandørklarering der leverandøren vil få tilgang til klassifiserte områder innen skjermingsverdig objekt eller infrastruktur. Dette er nærmere redegjort for i vedlegg B om rammebetingelser etter sikkerhetsloven. Leverandørklarering forutsetter at klareringsmyndigheten faktisk og rettslig har mulighet til å vurdere om en leverandør er sikkerhetsmessig skikket, jf. sikkerhetsloven § 9-3. Tilsvarende vil gjelde leverandørens personell som skal underlegges personkontroll. Klarering av utenlandske leverandører forutsetter en sikkerhetsavtale mellom Norge og leverandørens hjemstat. I dag eksisterer det ingen avtaler med andre stater om klarering av leverandører for tilgang til annet enn sikkerhetsgradert informasjon. Det er heller ikke gitt at andre stater har et internrettslig hjemmelsgrunnlag for å kunne gi leverandørklarering for tilgang til skjermingsverdige objekter og infrastruktur. Tilsvarende gjelder for adgangsklarering av leverandørens personell. I praksis vil det derfor neppe være mulig å klarere utenlandske leverandører, og deres personell, for tilgang til ugradert skjermingsverdig informasjonssystem klassifisert som skjermingsverdig objekt eller infrastruktur. Dette medfører en betydelig risiko for at K5 i praksis ikke vil kunne benyttes til å behandle skjermingsverdig ugradert informasjon eller skjermingsverdig infrastruktur.

K6: Nasjonal hybrid sky tas heller ikke videre som et eget konsept, fordi det i all hovedsak kan kombineres med øvrige konsepter ved at utvalgte allmenne skytjenester kan tilbys i alle øvrige konsepter, under gitte betingelser. Det er flere grunner til dette. For det første er det en rekke viktige tjenester som per i dag forutsetter bruk av allmenn sky. Å ekskludere alle muligheter for å benytte disse er etter utredningens vurdering ikke hensiktsmessig. Det er i tillegg en bevegelse i retning av at de store globale skyaktørene etablerer datasentre og løsninger som i praksis innebærer at de kan være i ferd med helt eller delvis å imøtekomme kravene om nasjonal kontroll. Det vil av den grunn være en betydelig fordel for en nasjonal løsning for beskyttelsesverdige data å kunne benytte et selektivt utvalg av offentlige skytjenester på sikt. Det vil, hvis denne muligheten både tillates og benyttes, bidra til å løfte tjenestetilbudet i en positiv retning og føre til en bedret behovsdekning og økt måloppnåelse (E2 og E3) for alle konseptene.

Det innebærer at fem konsepter (i tillegg til nullalternativet) tas med videre til alternativanalysen for ytterligere detaljering og analyse med følgende begrunnelser:

- **K1: Reguleringskonseptet** kan tilfredsstillende rammebetingelsene, men krever at enkelte problemstillinger og utfordringer løses (se Vedlegg E for nærmere vurdering). K1 kan gi bedret effektivitet for virksomheter som i dag ikke benytter skyløsninger, men konseptet vil i liten grad legge til rette for utnyttelse av stordriftsfordeler. Målet om fleksibilitet ivaretas også på middels nivå. Det varierende tjenestetilbudet i K1 vil til en viss grad møte de operative behovene om bredt spenn av tjenester, fleksibilitet og kapasitet.
- **K2: Statlig skymegler** kan tilfredsstillende rammebetingelsene, men krever at enkelte problemstillinger og utfordringer løses (se Vedlegg E for nærmere vurdering). Gitt at de statlige tjenesteleverandørene iverksetter nødvendige tiltak, vil målene om sikkerhet, effektivitet og fleksibilitet tilfredsstilles. Konseptet vil ha middels eller høy grad av nasjonal kontroll, avhengig av type involvering og valg av kommersielle

underleverandører. De parallelle tjenestetilbyderne vil kunne oppnå individuelle stordriftsfordeler som kan gjenspeiles i tjenesteprisen, men ikke på tvers av leverandører. Fleksibiliteten vil være høy og gi en god måloppnåelse, selv om det også her vil være et uforløst potensial. Tjenestetilbudet i K2 vil i høy grad kunne møte de operative behovene om bredt spenn av tjenester, fleksibilitet og kapasitet.

- **K3: Lukket statlig sky** kan tilfredsstillende rammebetingelsene, men krever at enkelte problemstillinger og utfordringer løses (se Vedlegg E for nærmere vurdering). Gitt at den statlige tjenesteleverandøren iverksetter nødvendige tiltak, vil målene om sikkerhet, effektivitet og fleksibilitet tilfredsstilles. Konseptet vil innebære høy grad av nasjonal kontroll og vil kunne gi stordriftsfordeler som kan gjenspeiles i tjenesteprisen. Funksjonaliteten er kan være lavere enn i K2 på enkelte tjenester, men vil fortsatt møte effektivitets- og fleksibilitetsmålene.
- **K4: Lukket kommersiell sky** kan tilfredsstillende rammebetingelsene, men krever at enkelte problemstillinger og utfordringer løses (se Vedlegg E for nærmere vurdering). Gitt at tjenesteleverandørene iverksetter nødvendige tiltak, vil målene om sikkerhet, effektivitet og fleksibilitet tilfredsstilles. Konseptet vil ha middels grad av nasjonal kontroll. De kommersielle tjenestetilbyderne vil kunne utnytte egne stordriftsfordeler som kan gjenspeiles i tjenesteprisen, og konkurransen i markedet bør bidra til en effektiv utvikling av konkurransedyktige tjenester. Fleksibiliteten vil være høy og gi en god måloppnåelse. Det gode tjenestetilbudet i K4 vil i høy grad kunne møte de operative behovene om bredt spenn av tjenester, fleksibilitet og kapasitet.
- **K7: Kombinasjonskonseptet** kan tilfredsstillende rammebetingelsene, men krever at enkelte problemstillinger og utfordringer løses (se Vedlegg E). Konseptet kombinerer egenskapene fra K3 og K4, men legger i større grad til rette for en løsning som tilpasser graden av nasjonal kontroll til verdien av de dataene og systemene som skal inngå. Konseptet gir gode mulighetene for utnyttelse av stordriftsfordeler, men vil medføre noen ulemper knyttet til etablering og drift av to parallelle tjenestemodeller.

Alle konseptene er dimensjonert likt med hensyn til hvilken mengde beskyttelsesverdige data de skal ha kapasitet til å håndtere. Dette er gjort av flere grunner. For det første er det stor usikkerhet rundt mengden beskyttelsesverdige data som bør ligge i en nasjonal skyløsning. Denne usikkerheten er både knyttet til hvor mye beskyttelsesverdige data som finnes i dag, hvor mye datavolumene forventes å vokse, og ikke minst hvilke data som har behov for ulike nivåer av nasjonal kontroll. Videre vil datavolumene ha stor innvirkning på kostnadsnivået og muligheter til å utnytte stordriftsfordeler. Det viktigste argumentet er at dimensjoneringen med hensyn til datavolumer har liten betydning for hvilket konsept som er det mest hensiktsmessige.

Alle konseptene som er tatt videre til alternativanalysen er utformet på en måte som legger til rette for at omfanget kan justeres vesentlig på et senere tidspunkt, uten at det er behov for å endre på den konseptuelle løsningen. Utredningens vurdering er at det på den måten legges best mulig til rette for å finne den mest hensiktsmessige avveiningen mellom nasjonal kontroll, funksjonalitet, kostnadseffektivitet og fleksibilitet.

En videre spesifisering av hva de ulike konseptene innebærer, og hvilke virkninger de vil medføre er beskrevet i Alternativanalysen.

7 Alternativanalyse

Den samfunnsøkonomiske analysen viser at kostnadene som følger av nasjonal kontroll er store. Manglende nasjonal kontroll kan imidlertid medføre store konsekvenser, særlig i en krise eller krigssituasjon. Verdien av økt nasjonal kontroll er svært vanskelig å anslå og det er derfor krevende å vurdere den samlede samfunnsøkonomiske lønnsomheten av de ulike konseptene. Basert på prissatte virkninger alene er det K4 som medfører de laveste kostnadene utover nullalternativet. For de ikke-prissatte virkningene av nasjonal kontroll er det størst positiv påvirkning i K3. For virkningene knyttet til endret funksjonalitet og fleksibilitet er det K4 som har minst negativ virkning av konseptene og er nærmest nullalternativet.

Hvilket konsept som bør gjennomføres blir derfor i all hovedsak en vurdering om hvilken risiko knyttet til manglende nasjonal kontroll man er villig til å akseptere. Med manglende grunnlag for å vurdere hvor stor denne risikoen er i de ulike konseptene, er dette mer et spørsmål om politiske prioriteringer enn samfunnsøkonomifaglige vurderinger. Utredningens vurdering er likevel at K7 Kombinasjonskonseptet bør tas med videre i planleggingsarbeidet i neste fase. Selv om det, per nå, ikke er tilstrekkelig grunnlag til å fastslå at dette alternativet er det mest samfunnsøkonomisk lønnsomme, gir en slik løsning tilstrekkelig fleksibilitet til å finne en hensiktsmessig balansegang mellom nasjonale sikkerhetsinteresser og behovet for kostnadseffektive og funksjonelle løsninger.

Alternativanalysen er en samlet vurdering av de samfunnsøkonomiske kostnads- og nyttevirkningene som følger av konseptene. De prissatte og ikke-prissatte virkningene danner grunnlaget for anbefaling om videre gjennomføring av en nasjonal sky.

Som beskrevet i mulighetsstudien er det fem konsepter som analyseres nærmere i alternativanalysen, i tillegg til nullalternativet. I alle konsepter ligger det til grunn en tydeliggjøring og skjerping av krav til nasjonal kontroll over beskyttelsesverdige data og systemer. De virksomhetene som benytter løsninger som ikke imøtekommer disse kravene må finne nye løsninger eller reforhandle betingelser med den leverandøren de bruker. Det vil ha konsekvenser for virksomhetenes drift og forvaltning av beskyttelsesverdige data og systemer. I de ulike konseptene vil det også påløpe kostnader knyttet til etablering, organisering, anskaffelse og/eller leveranse av nye skytjenester. Konseptene kan også medføre endret funksjonalitet og fleksibilitet som vil kunne påvirke de statlige virksomhetenes tjenesteproduksjon. Gevinstene vil komme i form av økt nasjonal kontroll over beskyttelsesverdige data og systemer, og med det redusert risiko knyttet til bortfall og integritetsbrudd i, eller uautorisert tilgang til, sentrale offentlige tjenester i fred, krise eller som følge av væpnet konflikt. En overordnet skisse av hvordan de ulike virkningene utløses er vist i årsak-virkningsdiagrammet under.



Figur 7-1 - Årsak-virkningsdiagram

De prissatte virkningene omfatter investerings- og driftskostnader og er brutt ned i kategorier som vises i nedbrytningsstrukturen under. I tillegg legges det til skattefinansieringskostnader på samtlige kostnader ettersom alle prissatte kostnader finansieres over statsbudsjettet.



Figur 7-2 Oversikt over prosjektnedbrytningsstruktur

I tillegg til de prissatte virkningene vil konseptene utløse virkninger som er krevende å prissette. De viktigste ikke-prissatte virkningene er virkninger som kommer av endret

nasjonal kontroll og endret funksjonalitet og fleksibilitet. Overordnet vil virkninger av endret nasjonal kontroll være knyttet til endret risiko for bortfall eller integritetsbrudd i sentrale offentlige tjenester i fred, krise og væpnet konflikt. Endret funksjonalitet og fleksibilitet vil kunne påvirke de statlige virksomhetenes tjenesteproduksjon og de som benytter seg av tjenestene de produserer. Disse virkningene er beskrevet som ikke-prissatte virkninger. Det er vanskelig å vurdere hvilken konkret betydning disse virkningene har, men de har likevel stor innvirkning på den samlede samfunnsøkonomiske lønnsomheten av konseptene.

I vurderingene av disse virkningene etterstrebes det å følge de samme prinsippene som for de prissatte virkningene ved å vurdere⁴⁸ hvor mange som blir berørt, hvordan de blir påvirket og hvilke verdier/tap det medfører. Som for alle ikke-prissatte virkninger er det stor usikkerhet rundt alle disse tre parameterne og det har ikke vært grunnlag for å kvantifisere dem. I vurderingene av de ikke-prissatte virkningene er det derfor gjennomført mer overordnede vurderinger som, basert på den informasjonen som har vært tilgjengelig, forsøker å synliggjøre virkninger som *kan* oppstå og *mulig* omfang av disse virkningene.

I delkapitlene nedenfor gis først en nærmere beskrivelse av de alternativene som er analysert og hvilke overordnede konsekvenser de vil ha for hvordan de berørte virksomhetene lagrer og behandler beskyttelsesverdige data og systemer. Deretter gis en beskrivelse av prissatte og ikke-prissatte samfunnsøkonomiske virkninger og usikkerheten som er forbundet med resultatene. Til slutt gis en samlet vurdering og anbefaling.

7.1 Beskrivelse av analyserte alternativer

Som beskrevet i mulighetsstudien er det fem konsepter som er tatt med til nærmere vurdering i alternativanalysen, i tillegg til nullalternativet. I alle konsepter ligger det til grunn en tydeliggjøring og skjerping av krav til nasjonal kontroll over beskyttelsesverdige data og systemer, i tillegg til ulike løsninger for at statlige virksomheter kan lagre og behandle sine beskyttelsesverdige data og systemer. Med utgangspunkt i behovsanalysen legger vi til grunn at det er beskyttelsesverdig data som er særskilt viktig i krise og væpnet konflikt som bør inngå i en nasjonal sky. Dette er nærmere beskrevet i kapittel 3.1 om behov for å sikre beskyttelsesverdige data og systemer i hele krisespekteret. Basert på den informasjonen utredningen har innhentet og de analysene som er gjennomført i behovsanalysen utgjør dette om lag [redacted] av de dataene statsforvaltningen besitter med en forventet årlig vekst i datavolumer på 10 prosent. Dette er datavolumene som er lagt til grunn vurderingene av alle konsepter.

Konsept 0 – Nullalternativet

I nullalternativet står virksomhetene i statsforvaltningen fritt til å ta i bruk skyløsninger innenfor rammene av eksisterende regelverk i tråd med dagens praksis. Dette viderefører et sammensatt bilde hvor:

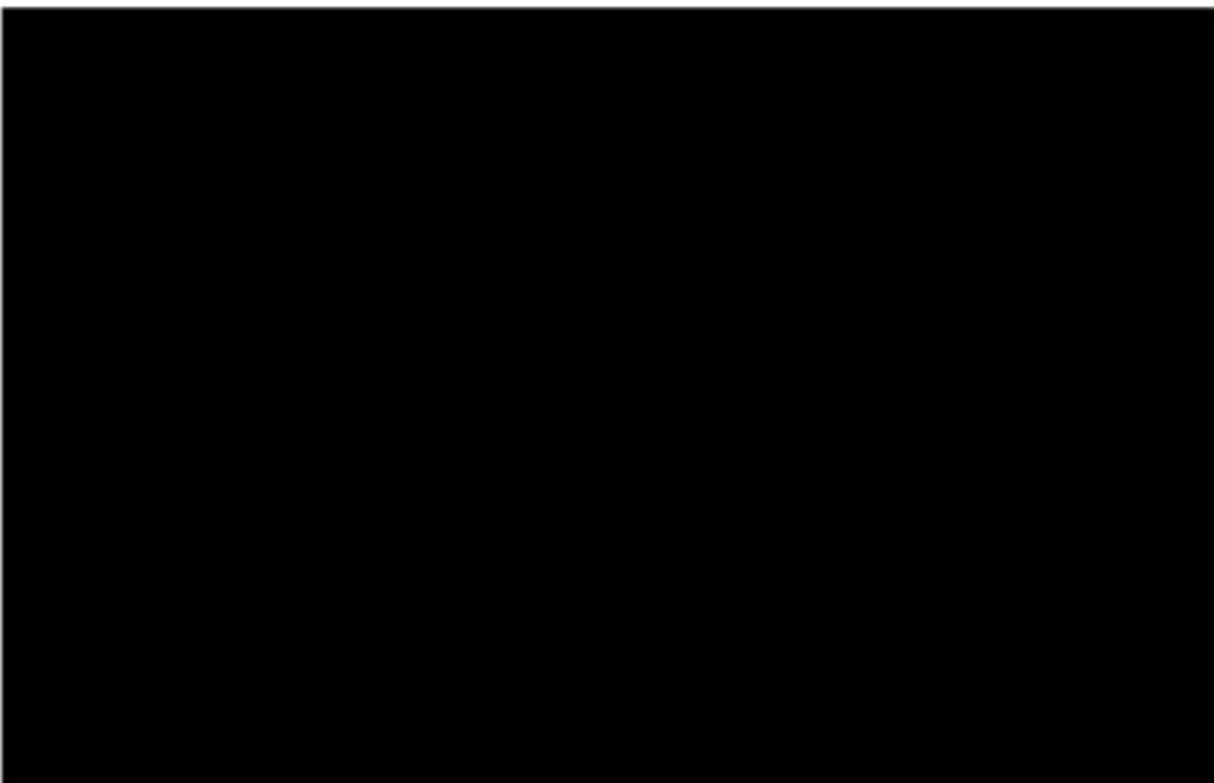
- Noen virksomheter legger opp til å videreføre eller etablere egne IKT-tjenester på egendriftede eller tjenesteutsatte plattformer

⁴⁸ Rapport - Forbedring av metode for vurdering av ikke-prissatte virkninger i samfunnsøkonomiske analyser, Menon, 2020

- Andre har kjøpt eller planlegger å kjøpe lukkede skytjenester hos kommersielle aktører
- Mange benytter eller planlegger å benytte allmenne skytjenester

Dette betyr at staten fortsetter å benytte en rekke tjenesteleverandører og teknologier som opererer i parallell og som er uavhengig av hverandre. Dette fører til vedvarende fragmenterte løsninger hvor staten samlet sett har begrenset kontroll på hva som ligger hvor av beskyttelsesverdige data og systemer.

Basert på den informasjonen vi har innhentet gjennom problembeskrivelsen og behovsanalysen forventes det at en økende andel av beskyttelsesverdige data og systemer vil flyttes til skybaserte løsninger gjennom analyseperioden. Framskrivninger av dataomfang og hvordan det fordeler seg på ulike tjenestemodeller i nullalternativet er vist i figuren under.



Basert på disse framskrivningene, vil 80 prosent av beskyttelsesverdige data og systemer være i skybaserte løsninger i 2032 med en tilnærmet lik fordeling mellom allmenne og lukkede skytjenester. De resterende 20 prosentene av datavolumet forventes å forbli på egendriftede plattformbaserte løsninger. Denne fordelingen forventes deretter å holde seg stabil utover analyseperioden mens de samlede volumene av data og systemer forventes å vokse kontinuerlig.

I analysene er de samlede kostnadene for kjøp, drift og forvaltning av beskyttelsesverdige data og systemer for de 185 statlige virksomhetene vurdert til i overkant av [REDACTED]. Dette ligger til grunn for nullalternativet, og kostnadene er blant annet basert

på tall fra Statsregnskapet og priser fra kommersielle skyleverandører⁴⁹. Samlet over hele analyseperioden, neddiskontert og justert for usikkerhet, innebærer det en total kostnad i nåverdi på [REDACTED] kroner av disse er knyttet til kjøp av skytjenester, mens resten er knyttet til egendrivede og tjenesteutsatte plattformer.

I nullalternativet vil de statlige virksomhetene forholde seg til prisene som skapes i markedet. Vi antar at det kun er noen av de større statlige virksomhetene som i dag kan dra nytte av stordriftsfordeler da det ikke er en større samordning av data i dagens situasjon. Dette er inkludert i prisene vi benytter i nullalternativet.

Konsept 1 – Reguleringskonseptet

Reguleringskonseptet handler om å samle, klargjøre og eventuelt styrke dagens regelverk, inkludert nødvendige tiltak. I dette konseptet står virksomhetene i statsforvaltningen fritt til å ta i bruk skyløsninger innenfor rammene av regelverket. Konseptet inkluderer å etablere / styrke en statlig tilsynsmyndighet og rådgivningstjeneste, med mulighet for en sertifiseringsordning.

Konseptet innebærer at statsforvaltningen fortsetter å benytte ulike tjenesteleverandører og teknologier som opererer i parallell og uavhengig av hverandre. Hver enkelt virksomhet må finne og anskaffe egne løsninger som er i tråd med de spesifiserte kravene. Kravene vil blant annet kunne omfatte bruk av norske datasentre på norsk jord med personell underlagt norsk jurisdiksjon. De virksomhetene som ikke opererer i tråd med kravene som stilles, må migrere ut av de skyløsningene de har eller tilpasse eksisterende avtaler.

I tråd med vurderingene i problembeskrivelsen og behovsanalysen gir allmenne skyløsninger, slik disse tjenestene leveres i dag, lav grad av nasjonal kontroll. Det er derfor lagt til grunn at de som benytter slike løsninger for beskyttelsesverdige data og systemer ikke ivaretar den graden av nasjonal kontroll som innføres i alle konsepter. Det innebærer at alle statlige virksomheter som bruker slike løsninger i nullalternativet må migrere over til lukkede skyløsninger som imøtekommer kravene. Av de som befinner seg i lukkede skyløsninger legger vi til grunn at omtrent halvparten er i henhold til kravene og kan forbli på sine eksisterende løsninger. Resterende må reforhandle avtaler med sine skyleverandører eller migrere over til andre løsninger. Dermed må kun noen virksomheter migrere alt av data og systemer til en godkjent lukket skytjeneste, mens andre kun trenger å gjøre mindre tilpasninger. Det legges videre til grunn at virksomheter som har IKT-tjenester på egendrivede plattformer i hovedsak benytter norske datasentre på norsk jord med personell underlagt norsk jurisdiksjon, og at disse virksomhetene derfor tilfredsstiller kravene som presiseres i regelverket. Dette er nærmere beskrevet i Vedlegg G – Estimering av konsepter.

Som i nullalternativet vil de statlige virksomhetene måtte forholde seg til prisene som skapes i markedet, men tjenestepriene vil øke som følge av at skjerpede krav til nasjonal kontroll vil føre til økte kostnader for leverandørene. Ettersom det i dette konseptet ikke gjøres samordnede innkjøp, vil det som for nullalternativet i all hovedsak være de større statlige virksomhetene som vil kunne oppnå vesentlige stordriftsfordeler og rabatter.

Avhengig av behovet for nye regler og hvilke krav som stilles, kan kravene også få betydning for andre virksomheter utenfor statsforvaltningen som forvalter data og systemer, som kan

⁴⁹ Se mer detaljer i vedlegg G Estimering av konsepter.

anses som beskyttelsesverdige. Hvorvidt kravene også vil gjelde for andre virksomheter, må vurderes i det videre arbeidet. I tråd med avgrensningene i mandatet har vi derfor lagt til grunn at det er de beskyttelsesverdige dataene og systemene i statsforvaltningen som primært omfattes av kravene som stilles.

Selv om konseptet trolig vil føre til vedvarende fragmenterte løsninger, vil skjerpet regulering, økt veiledning og mer statlig tilsyn føre til noe bedre nasjonal kontroll enn i nullalternativet.

Konsept 2 – Statlig skymegler

I dette konseptet organiserer staten en skytjeneste som leveres av et fåtall (5-10) eksisterende statlig eide tjenesteleverandører. De samme regelverksendringene som er beskrevet i konsept 1 er lagt til grunn for dette konseptet. Videre vil en sentral enhet få ansvar for å operere som en tjenestemegler mellom enkeltvirksomheter og utvalgte statlige tjenesteleverandører. Disse tjenesteleverandørene etablerer, videreutvikler og tilbyr et bredt tilbud av ulike pakker av skytjenester i parallell. De står fritt til å inngå nødvendige partneravtaler med underleverandører for å etablere og videreutvikle lukkede skytjenester. Virksomhetene er fortsatt underlagt sine respektive departementer med egne styringslinjer og budsjettprosesser, og kan (når lovverket tillater det) levere tjenester også utenfor egen sektor.

Det er lagt til grunn at de statlige tjenesteleverandørene utnytter eksisterende infrastruktur og datasentre, men at det vil være behov for noen investeringer for å dekke et økt kapasitetsbehov når de statlige tjenesteleverandørene skal levere til flere statlige virksomheter. Det er også inkludert løpende driftskostnader for datasentrene som det økte behovet utløser. Konseptet omfatter infrastruktur-, plattform- og applikasjonstjenester (IaaS, PaaS og SaaS) og all data skal lagres og behandles av de statlige tjenesteleverandørene.

I dette konseptet vil flere tjenesteleveranser være samordnet og man kan i større grad oppnå stordriftsfordeler enn i konsept 1. Disse stordriftsfordelene kommer i form av at noe av det administrative arbeidet kan sentraliseres. Infrastrukturen (IaaS-laget) bygges og driftes av de statlige tjenesteleverandørene og eventuelle stordriftsfordeler ved å samordne dette arbeidet internt i statlig sektor er innbakt disse i kostnadene.

Vi legger til grunn at alle de 185 statlige virksomhetene flytter sine beskyttelsesverdige data og systemer som ligger i skyen i nullalternativet, over til de statlige tjenesteleverandørene. Det gir høyere grad av nasjonal kontroll enn i konsept 1, men også økte migreringskostnader. Anskaffelseskostnadene er imidlertid lavere som følge av større samordning på tvers av virksomhetene.

Konsept 3 – Lukket statlig sky

Konsept 3 innebærer at staten enten etablerer en ny eller gir en eksisterende statlig virksomhet ansvar for å eie og drifte en lukket skyløsning i Norge, underlagt norsk jurisdiksjon. Virksomheten benytter eksisterende datasentre, men gjør nødvendige tekniske tilpasninger for å sikre at disse oppfyller kravene om nasjonal kontroll. Videre vil det være behov for investeringer i utstyr for å levere tjenester og sikre tilstrekkelig kapasitet. For å sikre redundans er det lagt til grunn [REDAKERT] med [REDAKERT] av den totale datasenterkapasiteten som er nødvendig ved analyseperiodens slutt. Det tas altså høyde for

en årlig vekst i mengde data allerede ved etableringen av datasentrene. Investeringer i hardware skaleres opp i takt med migrering til nasjonal sky. Konseptet omfatter infrastruktur-, plattform- og applikasjonstjenester (IaaS, PaaS og SaaS) og all data skal lagres og behandles på den nasjonale plattformen., plattform- og applikasjonstjenester (IaaS, PaaS og SaaS) og all data skal lagres og behandles på den nasjonale plattformen.

Konseptet innebærer sterk statlig styring og høy grad av nasjonal kontroll. Vi forutsetter at alle de 185 statlige virksomhetene flytter sine beskyttelsesverdige data og systemer over i en lukket statlig sky, med unntak det som blir værende på egendrevne plattformer. I dette konseptet kan man oppnå enda større administrative stordriftsfordeler enn i konsept 2 da mer data og systemer er samlet ett sted. Staten har også mulighet til å utnytte ressursene bedre, og eventuelle stordriftsfordeler ved å samordne arbeidet internt i statlig sektor er innbakt disse i kostandene. I tillegg reduseres den administrative kostnaden (anskaffelseskostnadene) som tilfaller alle de statlige virksomhetene i likhet med i konsept 2. I dette konseptet gjøres det store investeringer ved etableringen av datasentrene, og datasentrene som etableres tar høyde for all beskyttelsesverdig data, samt en årlig vekst i mengde data ut analyseperioden.

Konsept 4 – Lukket kommersiell sky

I konsept 4 gir man en statlig enhet ansvar for å inngå langsiktige avtaler med en eller et fåtall kommersielle aktører som eier, leverer, videreutvikler og drifter skyløsningene. Det stilles spesifikke krav knyttet til nasjonal kontroll av skytjenestene som leverandørene må tilfredsstille og gi garantier for.

Det bygges opp en sentral statlig organisasjon for å styre og videreutvikle samarbeidet med leverandørene. Løsningen vil være basert på at leverandørene forplikter seg til å benytte en drifts- og forvaltningsorganisasjon på norsk jord underlagt norsk jurisdiksjon. Konseptet omfatter infrastruktur-, plattform- og applikasjonstjenester (IaaS, PaaS og SaaS) og all data skal lagres og behandles på den nasjonale plattformen.

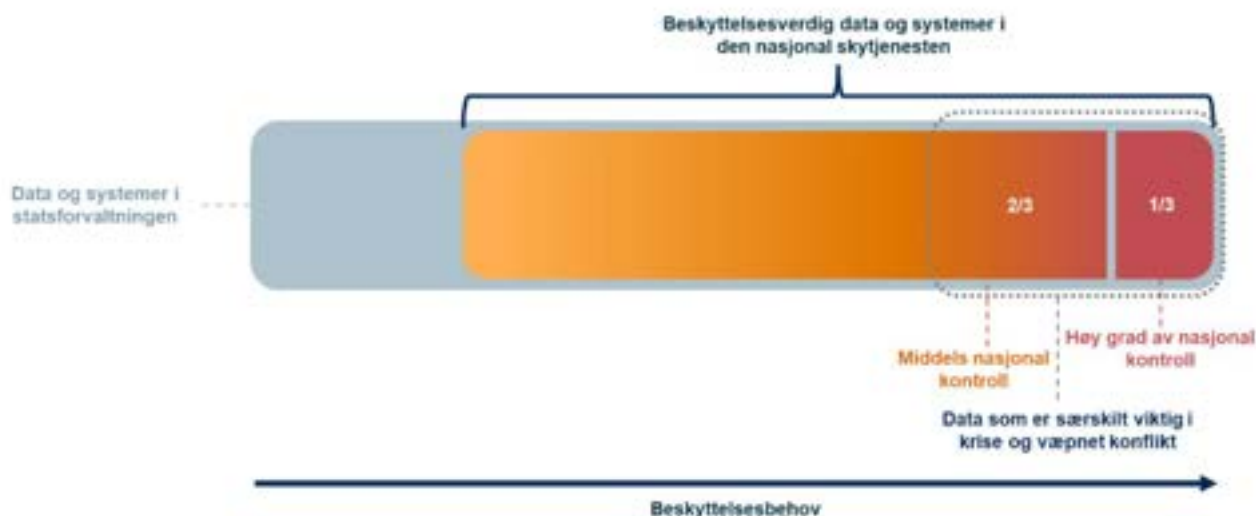
Vi forutsetter at alle de 185 statlige virksomhetene flytter sine beskyttelsesverdige data og systemer som ligger i sky i nullalternativet over i den nasjonale kommersielle skyen. Det gir større nasjonal kontroll over beskyttelsesverdige data og systemer enn i nullalternativet, men bruk av private tjenesteleverandører gir mindre kontroll enn i K3.

I dette konseptet utløses økte stordriftsfordeler som reduserer kostnadene som følge av samordnede innkjøp og leveranser for IaaS-laget. Det er grunnet at ressursene hos de få kommersielle aktørene som leverer den nasjonale skyen kan utnyttes bedre. I tillegg vil deler av de administrative kostnadene (anskaffelseskostnadene) reduseres i hver statlig virksomhet fordi oppgavene sentraliseres i større grad og ressursene kan utnyttes mer effektivt. Dette er i likhet med i konsept 2 og 3.

Konsept 7 – Kombinasjonskonseptet

Konsept 7 er en kombinasjon av konsept 3 og konsept 4. Beskyttelsesverdige data med behov for høy grad av nasjonal kontroll, lagres og behandles i lukket statlig sky (som K3). Andre beskyttelsesverdige data kan virksomhetene velge å lagre og behandle i lukket kommersiell sky (som K4) med middels grad av nasjonal kontroll, ut fra en konkret vurdering av deres behov for sikkerhet og funksjonalitet.

Det er lagt til grunn at om lag 1/3 av det totale datavolumet lagres og behandles i en lukket statlig sky, mens 2/3 skal håndteres i en lukket kommersiell sky, som vist i figuren under.



Figur 7-4 Fordeling mellom data og systemer i K7

Konseptet innebærer at det er en statlig virksomhet som eier og drifter den statlige skyløsningen i Norge, underlagt norsk jurisdiksjon, i tillegg til å ha ansvar for å inngå langsiktige avtaler om tjenestekjøp med kommersielle aktører. Dette konseptet medfører derfor en større varig organisasjon enn konsept 3 og 4 hver for seg.

Vi forutsetter at hele statsforvaltningen flytter sine beskyttelsesverdige data og systemer som ligger i sky i nullalternativet over i den todelte nasjonale skyløsningen. I konsept 7 vil man også oppnå stordriftsfordeler, men totalt utgjør dette mindre enn i konsept 4.

7.2 Vurdering av samfunnsøkonomiske virkninger

Virkningene av konseptene kan i all hovedsak knyttes opp mot fire overordnede kategorier:

- Investeringskostnader
- Driftskostnader
- Virkninger av endret nasjonal kontroll
- Virkninger av endret funksjonalitet og fleksibilitet.

Dette er virkninger som i hovedsak påvirker statsforvaltningen som behandler beskyttelsesverdig data og systemer.

De prissatte virkningene omfatter investerings- og driftskostnader. I tillegg legges det til skattefinansieringskostnader på samtlige kostnader ettersom dette vil finansieres over statsbudsjettet. I tillegg til de prissatte virkningene vil konseptene utløse virkninger som er krevende å prissette. De viktigste ikke-prissatte virkningene er virkninger som kommer av endret nasjonal kontroll og endret funksjonalitet og fleksibilitet.

Resultatene som kommer frem i tabellen under oppsummerer de prissatte og de ikke-prissatte virkningene for de fem konseptene (intern rangering for hver virkning er oppgitt i parentes).

Tabell 7-1 - Oppsummering av prissatte og ikke-prissatte virkninger relativt til nullalternativet med rangering i parentes. De ikke-prissatte virkningene vurderes på en fem-delt skala (svært liten, liten, middels, stor, svært stor)

Virkning	Konsept 1	Konsept 2	Konsept 3	Konsept 4	Konsept 7
Prissatte virkninger, MNOK i 2022-kroner, ekskl. mva.					
Ikke-prissatte virkninger					
Virkninger av økt nasjonal kontroll	Liten positiv virkning (5)	Middels positiv virkning (3)	Svært stor positiv virkning (1)	Middels positiv virkning (3)	Stor positiv virkning (2)
Virkninger av endret funksjonalitet / fleksibilitet	Middels negativ virkning (5)	Liten negativ virkning (3)	Liten negativ virkning (3)	Svært liten negativ virkning (1)	Svært liten negativ virkning (2)

I delkapitlene nedenfor gir vi en overordnet beskrivelse og forklaring av analysen. Overordnede forutsetninger for analysen er gitt i boksen nedenfor, mens detaljbeskrivelser av beregningsforutsetninger og kilder er nærmere beskrevet i vedlegg G – Estimering av konsepter.

Overordnede forutsetninger

Beregningsforutsetningene i denne konseptvalgutredningen følger Finansdepartementets rundskriv R-109/21. Under gis en oversikt over de sentrale forutsetningene som ligger til grunn for analysen.

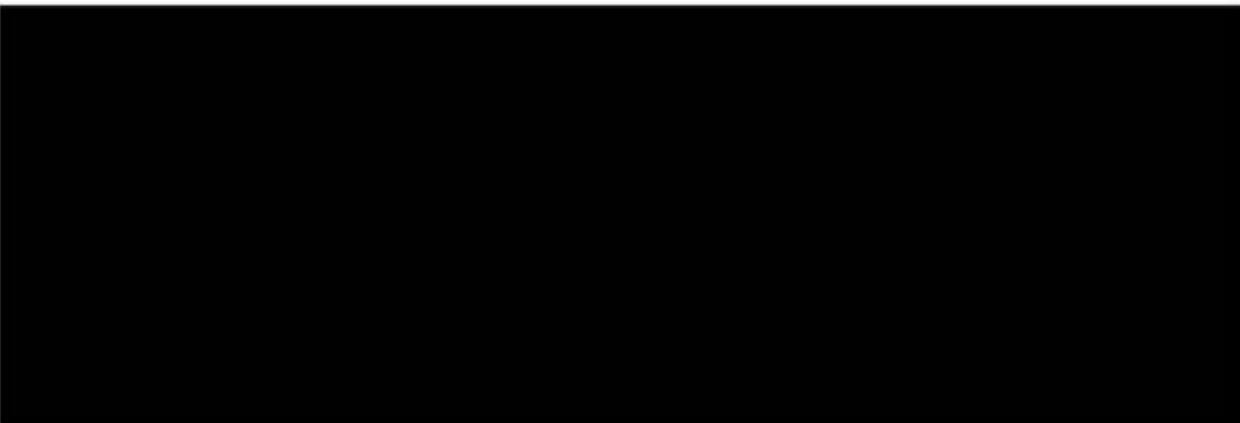
- 1 **Investeringsperiode:** Investeringsperioden er ulik for de ulike konseptene. Den er 3,5 år for konsept 1, 5,5 år for konsept 2, 4 år for konsept 3 og konsept 4.
- 2 **Levetid:** Vi legger til grunn at konsept 2 vil ha en levetid på ti år. For å sikre at alle konsepter analyseres over den samme analyseperioden, i og med at de ulike konseptene vil kunne settes i produksjon på ulike tidspunkt, har vi lagt inn reinvesteringer i relevante konsepter for å sikre at disse får en levetid som er lang nok til at alle konseptenes levetid er uttømt ved utløpet av 2038.
- 3 **Datamengde:** Det er lagt til grunn samme mengde data i alle konsepter. Mengde data som er relevant for nasjonal sky tar utgangspunkt i datamengde i statlige virksomheter i dag, og en årlig vekst lik 10 prosent ut analyseperioden. For mer detaljer knyttet til beregning av datamengde vises det til vedlegg G, kapittel 3.1/ 3.2.
- 4 **Analyseperiode og kroneverdi:** Det er lagt til grunn en analyseperiode på 16 år, fra 2023 til 2038. Dette tilsvarer minimum 10 år med gevinstrealisering for hvert konsept. Alle beløp er diskontert til 2022, og alle beløp er oppgitt i 2022-kroner.
- 5 **Restverdi:** Restverdier er markedsverdien av de eiendelene konseptene innebærer investeringer i, ved utløpet av analyseperioden. Datasenter har levetid lik 20 år og det er derfor beregnet restverdier for datasenter. Hardware har levetid lik 5 år, med kontinuerlige reinvesteringer, og det er derfor også beregnet restverdier for disse investeringene. Restverdier inngår i beregning av samfunnsøkonomisk kostnad for konsept 2, 3 og 7.
- 6 **Skattefinansieringskostnad:** I henhold til R-109/21 skal det for alle tiltak som finansieres over offentlige budsjetter beregnes en skattefinansieringskostnad som inngår i analysen. Skattefinansieringskostnaden er den marginale kostnaden ved å hente inn en ekstra skattekrone og den er satt til 20 øre per krone. Denne skal benyttes av alle sektorer. Alle offentlige budsjettvirkninger er derfor tillagt en skattefinansieringskostnad på 20 prosent.
- 7 **Kalkulasjonspriser:** I beregningen av de prissatte virkningene er det benyttet antatte markedspriser for de ulike tjenestekomponentene som inngår i hvert konsept og brutto reallønn (inkludert arbeidsgiveravgift og administrative kostnader).

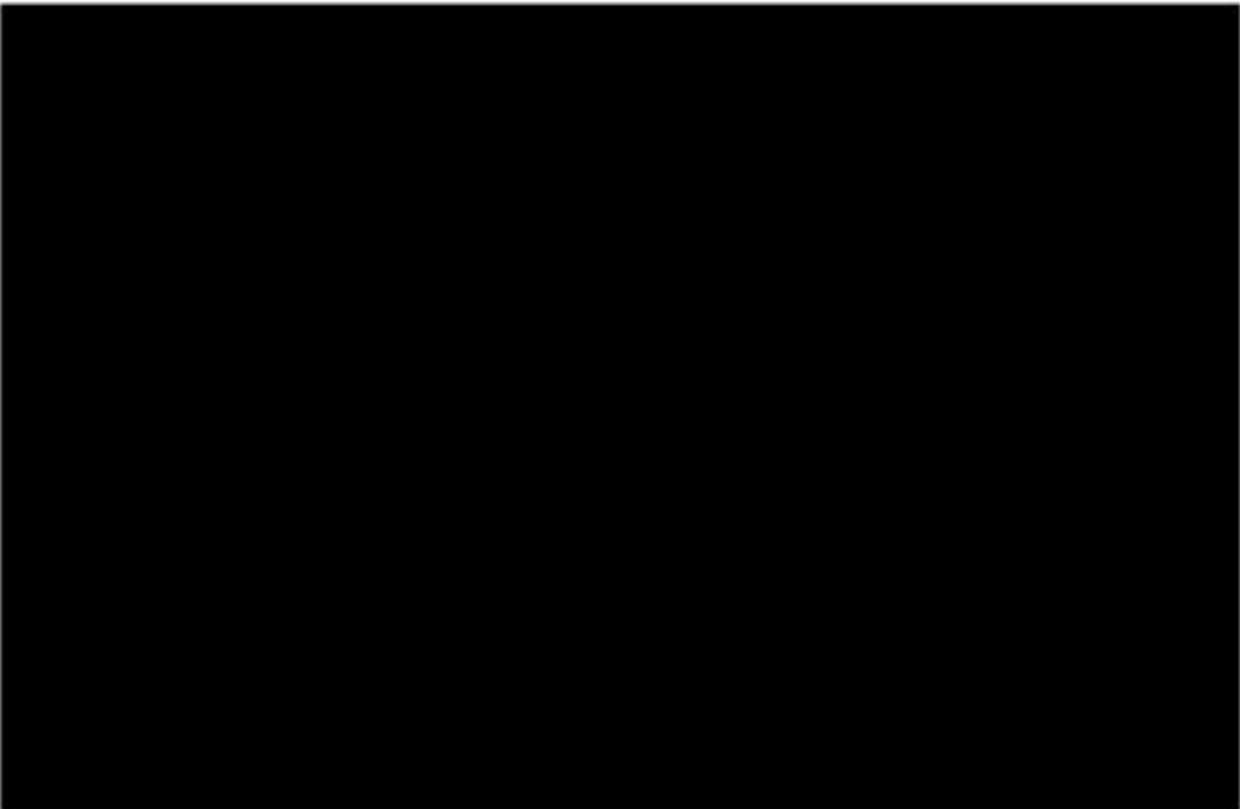
Overordnede forutsetninger forts.

- **Kalkulasjonsrente:** Det benyttes en standard risikojustert kalkulasjonsrente på 4,0 prosent, i henhold til rundskriv R-109/21. Enkelte av konseptene har elementer som kan vurderes å være i direkte konkurranse med private aktører. I slike tilfeller skal det i utgangspunktet benyttes en kalkulasjonsrente tilsvarende de private aktørenes normalavkastningskrav. Det er ikke gjort i denne KUVen fordi det kun er kostnadssiden ved konseptene som er verdsatt. Bruk av forskjellige kalkulasjonsrente vil da føre til at nåverdien av kostnaden ved konseptene som driftes i statlig egenregi framstår lavere, sett opp mot øvrige konsepter, enn ved bruk av samme kalkulasjonsrente. Det er etter utredningens vurdering ikke i tråd med intensjonen bak føringen om justering av kalkulasjonsrenten for konsepter i direkte konkurranse med private aktører.
- **Arbeidsgiveravgift og merverdi:** I den samfunnsøkonomiske analysen er kostnader uten merverdiavgift. Tid i arbeid skal verdsettes til arbeidsgivers betalingsvillighet for tiden, altså brutto timelønn inkludert arbeidsgiveravgift og andre administrative kostnader, her satt til 30 prosent.
- **Realprisjustering:** Det er ikke lagt til grunn realprisjustering av lønnskostnader. For å realprisjustere lønnskostnader er det ikke tilstrekkelig at du forventer at alternativverdien av arbeidskraft vil øke over tid i forhold til andre varer og tjenester. Hvis arbeidskraften også blir mer effektiv, trenger ikke de samlede reallønnskostnadene å øke selv om reallønnen per enhet arbeidsinnsats øker. For å begrunne en realprisjustering av tid i arbeid må det derfor også være begrenset potensial for at arbeidskraften ikke kan utføre sine tjenester mer effektivt i framtiden, for eksempel med økt humankapital. Det finner vi ikke et solid teoretisk og empirisk grunnlag for å anta i denne sammenheng

7.2.1 Prissatte virkninger

Tabellen nedenfor gir en sammenstilling av de prissatte virkningene som følger av konseptene. Alle tall er presentert som nåverdi av forventningsverdier over hele analyseperioden. Hvordan konseptene er estimert er utførlig beskrevet i vedlegg G – Estimering av konsepter. Usikkerhetsvurderingene som gir forventningsverdiene er omtalt på et overordnet nivå i kapittel 7.3, og mer detaljert i vedlegg H – Usikkerhetsanalyse.





Basert på prissatte virkninger alene er det konsept 4 som medfører de laveste samfunnsøkonomiske kostnadene utover nullalternativet. Årsaken er at konseptet legger til grunn størst grad av samordning, hvilket legger til rette for at både leverandører og kundene av den nasjonale skyen kan oppnå vesentlige stordriftsfordeler. Konsept 1 er det nest-billigste alternativet som følge av lite usikkerhet i realiseringen, men gir økt tjenestepris og lite stordriftsfordeler. Konsept 2 drar nytte av en del stordriftsfordeler, men krever også investeringer som drar ned lønnsomheten. I tillegg er usikkerheten stor, noe som gjør at den forventede kostnadsvirkningen blir stor. Konsept 7 er en kombinasjon av konsept 3 og 4 og plasserer seg kostnadmessig mellom disse konseptene. Konsept 3 er det nest-dyreste alternativet drevet av vesentlige investeringer i hardware og etablering av datasenter.

En nærmere beskrivelse av de ulike virkningene og forskjellen mellom de ulike alternativene følger i avsnittene nedenfor.

Kostnadspost 1 – Datasenter



Kostnadspost 2 – Hardware

Kostnadsposten dekker kostnaden for fysiske komponenter som er nødvendig for driften av et datasenter. Dette inkluderer servere, serverracker, nettverkutstyr som router og switcher samt utstyr til sikkerhetskopiering som harddisker. Mengden hardware og dermed kostnaden kan oppskaleres etter behov.

Investeringer og reinvesteringer i hardware inngår i konsept 2, 3 og 7. I konsept 2 legges det til grunn at det trengs mindre investering i hardware fordi man kan utnytte noe av de statlige tjenesteleverandørenes eksisterende kapasitet. Dette sikrer redundansen og innkjøpet av hardware tilsvarer følgelig det til enhver tid reelle behovet.

Videre har hardware en levetid på 5 år og det ligger derfor til grunn en periodisering av innkjøp og en reinvestering som drar opp kostnadene. Det er derfor også beregnet en restverdi av hardware ved analyseslutt.

Kostnadspost 3 – Tjenestelag

Denne kostnadsposten omfatter kostnader for de tre (mest vanlige) tjenestemodellene for skytjenester, IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service). I de konseptene hvor tjenestene leveres fra kommersielle tjenesteleverandører dekker kostnaden i tjenestelaget også leverandørens kostnader knyttet til datasenter, hardware, nødvendig programvare og påfølgende drift av tjenestene. Dette skyldes at det for kommersielle skytjenester oppgis en pris for et tjenestekjøp, der prisen for hele tjenesten inngår. Dette gjelder for både IaaS, PaaS og SaaS-tjenester.

Prisene fra leverandørene er gitt basert på behovet for prosessering, lagring og support. Konsept 3 innebærer at staten etablerer eller gir ansvar til en virksomhet som blir tjenesteleverandør og i tjenestelaget inngår derfor kun SaaS-kostnad. Kostnadene for IaaS og PaaS ligger innebygd i kostnadene for datasenter, hardware og mellomvare, henholdsvis kostnadspost 1 og kostnadspost 2 i nedbrytningsstrukturen. For konsept 2 vil de statlige tjenesteleverandørene tilby IaaS-tjenester og kostnadsberegningene for konseptet tar utgangspunkt i samme forutsetninger som for konsept 3. Når det kommer til PaaS- og SaaS-tjenester beregnes disse på tilsvarende måte som i K1 og K4, da det ikke er lagt til grunn at de statlige tjenesteleverandørene skal utvikle og levere disse tjenestene selv.

Prisen for tjenestekjøp er høyere enn i nullalternativet for alle konsepter som følge av at skjerpede krav til nasjonal kontroll vil føre til økte kostnader for leverandørene. Prispåslaget tar utgangspunkt i svarene kommersielle leverandører av skytjenester har oppgitt for ulike tjenester med forskjellige krav til nasjonal kontroll i RFlen som er sendt ut i regi av utredningen. I konsept 4 og 7 vil det imidlertid kunne utløses økte stordriftsfordeler som reduserer kostnadene som følge av samordnede innkjøp og leveranser for IaaS-laget.

Kostnadspost 4 – Prosjekt- og transisjonskostnader

Kostnaden omfatter midlertidige aktiviteter som er nødvendig for realisering av konseptene. Dette er kostnader knyttet til prosjektorganisasjon, sammenstilling og tydeliggjøring av regelverk, KS1, forprosjekt, KS2, migreringskostnader for de som flytter seg fra en sky i nullalternativet og over til noe annet, og anskaffelseskostnader.

Som beskrevet tidligere i kapitlet vil varighet og omfang av prosjektorganisasjonen variere mellom konseptene. For K2 legger vi til grunn en programorganisering. Varigheten for konsept 3 er lenger enn konsept 4 og konsept 2. Vi legger til grunn samme mengde forflytning fra dagens situasjon og ut i sky, men i konsept 1 vil de virksomhetene som er i lukket skytjeneste og som opptre iht. retningslinjene få en lavere migreringskostnad. Det kommer som følge av at enkelte virksomheter kun vil trenge å justere eksisterende avtaler eller migrerer internt mellom datasentre hos samme leverandør. For anskaffelser har konsept 1 en noe høyere kostnad enn resten av konseptene fordi virksomhetene må gjøre anskaffelsene hver for seg. I konsept 2 til konsept 4 vil den sentrale organiseringen gjøre det meste av arbeidet knyttet til anskaffelse av sky, og kostnadene for hver virksomhet er lavere.

Kostnadspost 5 – Varige organisasjonskostnader

Kostnadsposten omfatter de varige organisasjonskostnadene som konseptet medfører. Dette er den ordinære driften og forvaltning av skyen, sikkerhetskopi av dataene i skyen, samt de varige organisatoriske kostnadene som følger av konseptene.

Årsaken til variasjon i denne kostnadsposten er de varige organisasjonskostnadene til konsept 1, konsept 3 og konsept 4 (henholdsvis etablering av tilsynsmyndighet, ny organisasjon «Statlig sky» og administrasjon av skytjenester) og sikkerhetskopi som varierer som følge av stordriftsfordeler i konsept 2 til konsept 4, mens konsept 1 ikke får noen stordriftsfordeler. Den ordinære drift og forvaltningen av skyen er tilsvarende i alle konseptene.

Kostnadspost 6 – Uspesifisert

Kostnadsposten skal reflektere kostnader som erfaringsmessig forventes å påløpe, men som ikke kan identifiseres på tidspunktet estimatet utarbeides, såkalte «kjente ukjente» kostnader. Uspesifiserte kostnader skiller seg fra uforutsette kostnader. Uforutsette kostnader er kostnader som ikke kunne forutses på analysetidspunktet. Uforutsette kostnader forventes å dekkes inn med hjelp av usikkerhetsavsetningen i prosjektet. Det varierer på tvers av konseptene om det er inkludert uspesifiserte kostnader, og det er bare inkludert uspesifiserte kostnader på investeringskostnad.

Denne kostnadsposten følger av den totale investeringskostnaden, da er identifisert flere mulige punkter for uspesifisert. I de andre konseptene er det ikke identifisert konkrete punkter som vil være grunnlag for en uspesifisert faktor.

Skattefinansieringskostnad

Følger av bestemmelsene i rundskriv 109/21 og legges til i hvert av konseptene.

7.2.2 Ikke-prissatte virkninger

Noen av kostnads- og nyttevirkingen som følger av konseptene er krevende å prissette. De viktigste ikke-prissatte virkninger som følger av de forskjellige konseptene er virkninger som kommer av endret nasjonal kontroll og endret funksjonalitet og fleksibilitet.

Overordnet vil virkninger av **endret nasjonal kontroll** være knyttet til endret risiko for integritetsbrudd, konfidensialitetsbrudd eller bortfall av sentrale offentlige tjenester i fred, krise og væpnet konflikt. Dette kan føre til:

- Reduserte kostnader for innbyggere og næringsliv ved bortfall av tjenester
- Økt trygghet for innbyggerne

Endret funksjonalitet og fleksibilitet vil kunne påvirke de statlige virksomhetenes tjenesteproduksjon som vil kunne føre til:

- Endrede kostnader knyttet til produksjonen av tjenester hos de statlige virksomhetene
- Endring i brukerkostnader (tilgjengelighet) og/eller nytte av å bruke tjenestene (verdien av tjenestene) for innbyggere, næringsliv og andre offentlige virksomheter

I tabellen nedenfor har vi oppsummert resultatene fra vurderingen av ikke-prissatte virkninger:

Tabell 7-3 - Oppsummering av ikke-prissatte virkninger relativt til nullalternativet med rangering i parentes. De ikke-prissatte virkningene vurderes på en fem-delt skala (svært liten, liten, middels, stor, svært stor)

Virkning	Konsept 1	Konsept 2	Konsept 3	Konsept 4	Konsept 7
Ikke-prissatte virkninger					
Virkninger av økt nasjonal kontroll	Liten positiv virkning (5)	Middels positiv virkning (3)	Svært stor positiv virkning (1)	Middels positiv virkning (3)	Stor positiv virkning (2)
Virkninger av endret funksjonalitet / fleksibilitet	Middels negativ virkning (5)	Liten negativ virkning (3)	Liten negativ virkning (3)	Svært liten negativ virkning (1)	Svært liten negativ virkning (2)

De to ikke-prissatte virkningene kan variere i form av omfang og alvorlighet for samfunnet. Utredningens vurdering er at det er lite grunnlag for å vurdere hvilke av virkningene som er størst. Konsekvensene av manglende nasjonal kontroll kan i verste fall være katastrofale, men sannsynligheten for hendelser er noe mer begrenset. Den direkte virkningen av tapt produktivitet og fleksibilitet vil nok være vesentlig mindre per aktør som blir berørt, men sannsynlighet for at det inntreffer er høyere og det vil være gjeldende gjennom hele analyseperioden.

Det er vanskelig å vurdere konkret hvilken betydning disse virkningene har, men de kan likevel ha stor betydning for den samlede samfunnsøkonomiske lønnsomheten av

konseptene. I vurderingene av disse virkningene har etterstrebet å følge de samme prinsippene som for de prissatte ved å vurdere⁵⁰:

- Hvor mange blir berørt?
- Hvordan blir de påvirket?
- Hvilke verdier/tap medfører det?

Som for alle ikke-prissatte virkninger er det stor usikkerhet rundt alle disse tre parameterne, og vi har kun hatt grunnlag for å gjøre grove kvalitative vurderinger av dem.

Problemstillingene og konseptene vi vurderer i denne utredningen favner bredt og er rettet mot en rekke ulike virksomheter, systemer og data som benyttes i produksjonen av mange forskjellige offentlige tjenester. Hvordan disse verdikjedene blir påvirket av konseptene og hvilke implikasjoner det har for produksjonen av og kvaliteten på tjenestene som leveres, er avgjørende for å kunne vurdere effekten av både endret nasjonal kontroll, funksjonalitet og fleksibilitet.

Videre er informasjon om hvem som bruker disse tjenestene og til hva, helt avgjørende for å kunne vurdere den samfunnsøkonomiske verdien eller kostnaden konseptene utløser. Dette krever detaljerte verdivurderinger av hvert enkelt system i hver virksomhet, inkludert informasjonen det behandler og dets funksjon opp mot leveranser til samfunnet og eventuelt grunnleggende nasjonale funksjoner. Slike verdivurderinger skal gjennomføres av verdieier, i dette tilfellet virksomhetene selv. Dette er fordi verdieier har den mest helhetlige oversikten over informasjonen og systemene de selv forvalter. Virksomhetene sitter på de nødvendige detaljene rundt kritikaliteten av tjenester og leveranser de står ansvarlige for, som igjen kreves for å gjennomføre en helhetlig verdivurdering. I forbindelse med sikkerhetslovarbeidet utfører virksomhetene skadevurderinger av egen infrastruktur som understøtter grunnleggende nasjonale funksjoner. Basert på dette arbeidet, fremskaffer departementene bedre oversikt over skjermingsverdige ugraderte informasjonssystemer, eventuelt som del av utpekte skjermingsverdige infrastrukturer. Denne oversikten vil normalt inneholde en overordnet beskrivelse av systemets eier, funksjon og konsekvens ved bortfall, men dette arbeidet pågår. En tilsvarende prosess for kartlegging av systemer utenfor rammene av sikkerhetsloven og konsekvenser ved bortfall finnes ikke per i dag. Vi har derfor ikke oversikt over de totale verdiene virksomhetene i statsforvaltningen forvalter i ulike IKT-systemer, og utredningens videre vurderinger påvirkes av dette.

I vurderingene av de ikke-prissatte virkningene har vi derfor gjennomført mer overordnede vurderinger som, basert på den informasjonen vi har tilgjengelig, forsøker å synliggjøre virkninger som *kan* oppstå og *mulig* omfang av disse virkningene.

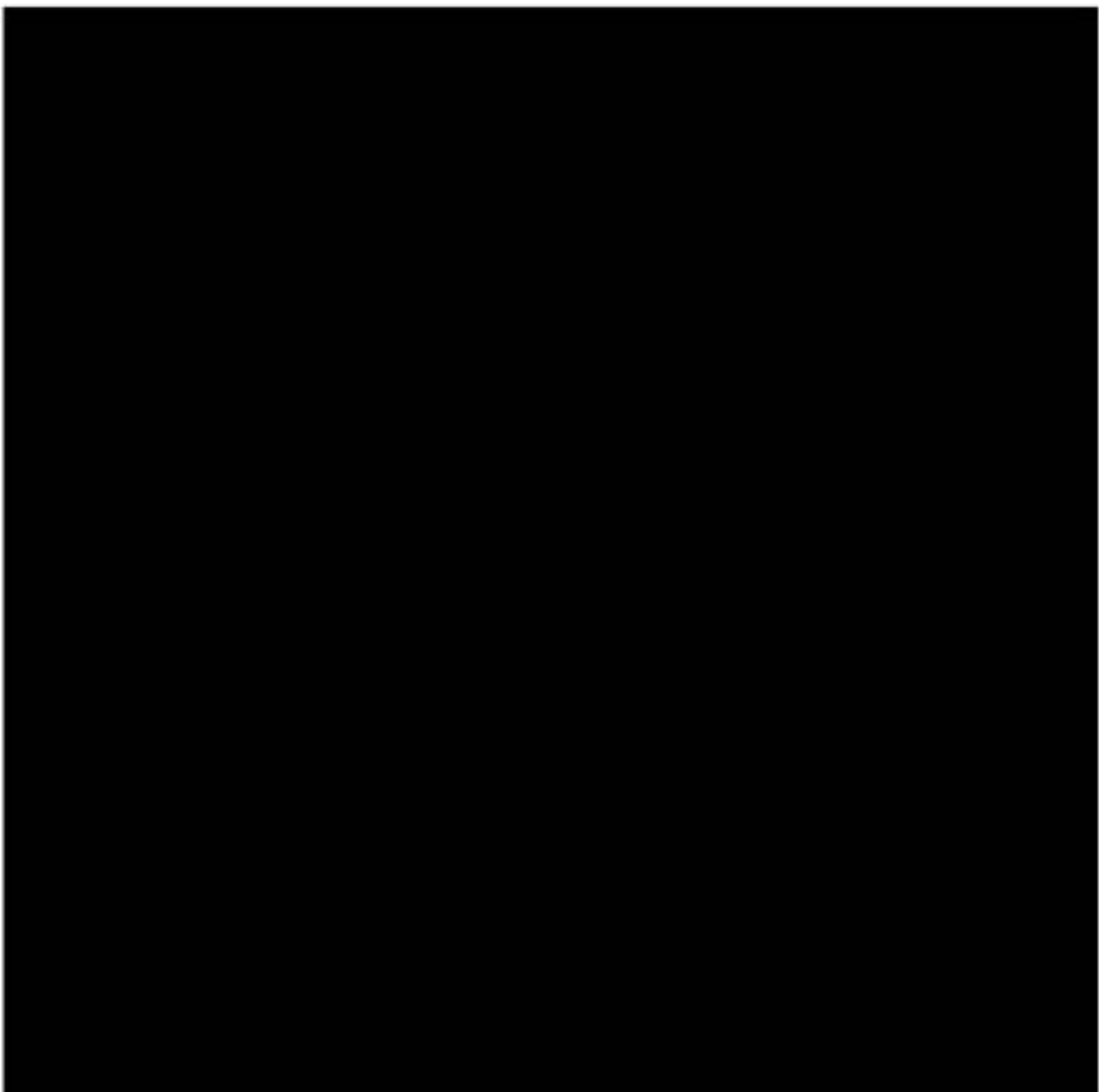
Virkninger av endret nasjonal kontroll

Aktørene som blir berørt av virkningene av endret nasjonal kontroll er de statlige virksomhetene som vil benytte seg av den nasjonale skyen og alle brukere av virksomhetenes tjenester som baserer seg på beskyttelsesverdige data og systemer.

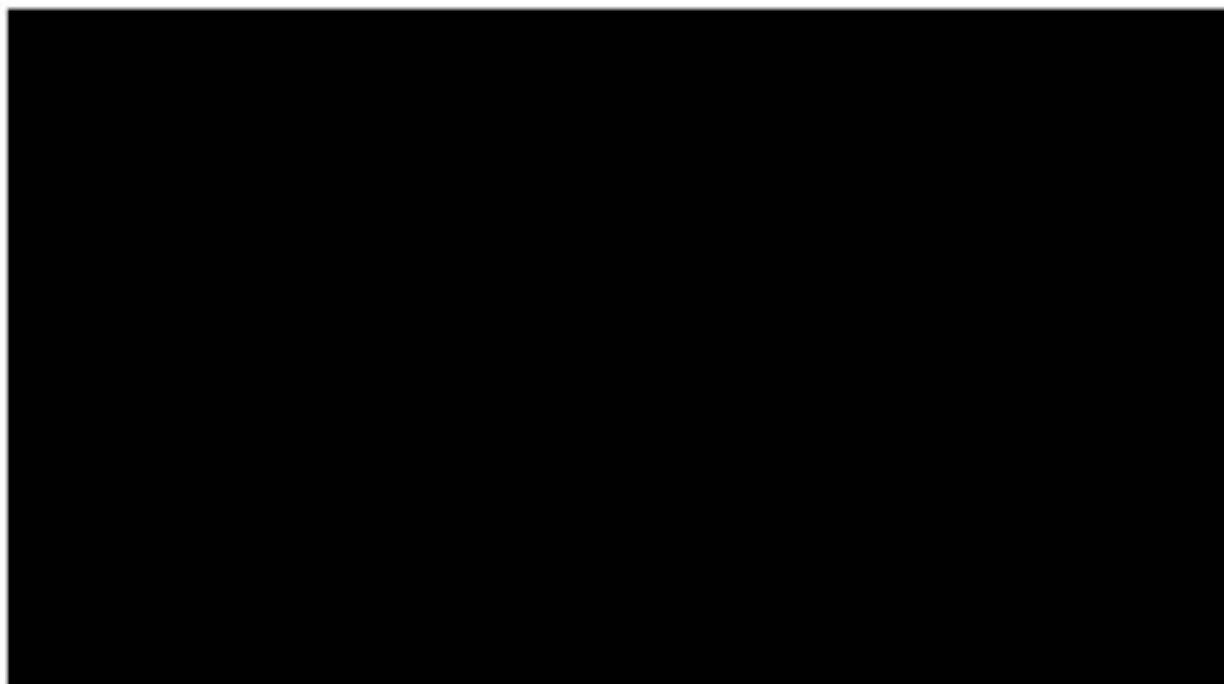
⁵⁰ Rapport - Forbedring av metode for vurdering av ikke-prissatte virkninger i samfunnsøkonomiske analyser, Menon, 2020

Det er foreløpig 185 virksomheter i statsforvaltningen som er identifisert som relevante for den nasjonale skyen. Noen av disse vil trolig velge å bli værende på egendriftede plattformer. Det vil også kunne være virksomheter som potensielt ikke forvalter beskyttelsesverdige data og dermed ikke vil bli berørt. Med utgangspunkt i de 185 relevante virksomhetene anslår vi grovt sett at om lag 49 000 statlige ansatte potensielt kan bli berørt, men vi har ikke detaljert innsikt i hvilke av disse som forvalter beskyttelsesverdige data i sitt arbeid og i hvilket omfang. Anslaget på antall ansatte som blir berørt er nærmere beskrevet og redegjort for i Vedlegg G.

Videre vil alle brukere av virksomhetenes tjenester som baserer seg på beskyttelsesverdige data og systemer kunne bli berørt. Dette kan være hele eller deler av befolkning og næringslivet. Tabellen under viser eksempler på tjenester som kan inneholde beskyttelsesverdige data.



⁵¹ Samfunnets kritiske funksjoner ver. 1, Direktoratet for samfunnssikkerhet og beredskap, 2016



Konseptene i utredningen gir ulike virkninger på nasjonal kontroll. Vedlegg J om nasjonal kontroll gir en oversikt over og beskriver forskjellige faktorer som påvirker graden av nasjonal kontroll. Basert på disse faktorene er det utarbeidet fire dimensjoner som hvert konsept er vurdert opp mot: Statlig styring, avhengigheter, sikkerhetskrav og kontrollmekanismer, og sikkerhetsorganisering. Disse fire dimensjonene er nærmere beskrevet under:

- **Statlig styring** – i hvilken grad staten kan styre eller utøve kontroll over innsatsfaktorene i skytjenesten, og styre videreutviklingen av tjenesten, har betydning for nasjonal kontroll. Statlig styring kan skje indirekte gjennom avtaler og kontrakter, eller direkte gjennom statlig eierskap og statlig drift i verdikjeden. Norsk jurisdiksjon er en forutsetning for statlig styring av betydning.
- **Avhengigheter** – i hvilken grad staten er avhengig av tredjeparter for å drifte eller levere viktige tjenester, herunder avhengigheter til leverandører underlagt andre lands jurisdiksjon, vil ha betydning for sikkerhet med hensyn til verdikjeder. Dette er nært knyttet til statlig styring, men handler i større grad om hvordan avhengigheter er risikovurdert og redusert til et nivå som ivaretar behovet for kontroll og reduserer risikoen for at tredjeparter kan innføre og utnytte sårbarheter i verdikjeden for å få tilgang til verdier, eller legge press på norske myndigheter.
- **Sikkerhetskrav og kontrollmekanismer** – hvor omfattende kravene til sikkerhet og nasjonal kontroll er med hensyn til plassering av datasentre, plassering av drift- og støttefunksjoner og tilgangsstyring, vil ha betydning for graden av nasjonal kontroll. Krav om geografisk plassering av funksjoner i Norge er avgjørende for jurisdiksjonsspørsmålet, som påvirker muligheten norske myndigheter har til å følge opp eller kontrollere sikkerheten, og til å eventuelt gripe inn og sanksjonere aktører som ikke innfrir krav.

⁵² Dette er folkeregisteret, Skatteetaten, jan 2023

- **Sikkerhetsorganisering** – den grunnleggende sikkerheten i en nasjonal skytjeneste kan påvirkes av hvorvidt sikkerhetsstyringen er a) fragmentert og fordelt på mange virksomheter, b) koordinert mellom færre virksomheter, eller c) samordnet og integrert som en del av virksomhetsstyringen i én virksomhet eller organisasjon. Samordnet og integrert sikkerhetsstyring vil generelt bidra til å styrke den grunnleggende IKT-sikkerheten i en virksomhet. Fragmentert sikkerhetsstyring vil på den andre siden kunne undergrave sikkerheten i virksomheten, blant annet ved at roller og ansvar kan være uklare, at oversikt over enheter og brukere kan være mangelfull, eller at oppfølgingen av sikkerhetstiltak generelt er reaktiv eller hendelsesbasert. Denne dimensjonen omfatter også i hvilken grad konsepter legger til rette for å oppnå sikkerhetsmessige stordriftsfordeler i form av et større samlet sikkerhetsmiljø med omfattende bruk av standardisering og automatisering.

Tabellen under viser hvordan de fire dimensjonene er knyttet opp mot ulike grader av nasjonal kontroll. Hvert konsept er vurdert opp mot disse fire dimensjonene.

Tabell 7-4 Dimensjoner ved nasjonal kontroll som er vurdert for hvert konsept i utredningen

	Lav grad av nasjonal kontroll	Middels grad av nasjonal kontroll	Høy grad av nasjonal kontroll
Statlig styring	Tillitsbasert tilnærming, styring gjennom avtaler	Risikobasert leverandøervalg med lav risikoaksept	Direkte statlig styring
Avhengigheter	Omfattende	Balanserte	Minimale
Sikkerhetskrav og kontrollmekanismer	Ordinære markedsvilkår og etablert bransjepraksis	Utvidede krav ut over ordinære markedsvilkår	Omfattende krav og teknisk verifikasjon
Sikkerhetsorganisering	Fragmentert sikkerhetsstyring fordelt på mange virksomheter	Koordinert sikkerhetsstyring mellom færre virksomheter	Enhetlig / samordnet sikkerhetsstyring og sikkerhetsmessige "stordriftsfordeler"

Det er en utbredt oppfatning om at data og systemer i dag er fordelt på et stort antall ulike løsninger i nullalternativet, slik at konsentrasjonsrisikoen i nullalternativet vil være redusert sammenlignet med konsepter som samler beskyttelsesverdige data og systemer i en skytjeneste driftet av én eller få leverandører. Utredningen mener at dette ikke er tilfelle, fordi ulike tjenester i nullalternativet i realiteten driftes ved hjelp av basistjenester som er samlet hos svært få leverandører. Konsentrasjonsrisikoen finnes med andre ord også i nullalternativet i dag, som også er beskrevet i problembeskrivelsen. Nullalternativet har ikke ytterligere egenskaper som øker robustheten. De ulike konseptene åpner for en rekke risikoreduserende tiltak som kan iverksettes for å øke robustheten og redusere konsentrasjonsrisiko i de ulike konseptene.

Konsentrasjonsrisiko er derfor ikke vurdert som en særskilt faktor som skiller nullalternativet fra de ulike konseptene.

Tabellen under gir en rangering av hvert konsept med hensyn til virkningen på nasjonal kontroll.

Tabell 7-5 Rangering av konsepter med hensyn til nasjonal kontroll. De ikke-prissatte virkningene vurderes på en seks-delt skala (svært liten, liten, middels, stor, svært stor)

Vurdering av endret nasjonal kontroll		Forventet samlet konsekvens	Rangering
Konsept 1	Tydeligere krav til lagring og behandling, og tettere oppfølging av hvordan krav ivaretas sammenlignet med nullalternativet	Liten positiv virkning	(5)
Konsept 2	Statlig drift med innslag av tjenestekjøp, fordelt på eksisterende statlige driftsmiljøer og tjenesteleverandører.	Middels positiv virkning	(3)
Konsept 3	Hovedsakelig statlig drift gjennom en statlig virksomhet med lagring og behandling i Norge. Svært strenge krav til tilgangsstyring.	Svært stor positiv virkning	(1)
Konsept 4	Koordinert tjenestekjøp med en risikobasert tilnærming til leverandørvalg og strenge krav til tilgangsstyring. Krav om lagring og behandling i Norge.	Middels positiv virkning	(3)
Konsept 7	De mest kritiske dataene behandles i en statlig driftet sky, mens andre beskyttelsesverdige data behandles i en lukket sky fremskaffet gjennom tjenestekjøp, med krav til lagring og behandling i Norge.	Stor positiv virkning	(2)

I K1 tydeliggjøres krav til lagring og behandling av beskyttelsesverdige data i Norge, inkludert krav om lagring og behandling av data på datasentre i Norge. Dette er avgjørende for jurisdiksjonsspørsmålet, det vil si hvorvidt norsk rett ligger til grunn for lagring og behandling av data. Hver enkelt virksomhet anskaffer fortsatt skytjenester ut fra egne mål og forutsetninger. Staten fører tilsyn med etterlevelse av krav. Staten gir virksomheter råd og veiledning knyttet til valg av løsninger. Konseptet vurderes å gi en liten positiv virkning sammenlignet med nullalternativet, men medfører et fortsatt fragmentert og komplekst landskap med et stort antall ulike leverandører og løsninger. Konseptet gir en liten positiv virkning på graden av nasjonal kontroll, hovedsakelig gjennom tydeligere kravstilling.

I K2 etableres et delt driftskonsept med både statlig drift og tjenestekjøp, herunder drift og støtte fra leverandører. Leverandørvalget er risikobasert med lav risikoaksept. Konseptet legger til rette for kombinasjoner av direkte statlig styring og indirekte styring gjennom avtaler/kontrakter. Konseptet er tilpasset utvidede krav til plassering av datasentre, personell og tilgangsstyring, der datasentre og driftsfunksjoner befinner seg i Norge. Støttefunksjoner med systemtilganger skal også befinne seg i Norge, men det åpnes for avgrensede lese- og

skrivetilganger for enkelte støttefunksjoner fra leverandører i utlandet. Konseptet legger opp til å koordinere sikkerhetsstyringen mellom de statlige tjenesteleverandørene i noen grad, men det vil fortsatt være til dels fragmentert og komplisert sikkerhetsorganisering, der sikkerhetsstyringen er fordelt på flere virksomheter med egne beslutningsprosesser. Konseptet vil kunne gi en middels positiv virkning på graden av nasjonal kontroll.

I K3 er et statlig driftskonsept der staten i stor grad styrer innsatsfaktorene direkte og står fri til å beslutte videre utvikling. Konseptet innebærer stor grad av statlig drift med minimale avhengigheter til tredjeparter. Konseptet legger opp til omfattende krav til plassering av datasentre, drifts- og støttefunksjoner og streng tilgangsstyring, der alle støttefunksjoner med lese- og skrivetilgang må befinne seg i Norge. Konseptet legger også opp til en grad av tekniske undersøkelser eller verifikasjon av IKT-produkter der avhengigheter ikke kan unngås. Konseptet legger til rette for enhetlig, samordnet sikkerhetsstyring med sikkerhetsmessige stordriftsfordeler, herunder utstrakt bruk av standardisering og automatisering. Dette konseptet gir svært stor positiv virkning på graden av nasjonal kontroll.

K4 bygger på et risikobasert leverandørvalg med lav risikoaksept, der staten legger opp til et koordinert tjenestekjøp gjennom én organisasjon. Denne organisasjonen kjøper tjenester på vegne av et stort antall virksomheter med samordnede krav til sikkerhet. I dette konseptet vil det fortsatt være avhengigheter til utvalgte leverandører. Konseptet er tilpasset utvidede krav til plassering av datasentre, drifts- og støttefunksjoner i Norge med streng tilgangsstyring. Konseptet åpner for å gi avgrensede lese- og skrivetilganger for enkelte nødvendige støttefunksjoner fra utlandet. Konseptet har potensial til å koordinere eller samordne sikkerhetsstyringen gjennom en samlet innkjøpsorganisasjon som kan følge opp hvordan krav ivaretas, og oppnå enkelte sikkerhetsmessige stordriftsfordeler. Konseptet vil kunne gi en middels positiv virkning.

K7 kombinerer det statlige driftskonseptet i K3 med tjenestekjøpet i K4, for å etablere to lukkede skytjenester. Den statlige driftede lukkede skytjenesten gir høy grad av nasjonal kontroll som i K3, mens den lukkede skytjenesten som fremskaffes gjennom et tjenestekjøp gir middels grad av nasjonal kontroll. Tjenestene håndteres av samme organisasjon, som legger til rette for enhetlig eller samordnet sikkerhetsstyring og oppfølging. Data fordeles mellom tjenestene ut fra kritikalitet, det vil si ut fra en verdi- og risikovurdering av systemene og dataene som skytjenestene skal håndtere. De mest kritiske dataene og systemene skal lagres og behandles i den statlige driftede lukkede skytjenesten. Andre beskyttelsesverdige data med lavere grad av kritikalitet kan behandles i en lukket skytjeneste levert av en kommersiell leverandør som imøtekommer krav til nasjonal lagring og behandling. Siden de mest kritiske dataene håndteres i den statlige lukkede skytjenesten, vil virkningen på nasjonal kontroll i K7 ligge nært opp til den positive virkningen i K3. Konseptet vurderes å kunne gi en stor positiv virkning. Konseptet rangeres likevel noe lavere enn K3 samlet sett, fordi noen beskyttelsesverdige data vil behandles i en skytjeneste levert av en kommersiell leverandør med noe lavere grad av nasjonal kontroll.

Virkninger av endret funksjonalitet og fleksibilitet

Med funksjonalitet mener vi egenskaper og tjenestetilbud. Dette er nærmere beskrevet i kapittel om mulighetsstudien. Konseptets egenskaper kan dekke en rekke forhold som ytelse, kapasitet, skalerbarhet, robusthet og utviklingsmulighet. Tjenestetilbudet omfatter

både omfanget av tjenester som tilbys, og hvilke tjenestenivåer (kvalitet og funksjon) som tilbys.

Med tydeliggjøring av dagens krav til nasjonal kontroll vil det medføre begrensninger på hvilke type leverandører og tjenester som kan benyttes, noe som kan bety visse begrensninger på funksjonalitet og fleksibilitet sett opp mot noen av de skytjenestene som benyttes i dag. Det kan blant annet medføre begrensninger på antall leverandører og deres mulighet til å utnytte stordriftsfordeler, noe som eksempelvis kan påvirke muligheten til å skalere ved behov. Videre kan det legges begrensninger på hvilke tjenester og leverandører som kan benyttes hvilket påvirker muligheten til å følge teknologikutviklingen. For virksomhetene kan behovet for (flere) parallelle løsninger også medføre enkelte ulemper utover det som påvirkes av funksjonalitet og fleksibilitet i selve skyen.

Vi deler inn i virkningene av endret funksjonalitet inn i tre kategorier:

1. **Endringer i tilbudet av SaaS:** Gjelder både antall, kvalitet og funksjoner på applikasjonene
2. **Endringer i tilbudet av PaaS:** Tilgjengelighet av verktøy, bibliotek, API-er og funksjon til plattformen
3. **Endringer i tilbudet av IaaS:** Skalerbarhet i infrastruktur

De berørte aktørene er de samme som er vurdert under delkapitlet om nasjonal kontroll. Samlet kan begrensninger på disse faktorene medføre:

- Økt tidsbruk og driftskostnader knyttet til utvikling og produksjon av tjenester til sluttbruker (ved bruk av skytjenestene)
- Redusert kvalitet på tjenestene som leveres til sluttbruker

For brukerne av tjenestene som de berørte virksomhetene produserer kan konsekvensene være at tjenestene blir vanskeligere å bruke eller at tjenestekvaliteten blir lavere. Dette kan resultere i:

- Økt tidsbruk ved bruk av tjenestene
- Lavere verdi ved bruk av tjenestene
- Redusert bruk av tjenestene og medfølgende tapte verdi

Virkningene vil treffe de ulike statlige virksomhetene på ulike måter avhengig av hva slags type skyløsning de benytter i nullalternativet. Dersom virksomhetene benytter en allmenn skyløsning vil konsekvensene for aktørene være annerledes enn dersom de benytter lukkede skytjenester eller ingen skyløsninger i det hele tatt. Som utgangspunkt for vurderingene har vi lagt til grunn samme antagelse som for prissatte virkninger, hvilket er at andelen som forblir på egne driftede plattformer er uendret fra nullalternativet i alle konsepter. Usikkerhet knyttet til dette er nærmere forklart i kapittel 7.3.2.

Tabellen under oppsummerer vurderingen av ikke-prissatte virkninger knyttet til endret funksjonalitet / fleksibilitet som følge av en nasjonal skytjeneste.

Tabell 7-6 Ikke-prissatte virkninger av endringer i funksjonalitet / fleksibilitet. Alle resultater er vurdert til forskjell fra referansebanen (nullalternativet). De ikke-prissatte virkningene vurderes på en seks-delt skala (svært liten, liten, middels, stor, svært stor)

	Virkning av endret funksjonalitet/fleksibilitet	Forventet samlet konsekvens	Rangering
Konsept 1	For de virksomhetene som går fra lukkede skytjenester i nullalternativet vil funksjonaliteten være <u>lavere</u> grunnet reduksjon i tilbudet av SaaS- og PaaS-tjenester. For IaaS-laget vil det være redusert skalerbarhet grunnet fragmentering av løsninger og begrensninger for leverandørene. For de virksomhetene som går fra allmenne skytjenester vil funksjonalitet være lavere enn i nullalternativet	Middels negativ virkning	(5)
Konsept 2	For de virksomhetene som går fra lukkede skytjenester i nullalternativet vil funksjonaliteten være omtrent <u>uendret</u>. De statlige aktørene kan levere et godt tilbud av SaaS og PaaS-tjenester. For IaaS-laget vil muligheten til å skalere være høy grunnet samordning av virksomheter. For de virksomhetene som går fra allmenne skytjenester vil funksjonalitet være lavere enn i nullalternativet.	Liten negativ virkning	(3)
Konsept 3	For de virksomhetene som går fra lukkede skytjenester i nullalternativet vil funksjonalitet være omtrent <u>uendret</u>. Det vil tilbys færre SaaS-tjenester, men tilbudet av PaaS vil være omtrent tilsvarende det som tilbys i markedet. I tillegg vil det tilbys betydelig kapasitet og skalerbarhet (IaaS). For de virksomhetene som går fra allmenne skytjenester vil funksjonalitet være lavere enn i nullalternativet.	Liten negativ virkning	(3)
Konsept 4	For de virksomhetene som går fra lukkede skytjenester i nullalternativet vil funksjonaliteten være <u>høyere</u> grunnet et større tjenestetilbud (SaaS og PaaS) og kapasitet og skalerbarhet (IaaS) som følge av høy grad av samordning. For de virksomhetene som går fra allmenne skytjenester vil funksjonalitet være lavere enn i nullalternativet.	Svært liten negativ virkning	(1)

	Virkning av endret funksjonalitet/fleksibilitet	Forventet samlet konsekvens	Rangering
Konsept 7	For de virksomhetene som går fra lukkede skytjenester i nullalternativet vil funksjonaliteten være <u>noe høyere</u> grunnet et større tjenestetilbud (SaaS og PaaS) og høy kapasitet og skalerbarhet (IaaS) som følge av høy grad av samordning. For de virksomhetene som går fra allmenne skytjenester vil funksjonalitet være lavere enn i nullalternativet.	Svært liten negativ virkning	(2)

Som vi ser av tabellen over spenner den samlede forventede konsekvensen av virkninger ved endret funksjonalitet / fleksibilitet i de fem konseptene fra middels negativ virkning til svært liten negativ virkning.

Det er størst negativ virkning i konsept 1. Der vil brukere oppleve en begrensning i tjenestetilbudet sett opp mot dagens situasjon. Per i dag vil ikke allmenne skytjenester imøtekomme kravene til nasjonal kontroll. Dette betyr at virksomhetene som går fra allmenne skytjenester i nullalternativet vil få lavere funksjonalitet i konsept 1. Videre vil tydeliggjøring av kravene til nasjonal kontroll kunne begrense antall potensielle leverandører, hvilke tjenester de kan tilby og leverandørens evne til å utnytte sine interne ressurser. Dette betyr at tilbudet av kommersielle/lukkede skytjenester begrenses, og betyr færre SaaS- og PaaS-tjenester. I tillegg vil ikke konseptet medføre noen nevneverdig samordning av tjenestekjøp hvilket ytterligere begrenser leverandørenes evne til å utnytte ressurser på tvers av kunder. Dette vil kunne redusere skalerbarheten og treffer IaaS-laget. Samlet innebærer det at funksjonaliteten vil oppleves som noe lavere enn i dagens lukkede skytjenester, og klart lavere enn dagens allmenne skytjenester. Over tid vil muligens flere tjenester kunne imøtekomme kravene hvilket vil redusere forskjellen i funksjonalitet sett opp mot nullalternativet utover analyseperioden.

I konsept 2 er det forventet en liten negativ virkning i funksjonalitet / fleksibilitet. Med styrt samordning av virksomhetene gjennom bruk av 5-10 statlige tjenesteleverandører, vil det være mer samordning av tjenestekjøp og -produksjon. De store statlige aktørene vil kunne levere et bredt spekter av tjenester på SaaS- og PaaS-laget, men muligheten for individuelle tilpasninger vil være noe mer begrenset enn i nullalternativet og konsept 1. De store statlige aktørene vil eksempelvis kunne levere gode verktøy, bibliotek og kode på PaaS-laget. I tillegg vil økt samordning øke leverandørenes mulighet til å skalere (IaaS-laget). Samlet vurderer vi at man kan forvente liknende funksjonalitet som dagens lukkede skytjenester. Det innebærer at de som går fra lukkede skytjenester fra kommersielle aktører i nullalternativet til de statlige tjenesteleverandørene i liten grad vil bli påvirket. Aktørene som går fra allmenne skytjenester, vil oppleve å få lavere funksjonalitet. Som for konsept 1 vil sannsynligvis flere tjenester kunne imøtekomme kravene over tid hvilket vil redusere forskjellen i funksjonalitet sett opp mot nullalternativet utover analyseperioden.

I konsept 3 er det forventet at funksjonaliteten vil være omtrent tilsvarende som for konsept 2. I dette konseptet vil det trolig være noe begrenset tjenestetilbud, spesielt for SaaS-laget

fordi det kan være enkelte leverandører som ikke kan eller ønsker å tilby sine SaaS-tjenester fra en statlig driftet plattform. Tilbudet av PaaS vil være tilsvarende det som tilbys i markedet med gode verktøy, bibliotek og kode. Konseptet legger imidlertid til grunn stor grad av samordning hvilket gir gode muligheter til å oppnå stordriftsfordeler i kapasitetsutnyttelsen og med det stor skalerbarhet (IaaS-laget). Samlet vurderer vi derfor at K3 vil kunne tilby en funksjonalitet / fleksibilitet som er liknende dagens lukkede skytjenester levert av kommersielle aktører. Aktørene som går fra allmenne skytjenester til nasjonale skytjenester, vil oppleve å få lavere funksjonalitet. Over tid vil det kunne være flere type tjenester som imøtekommer kravene til nasjonal kontroll og som kan kombineres med eller legges på den lukkede statlige sky. Det vil kunne redusere forskjellen i funksjonalitet sett opp mot nullalternativet utover analyseperioden, men i noe mindre grad enn i øvrige konsepter.

De negative virkningene er minst i konsept 4. Det vil være et større tilfang av SaaS-applikasjoner enn K3 fordi man kan trekke på store private leverandører. Videre vil det være noe bedre tilgang på verktøy, bibliotek og kode på PaaS-laget fra store private leverandører enn for K3. I tillegg vil man i dette konseptet dra nytte av økt samordning av innkjøp hvilket legger bedre til rette for at leverandørene kan utnytte stordriftsfordeler internt, noe som øker skalerbarheten (IaaS-laget). Samlet vurderer vi derfor at K4 vil gi en funksjonalitet / fleksibilitet som er høyere enn dagens lukkede skytjenester. Aktørene som går fra kommersielle/lukkede skytjenester i dag vil derfor kunne oppleve økt funksjonalitet, mens brukere av allmenne skytjenester fortsatt vil kunne oppleve noen begrensninger sett opp mot nullalternativet. Over tid vil muligens flere allmenne skytjenester også kunne imøtekomme kravene, hvilket vil redusere forskjellen i funksjonalitet utover i analyseperioden sett opp mot de som bruker allmenne skytjenester i nullalternativet.

I konsept 7 er det forventet en svært liten negativ virkning i funksjonalitet / fleksibilitet. Konseptet er en kombinasjon av konsept 3 og konsept 4, og vi har vurdert at 1/3 av datamengden inngår i statlig sky og 2/3 inngår i den kommersielle skyen drevet av private aktører. Dermed vil vurderingen av konsept 7 ligge nærmere konsept 4 enn konsept 3 for virkningene knyttet til funksjonalitet. Aktørene som går fra kommersielle / lukkede skytjenester i dag vil derfor kunne oppleve noe økt funksjonalitet, mens brukere av allmenne skytjenester fortsatt vil kunne oppleve noen begrensninger sett opp mot nullalternativet. Over tid vil muligens flere allmenne skytjenester også kunne imøtekomme kravene, hvilket vil redusere forskjellen i funksjonalitet utover i analyseperioden sett opp mot de som bruker allmenne skytjenester i nullalternativet. Samtidig vil det kunne være flere type tjenester som imøtekommer kravene til nasjonal kontroll og som kan kombineres med eller legges på den lukkede statlige skyen.

7.3 Vurdering av usikkerhet

Alternativanalysen i denne utredningen innehar stor usikkerhet. Utredningen favner bredt med opp mot 185 berørte statlige virksomheter med ulike data, systemer og infrastrukturer. Det har ikke vært mulig å innhente detaljert informasjon om alle relevante aspekter knyttet til alt fra kostnader til type beskyttelsesverdige data og systemer. Det gjør at analysene som er gjennomført er overordnede og preget av en rekke forutsetninger med større usikkerhet enn det som kan forventes i en KVVU med smalere fokus og omfang.

En av de største usikkerhetene i alternativanalysen er knyttet til mengden beskyttelsesverdige data og systemer i dag og i fremtiden. Videre er det også stor usikkerhet

knyttet til markedsutviklingen fremover, og usikkerhet knyttet til gjennomføring og organisering. Hvilke konkrete krav til kontroll som vil stilles, til hvilke kategorier av data og systemer og hvem disse kravene vil gjelde for er det også knyttet usikkerhet til. Disse usikkerhetene vil ha stor påvirkning på både de prissatte og ikke-prissatte virkningene.

I delkapitlene under går vi først gjennom usikkerhet knyttet til de prissatte virkningene, deretter usikkerheten knyttet til de ikke-prissatte virkningene og avslutningsvis presenterer vi noen utvalgte følsomhetsanalyser.

7.3.1 Usikkerhet knyttet til prissatte virkninger

I vurderingen av usikkerheten i de prissatte virkningene skiller vi mellom estimatusikkerhet og usikkerhetsfaktorer. Estimatusikkerhet er knyttet til usikkerhet i mengder og priser i underlaget. Usikkerhet og vurderinger knyttet til estimatusikkerhet er beskrevet i vedlegg H Usikkerhetsanalyse. Usikkerhetsfaktorer modellerer den kostnadmessige konsekvensen av alle forhold som ikke inkluderes i grunnkalkylen og estimatusikkerheten, men som likevel antas å kunne påvirke de endelige prosjektkostnadene. I tabellen under presenteres en oversikt over usikkerhetsfaktorene som er brukt i analysen.

Tabell 7-7 Oversikt over usikkerhetsfaktorer med beskrivelse

Usikkerhetsfaktor	Beskrivelse
U1 – Eierstyring og offentlige prosesser	Faktoren uttrykker usikkerhet knyttet til eiers evne til å ta riktige beslutninger til riktig tid for både gjennomføringen av prosjektet og nødvendig regelverksarbeid. Faktoren ivaretar eiers evne og vilje til å gi prosjektet riktige rammebetingelser for en god gjennomføring. Faktoren omhandler også eiers evne til å drive og forankre arbeid knyttet til tydeliggjøring eller eventuell endring av regelverk/forskrift for «sikker sky».
U2 – Løsning og prosjektmodenhet	Faktoren uttrykker usikkerhet knyttet til mulighet for å realisere konseptet, kompleksiteten, sikkerhetsaspekter, integrasjoner, applikasjoner, valg av teknologi og organisatoriske løsninger for det definerte omfanget. Faktoren ivaretar også prosjektunderlagets detaljeringsnivå og modenhet.
U3 – Marked og leverandører	Faktoren uttrykker usikkerhet knyttet til generelle markedsbetraktninger, kjennskap til det relevante markedet nasjonalt og lokalt, samt forventninger om utviklingen de neste årene. Faktoren retter seg f.eks. til tilgjengelig relevant kompetanse innen skyteknologi (migrering), leverandører av skytjenester, og IT-sikkerhet.
U4 – Prosjektstyring og gjennomføringsevne	Faktoren uttrykker usikkerhet knyttet til prosjektledelsens evne til å styre prosjektet og integrasjon mellom prosjekt og organisasjon. Denne faktoren omhandler kapasitet, kompetanse og kontinuitet i prosjektorganisasjonen. Faktoren retter seg mot den daglige og operative styringen «innad» i prosjektet og i transisjonen mellom den midlertidige prosjektorganisasjonen og den varige organiseringen av den nasjonale skyløsningen.
U5 – Driftsorganisasjon	Faktoren uttrykker usikkerhet knyttet til varige oppfølgingen av nasjonal skyløsning på en effektiv og sikker måte og sikre

Usikkerhetsfaktor	Beskrivelse
	tilstrekkelig kapasitet, kompetanse og kontinuitet i driftsorganisasjonen.
U6 – Mengde beskyttelsesverdige data	Faktoren uttrykker usikkerhet knyttet til total mengde beskyttelsesverdige data og systemer som er kartlagt hos de statlige virksomhetene. Kartleggingen inneholder både svar på mengde data fra spørreundersøkelsen og oppskaleringen av data for å dekke alle de 185 statlige virksomhetene.
U7 – Aktører og interessenter	Faktoren uttrykker usikkerhet knyttet til brukere, mottakere og interessenters direkte eller indirekte mulighet til å påvirke omfang, fremdrift, krav og løsningsvalg, og hvordan prosjektet påvirkes «fra siden» av omgivelsene, eks. retningsvalg som påvirker krav til anskaffelsen og krav til løsninger.

Usikkerhetsanalysen viser at det er stor usikkerhet knyttet til estimatene for konseptene, samt omkringliggende faktorer som kan påvirke kostnaden for konseptene. Det er særlig tre faktorer som dominerer usikkerhetsbildet i alle konseptene:

Usikkerhetsfaktoren *Mengde beskyttelsesverdig data* vil trolig ha størst innvirkning på kostnadene for alle konseptene da den omfatter de mest sentrale premissene for konseptene. Det er lagt til grunn den estimerte mengde beskyttelsesverdige data som virksomhetene vurderer som nødvendig i krise og væpnet konflikt ifølge utredningens spørreundersøkelse. Det er derimot usikkerhet knyttet til forståelsen av begrepet «beskyttelsesverdig informasjon» og hvordan spørsmålet i spørreundersøkelsen er tolket. Videre kan vurderingen av hva som er beskyttelsesverdige data og systemer, og hvilke krav som stilles til dem, endres over tid. Det er i tillegg stor usikkerhet knyttet til veksten i beskyttelsesverdige data. Alle konseptene har lik vurdering av usikkerheten med en betydelig spredning rundt mest sannsynlig verdi. I tillegg til å være den viktigste usikkerhetsfaktoren for estimeringen av de prissatte virkningene vil usikkerheten rundt hvilke og hvor mye data som vil inngå i den nasjonale skyen også ha stor innvirkning på de ikke prissatte virkningene.

Kravene som tydeliggjøres som en del av K1, og som er lagt til grunn i alle konseptene vil, avhengig av hvordan de utformes, også kunne påvirke virksomheter utenfor statsforvaltningen, dersom de forvalter data og systemer som er beskyttelsesverdige. Hvorvidt kravene også vil gjelde for andre virksomheter må vurderes i det videre arbeidet. I tråd med avgrensningene i mandatet har vi i alternativanalysen lagt til grunn at det er de beskyttelsesverdige dataene og systemene i statsforvaltningen som primært omfattes av kravene som stilles. Dette innebærer imidlertid at det er en usikkerhet knyttet til om kravene som stilles også kan utløse kostnads- og nyttevirkinger for flere enn det som er hensyntatt i denne analysen. Dette gjelder alle konsepter i og med at de grunnleggende «kravene» er like. De virkningene som eventuelt oppstår vil være tilsvarende som for statsforvaltningen, både for prissatte- og ikke prissatte virkninger, og dermed kun påvirke omfanget av virkningene og ikke de relative forskjellene mellom dem.

Usikkerhetsfaktoren *Marked og leverandører* uttrykker usikkerhet knyttet til generelle markedsbetraktninger, kjennskap til det relevante markedet nasjonalt og lokalt, samt

forventninger om utviklingen de neste årene. Usikkerheten er vurdert symmetrisk for alle konseptene, men med et større usikkerhetsspenn for konsept 2, 3 og 7. Dette skyldes at det i disse konseptene er høyere bruk av leverandører av utstyr, større usikkerhet knyttet til tilgjengelighet på varer og konseptet er således mer følsomt for valutasvingninger.

Usikkerhetsfaktoren *Eierstyring og offentlige prosesser* er vurdert forholdsvis likt for konseptene både når det gjelder investeringskostnader og varige kostnader. Det er utredningens vurdering at ved god eierstyring kan kostnadene både bli lavere og høyere. Konseptene omfatter hele statsforvaltningen og vil kreve god eierstyring på tvers av virksomhetene. Konsept 2 er derimot betydelig mer høyreskjev enn øvrige konsepter som følge av at potensielle statlige tjenesteleverandører samlet er underlagt flere departementer. Det innebærer at det er flere eierdepartementer som skal samarbeide og skape gode rammer for gjennomføringen, og utredningens vurdering er at dette vil kreve flere prosesser og mer jobb enn i de andre konseptene.

I tabellen under presenteres forventningsverdi og standardavvik per konsept. Standardavviket sier noe om spredningen av verdier og verdienes gjennomsnittlige avstand fra gjennomsnittet. Det relative standardavviket angir forholdet mellom standardavviket og gjennomsnittsverdien.



Konsept 2 er det konseptet med høyest standardavvik, etterfulgt av konsept 3 og 7. Konsept 2 er vurdert å være mest usikkert når det kommer til usikkerhetsfaktoren *Eierstyring og regulatoriske forhold*. Konsept 2 har også høyest vurdering av usikkerhet når det gjelder *Marked og leverandører*, *Løsning og prosjektmodenhet* og *Prosjektstyring og gjennomføringsevne*. Dette skyldes at konsept 2 er et konsept som krever at flere statlige tjenesteleverandører under ulike eierdepartement, sammen skal sikre en løsning som leverer like gode tjenester på tvers av sektorer og der løsningene er tilstrekkelig integrert.

Konsept 3 er det konseptet som er mest avhengig av utstyrsleveranser fra leverandører, og at disse blir levert når de trengs. Konseptet er sterkt påvirket av markedet. Videre vil og konseptet ha en stor prosjektorganisasjon som skal sikre en ny organisasjon som kan drifte den nasjonale skyen. Konsept 3 er også mer usikkert enn andre konsepter når det kommer til integrasjoner/applikasjoner, samt at lukket statlig sky kan bli utpekt som skjermingsverdig/GNF, som igjen vil påvirke fremdriften.

Konsept 7 har også relativt høyt standardavvik og følger mye av usikkerhetsvurderingene i konsept 3, men blir også påvirket i usikkerhetsvurderingene som følge av K4-delen i konseptet. Konseptet har høy usikkerhet når det gjelder *Løsning og prosjektmodenhet*, *Marked og leverandører* og *Prosjektstyring og gjennomføringsevne*.

Nullalternativet, konsept 1 og 4 har også høye standardavvik, men er vurdert å ha noe lavere usikkerhet enn de andre.

I tabellen under presenteres prosjektets mulighet til å styre usikkerheten.

Tabell 7-9 Oversikt over usikkerhetsfaktorer og prosjektets mulighet til å styre usikkerheten

Usikkerhet	Prosjektets mulighet til å styre usikkerheten
U1 – Eierstyring og regulatoriske forhold	Usikkerhet i eierstyring og regulatoriske forhold regnes som delvis styrbar. Tiltak kan forsterke muligheter og redusere trusler.
U2 – Løsning og prosjektmodenhet	Faktoren gjenspeiler usikkerhet som følge av prosjektering tilsvarende KVVU-modenhet i underlag for estimering. Det tilhører dermed historien og lar seg ikke styre direkte. Det er likevel mulig å iverksette tiltak i ettertid for å øke sannsynligheten for kostnadsreduksjoner i løsningsdesign, og sikre at det ikke velges løsninger som er veldig kostnadsdrivende. Slike tiltak bør vurderes i forprosjektet og tilhører usikkerheten som prosjektorganisasjon bør håndtere.
U3 – Marked og leverandører	Det er ikke mulig å styre markedet i den ene eller andre retningen, men usikkerheten kan reduseres ved konkrete tiltak mot markedet og leverandører. Usikkerheten er derfor delvis styrbar.
U4 – Prosjektstyring og gjennomføringsevne	Prosjektorganisasjon som usikkerhet er generelt betraktet som i stor grad styrbar. Utredningens vurdering er at det også er tilfelle i dette prosjektet. Usikkerhetsreducerende tiltak vil i denne fasen ivaretas i eierstyringen.
U5 – Driftsorganisasjon	Tilstrekkelig kompetanse, kontinuitet og tilgjengelighet på personell er ofte en usikkerhet i en driftsorganisasjon. I dette tilfellet vil det også være relevant med kompetanse man ofte henter utenlands. Usikkerheten er delvis styrbar, da man ved hjelp av tiltak kan tiltrekke seg og sikre kompetent personell.
U6 – Mengde beskyttelsesverdige data	Mengde beskyttelsesverdige data følger delvis av hvor mange av de statlige virksomhetene som velger å bruke sky-løsningen. Denne delen av usikkerheten er styrbar fra eiers perspektiv. Usikkerheten som ligger i beregningen av mengde beskyttelsesverdige data og utviklingen over tid er i liten grad styrbar.
U7 – Aktører og interessenter	Faktoren er delvis styrbar – prosjektet kan til en viss grad styre hvorvidt eksterne interesser skal påvirke omfang og kostnader.

7.3.2 Usikkerhet knyttet til ikke-prissatte virkninger

Det er gjennomført en overordnet usikkerhetsvurdering knyttet til realisering av konseptene. Vurderingene av de største usikkerhetene knyttet til de ikke-prissatte virkningene, utover det som følger av mengden beskyttelsesverdige data, er vist i tabellen nedenfor og er nærmere forklart i avsnittene nedenfor.

Tabell 7-10 – Intern rangering av risiko og muligheter knyttet til ikke-prissatte virkninger

	Konsept 1	Konsept 2	Konsept 3	Konsept 4	Konsept 7
Risiko og muligheter med rangering					
Risiko knyttet til etterlevelse av krav	5	4	1	3	2
Gjennomføringsrisiko knyttet til organisering	1	5	2	2	2
Mulighet knyttet til større overgang til sky	3	3	3	1	2

Risiko knyttet til etterlevelse av krav

I alle konseptene legger vi til grunn at aktørene etterlever krav til nasjonal kontroll. I denne vurderingen er det to viktige risikomomenter. Den første knytter seg til i hvilken grad (og hvor mange) tjenesteleverandører som er i stand til å etterleve kravene til nasjonal kontroll. Den andre knytter seg til i hvilken grad de statlige virksomhetene er i stand til å velge egnede leverandører. Denne risikoen er mest gjeldende i konsept 1 der hver aktør i statsforvaltningen må gjennomføre sine egne anskaffelser av skytjenester. Her treffer begge risikoaspektene inn, og det øker risikoen for at man ikke etterlever kravene som stilles.

I konsept 2 er det flere leverandører som skal koordineres og det øker dermed risikoen for at noen ledd i verdikjeden ikke etterlever kravene som er stilt. Samtidig vil risikoen knyttet til at de statlige leverandørene velger egnede leverandører for de tjenestene de ikke leverer selv reduseres, da dette blir gjort gjennom 5-10 statlige tjenesteleverandører med store og profesjonelle kompetansemiljøer.

I konsept 3 er risikoen for manglende etterlevelse vesentlig redusert ved at det er en sentral enhet som har ansvar for å levere løsningen i fullt statlig egenregi. I konsept 4 er ansvaret sentralisert, og man reduserer risikoen knyttet til at de statlige leverandørene selv må velge egnede leverandører i likhet med konsept 2. I tillegg er det færre kommersielle leverandører man skal følge opp og vurdere etterlevelsen av kravene for. I konsept 7 er også ansvaret sentralisert og noe leveres i egenregi og noe løses ved hjelp av egnede leverandører. Dette reduserer risikoen mer enn i konsept 4, men mindre enn i konsept 3.

Gjennomføringsrisiko knyttet til organisering

Det er lagt opp til ulike typer organisering i hvert konsept, og dette kan medføre ulik grad av risiko knyttet til realiseringen av konseptene og til drift og kontinuerlig utvikling. I konseptene er det flere statlige virksomheter, kommersielle leverandører og eierdepartementer som skal være involvert.

Valg av konsept 2 vil innebære at 5-10 statlige aktører skal levere tjenester til resten av statsforvaltningen. Konseptet legger opp til at disse statlige tjenesteleverandørene må gjøre organisatoriske og tekniske forberedelser slik at de kan levere tjenester til andre statlige virksomheter som møter deres behov over tid. Det vil være ulik grad av modenhet blant de statlige tjenesteleverandørene og deres evne til å sikre en god gjennomføring vil være varierende. Noen virksomheter leverer allerede tjenester til andre statlige aktører i dag og er allerede godt rigget til å utvide dette arbeidet. Andre aktører er mindre modne, og det vil kreve større endringer i organisasjonen for at dette skal fungere. I tillegg vil det potensielt være flere eierdepartement involvert, noe som kan bety komplekse tverrsektorielle prosesser. Dette medfører at det vil være høyest gjennomføringsrisiko knyttet til organisering i konsept 2. Denne usikkerheten er reflektert i usikkerhetsanalysen for de prissatte virkningene, men vil også påvirke de ikke-prissatte virkningene av nasjonal kontroll og endringer i funksjonalitet og fleksibilitet.

I konsept 1 fortsetter virksomhetene stort sett som i dag og det er ikke stor gjennomføringsrisiko knyttet til organiseringen. I konsept 3, 4 og 7 er organisasjonen som skal drive arbeidet sentralisert og enheten vil bygges opp fra bunnen av. Det forenkler arbeidet sett opp mot konsept 2, men innehar likevel mer gjennomføringsrisiko enn i konsept 1.

Mulighet knyttet til større overgang til sky

I analysene som er gjennomført er det lagt til grunn at konseptene ikke vil påvirke andelen beskyttelsesverdige data og systemer som flyttes ut i sky.

Utskiftning og/eller omlegging av eldre systemer med beskyttelsesverdige data til skyløsninger vil innebære en betydelig investering. Dette alene sannsynliggjør at det vil ta lang tid å foreta denne endringen. Prosesser med å skifte ut gamle applikasjoner tar normalt lenger tid enn planlagt. Det er både knyttet til lange tidsløp for å få tildelt nødvendige investeringsmidler, og at enkelte slike løsninger erstattes delvis, over lengre tid og gjennom flere smidige, små prosjekter.

Når nye løsninger bygges rundt de gamle, og med et moderne grensesnitt, innebærer det at de etablerte løsningene sementeres og får en lengre levetid enn forutsett. En relativt stor andel av eldre systemer er ofte dårlig tilrettelagt for å utnytte mulighetene som skyen kan tilby (skalering, sikkerhet, autentisering, osv.). De gamle løsningene vil i et slikt scenario fortsatt driftes lokalt, mens nye løsninger er skybaserte ("cloud native") og vil ofte ha datautveksling med de gamle løsningene. Det vil si at nyutvikling og innovasjon ikke nødvendigvis hemmes av de gamle løsningene, som også kan optimaliseres. Dette indikerer at det i lang tid vil være en andel IKT-systemer med beskyttelsesverdige data som ikke vil ligge i skyen.

I prinsippet kan gamle løsninger plasseres på en skyplattform selv om de i utgangspunktet ikke er tilpasset dette («lift and shift»), men det vil ofte kunne innebære en sikkerhetsrisiko og være en fordyrende løsning. Vi har ikke grunnlag for å estimere hvor stor andel som vil følge en slik strategi.

Tydeligere regulering og bedre tilrettelegging for valg av løsninger som sikrer at alle regler og krav er ivarettatt kan imidlertid føre til at flere finner det hensiktsmessig å flytte en større del av sine beskyttelsesverdige data og systemer ut i sky, med de fordelene det medfører. I

vurderingene av muligheten for at konseptene kan føre til større overgang til sky er det to mekanismer som trekker i ulike retninger.

Den første mekanismen handler om at det i noen av konseptene vil være enklere å identifisere og benytte skytjenester som imøtekommer særskilte krav til nasjonal kontroll over data og systemer. Usikkerhet knyttet til overholdelse av lover og regler ved bruk av skyløsninger er blant annet trukket fram som et vesentlig hinder i interessentanalysen. Vi har lagt til grunn at samme andel av virksomhetene, velger å la beskyttelsesverdige data og systemer være på egendriftet plattform. Når man tydeliggjør regelverket for beskyttelsesverdige data og systemer kan dette medføre at flere forstår hva som er lov og velger å løfte over beskyttelsesverdige data i sky. Det ville utløse økt funksjonalitet og potensielle kostnadsreduksjoner for de som i utgangspunktet ville blitt værende på egendriftet plattform.

Den andre mekanismen handler om at tjenesteprisen vil, som de prissatte virkningene viser, være høyere med strengere krav til nasjonal kontroll. Det kan føre til at færre virksomheter velger å gå ut i sky med sine beskyttelsesverdige data.

Disse to mekanismene trekker i ulike retninger og utredningen har per i dag ikke grunnlag til å kunne vurdere hvorvidt og i hvilket omfang de ulike konseptene påvirker hvor mange virksomheter som vil ta i bruk skyløsninger for sine beskyttelsesverdige data og i hvilket omfang. Det er likevel noen forskjeller mellom konseptene som er relevante.

Valg av K1 kan medføre en større overgang til sky, men den er noe mer begrenset enn i de andre konseptene. I K1 er kravene tydeliggjort, og det vil være tilgang på en rådgivningstjeneste som kan bistå virksomhetene. Dette vil redusere transaksjonskostnadene. På den andre siden øker tjenesteprisen betraktelig, hvilket kan medføre begrensninger på hvem som kan/vil gå ut i sky.

Ved valg av K2 vil det også være en mulighet for at flere velger overgang til sky, men noe begrenset. Når ansvaret for anskaffelsen av skytjenester med nasjonal kontroll er delvis sentralisert, reduseres transaksjonskostnadene. Samtidig, økt tjenestepris og mulige forviklinger med flere parallelle tilbydere vil kunne virke i motsatt retning. I K3, K4 og K7 legges det til rette for en enklere overgang til skyen. Forskjellene ligger i tjenesteprisen som er vesentlig lavere i K4 og delvis i K7, hvilket vil gjøre at oppsiden er størst for disse konseptene.

7.3.3 Følsomhetsanalyser

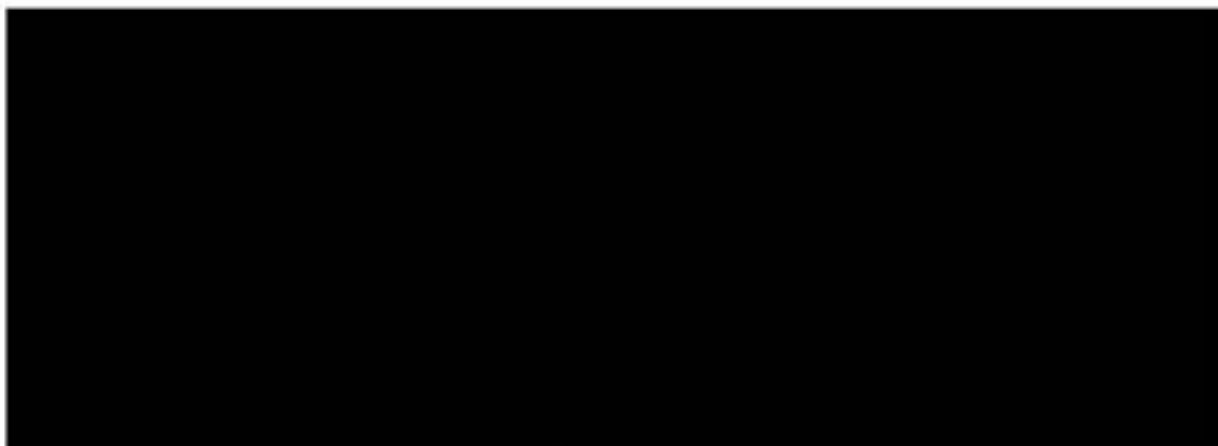
Gitt den store usikkerheten i alternativanalysen har vi valgt å gjennomføre noen utvalgte følsomhetsanalyser for å teste robustheten av rangeringene. Det er, som nevnt over, lagt til grunn flere forutsetninger for beregningene av konseptene som kan påvirke de prissatte virkningene. For å vurdere robustheten i konklusjonene har vi gjennomført ulike følsomhetsanalyser for å illustrere i hvilken grad endringer i ulike basisforutsetninger påvirker netto nåverdi til konseptene og rangeringen mellom dem. Analysene utdypes ytterligere i kapittel 6 i vedlegg H Usikkerhetsanalyse. De mest relevante følsomhetsanalysene er gjengitt i avsnittene under og inkluderer:

- Datamengde i nasjonal sky
- Splitt av datamengde i K7

- Tjenestepreis

Datamengde i nasjonal sky

Datamengde i den nasjonale skyen utgjør en betydelig usikkerhet i analysen og påvirker kostnaden for konseptene i stor grad. Det er derfor gjennomført analyser med både en halvering og en doubling av datamengden som inngår i konseptene.



Analysen viser at selv om kostnadene varierer stort med datamengden er det også en del «faste kostnader» som vil påløpe uavhengig av omfanget på løsningene. Dette indikerer at når man først har etablert en skytjeneste så vil eventuelle utvidelser ha en nokså lav marginalkostnad.

I konsept 3 (og deler av konsept 7) er det imidlertid behov for å gjøre initielle investeringer i datasentre som må ta høyde for framtidig vekst. For disse konseptene er det derfor viktig å ha bedre kontroll på forventet omfang enn for øvrige konsepter som i større grad er basert på tjenestekjøp som enklere kan skaleres fortløpende.

Splitt av datamengde i K7

For kombinasjonskonseptet (K7) er det lagt til grunn en fordeling av data som krever middels nasjonal kontroll (1/3 av datamengden) og høy grad av nasjonal kontroll (2/3 av datamengden). Det er gjennomført analyser for å se på hvordan ulik splitt mellom data som krever middels og høy nasjonal kontroll påvirker kostnadene for konseptet.

Følsomhetsanalysene viser også tall oppgitt uten kostnadspost 5 – Varige kostnader, da denne kostnadsposten utgjør en stor andel av de totale kostnadene, samtidig som den ikke påvirkes av fordeling av data mellom K3 og K4-delen i K7.

Tabell 7-12 Resultater av følsomhetsanalyse, endring i fordeling mellom K3-del og K4-del i K7. Resultater oppgitt i prosentvis endring av forventningsverdier av K7.

Konsept 7	Prosentvis endring	Prosentvis endring
% endring, lik fordeling i K3-del og K4-del	4 %	11 %
% endring, 10 % prosent i K3-del og 90 % i K4-del	-6 %	-16 %

Analysen viser at kostnadene ved kombinasjonskonseptet øker desto større andel av data som lagres i K3-delen av konseptet. Dette skyldes i hovedsak to momenter:

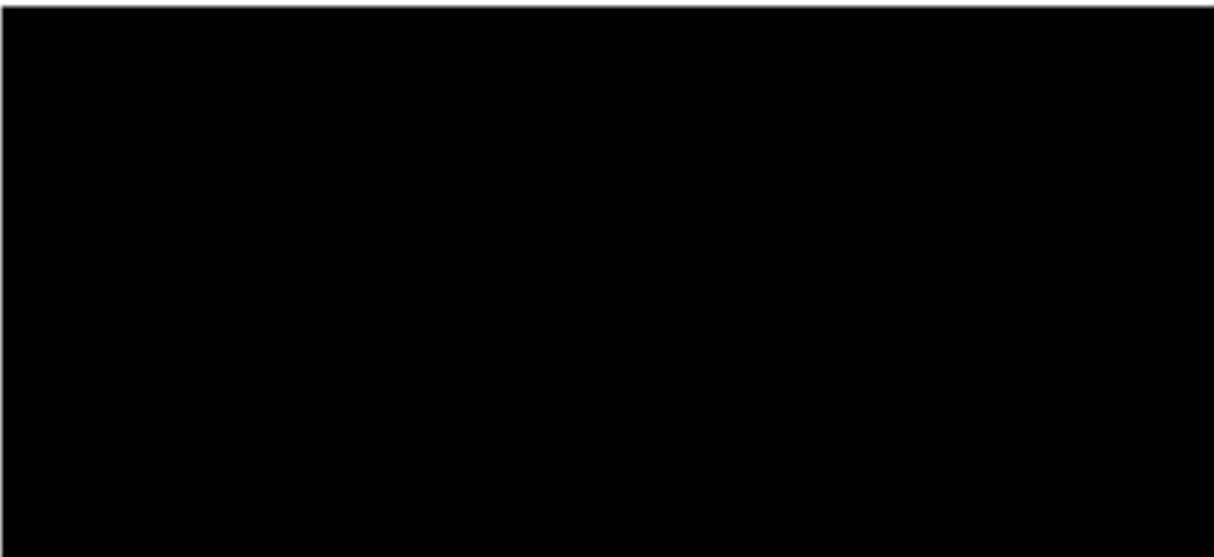
- Økt innkjøp av hardware og større arealer for datasenter. Datasenteret er ikke en fleksibel kostnad som kan tilpasses økende datamengde. Datasenterkostnaden tar høyde for den totale datamengden ved analyseslutt. Dette gir en betydelig up-front investering.
- Ved betydelige reduksjoner av datamengde i K4-delen vil også deler av stordriftsfordelene som følger av de kommersielle leverandørene reduseres. Dette medfører at enhetskostnadene øker.

Dette indikerer at konsekvensen ved å flytte data fra K4-delen (lukket kommersiell sky) til K3-delen (lukket statlig sky) vil kunne gi en dobbel effekt på kostnadene.

Følsomhetsanalysen viser at en høy andel data og systemer som krever høy nasjonal kontroll er kostnadsdrivende. Det vil være essensielt for konseptet å kartlegge hvilke data som krever en høy grad av nasjonal kontroll, for å sikre at kostnadene er tilpasset behovet.

Tjenestepreis

Omfanget av tjenestekjøp versus egenproduksjon utgjør en sentral forskjell mellom flere av konseptene. For de konseptene som baserer seg på tjenestekjøp er mye av kostnadsanslagene beregnet på bakgrunn av anslåtte tjenestepreiser det er knyttet stor usikkerhet til. Vi har derfor gjennomført en følsomhetsanalyse som ser på hvor mye tjenestepreisene må øke, relativt til det som er lagt til grunn, for å at forventningsverdien av totale kostnadene blir tilsvarende som konsept 3.



Følsomhetsanalysen viser at selv ved en stor kostnadsøkning i tjenestepreis, er det fremdeles stor prosentvis økning som kreves for å endre på rangeringen av konseptene. Den viser også at kombinasjonskonseptet er det konseptet hvor det kreves størst prosentvis økning for å komme opp på kostnadsnivået til K3.

7.4 Fordelingsvirkninger

Selv om konseptet viser seg å være lønnsomt for samfunnet totalt sett, kan konseptet medføre at ulike grupper påvirkes på ulike måter i negativ og positiv forstand. Når ulike

grupper i samfunnet påvirkes ulikt av et konsept vil det oppstå fordelingsvirkninger. Dersom noen grupper får store kostnadsvirkninger og andre får store nyttevirksomheter bør det beskrives godt hvordan virkningen er fordelt. I henhold til rundskriv R-109/21 skal det gis tilleggsinformasjon om fordelingsvirkninger av konseptet der det er relevant.

For de ulike konseptene vi vurderer vil det ikke være noen vesentlige fordelingsvirkninger mellom ulike grupper av befolkningen, utover at kostnadsøkninger sannsynligvis vil finansieres med skatt eller reduserte offentlige utgifter på andre områder. Det vil imidlertid kunne være noen forskyvninger mellom ulike offentlige virksomheter avhengig av hvilken finansieringsløsning som velges. De største forskjellene i fordelingsvirkninger på et overordnet nivå vil være forskyvningen mellom offentlige og kommersielle leverandører i K3 og til en viss grad K2 der staten helt eller delvis leverer tjenestene i egenregi, framfor bruk av kommersielle tjenesteleverandører.

Økningen i tjenestepreis i de ulike konseptene vil ikke medføre noen fordelingsvirkninger fordi vi legger til grunn at prisøkningen reflekteres av at leverandørene får økte kostnader.

7.5 Samlet vurdering og anbefaling

Rangeringen av konseptene etter samfunnsøkonomisk lønnsomhet skal inkludere både prissatte og ikke-prissatte virkninger. Analysen viser at kostnadene som følger av nasjonal kontroll er betydelige. Samtidig kan manglende nasjonal kontroll medføre store konsekvenser, særlig i en krise eller krigssituasjon, men disse er svært vanskelig å anslå. Virkningene av endret funksjonalitet kan også være vesentlige. Det gjør det svært krevende å vurdere den samlede samfunnsøkonomiske lønnsomheten av de ulike konseptene

7.5.1 Samlet vurdering

Resultatene som kommer frem i tabellen under oppsummerer de prissatte og de ikke-prissatte virkningene for de fem konseptene (intern rangering for hver virkning er oppgitt i parentes).

Tabell 7-14 - Oppsummering av prissatte og ikke-prissatte virkninger relativt til nullalternativet med rangering i parentes. De ikke-prissatte virkningene vurderes på en seks-delt skala (svært liten, liten, middels, stor, svært stor)

Virkning	Konsept 1	Konsept 2	Konsept 3	Konsept 4	Konsept 7
Prissatte virkninger, MNOK i 2022-kroner, ekskl. mva.					
Ikke-prissatte virkninger					

Virkning	Konsept 1	Konsept 2	Konsept 3	Konsept 4	Konsept 7
Virkninger av økt nasjonal kontroll	Liten positiv virkning (5)	Middels positiv virkning (3)	Svært stor positiv virkning (1)	Middels positiv virkning (3)	Stor positiv virkning (2)
Virkninger av endret funksjonalitet / fleksibilitet	Middels negativ virkning (5)	Liten negativ virkning (3)	Liten negativ virkning (3)	Svært liten negativ virkning (1)	Svært liten negativ virkning (2)
Usikkerhet knyttet til ikke-prissatte virkninger					
Risiko knyttet til etterlevelse av krav	(5)	(4)	(1)	(3)	(2)
Gjennomføringsrisiko knyttet til organisering	(1)	(5)	(2)	(2)	(2)
Mulighet knyttet til større overgang til sky	(3)	(3)	(3)	(1)	(2)
Samlet rangering etter de prissatte og ikke-prissatte virkningene	(4)	(5)	(2)	(2)	(1)

Basert på prissatte virkninger alene er det konsept 4 som medfører de laveste samfunnskostnadene utover nullalternativet. Årsaken er at konseptet legger til grunn samordnede anskaffelse av løsninger fra kommersielle leverandører hvilket legger til rette for at både leverandører og kundene av den nasjonale skyen kan oppnå vesentlige stordriftsfordeler. Konsept 1 er det nest billigste alternativet, men medfører likevel økte tjenestepriser og begrenset utnyttelse av stordriftsfordeler. Konsept 2 drar nytte av en del stordriftsfordeler, men ikke i like stor grad som K3 og K4. Samtidig krever også konseptet en større grad av samordning mellom de statlige tjenestetilbyderne. I tillegg er usikkerheten stor og høyreskjev, hvilket øker den forventede kostnaden. Konsept 3 er det nest dyreste alternativet drevet av vesentlige investeringer i hardware og etablering av datasentre. Konsept 7 er noe dyrere enn K4 og K1. Konseptet drar nytte av stor grad av samordning og oppnår stordriftsfordeler som reduserer kostnadene, men det må samtidig gjøres vesentlige investeringer i hardware og etablering av datasentre som trekker opp kostnadene.

For de ikke-prissatte virkningene av nasjonal kontroll er det størst positiv virkning i konsept 3. I dette konseptet er det staten som har kontroll over hele verdikjeden med minimale

avhengigheter til tredjeparter. Det fører til redusert risiko for tap av de beskyttelsesverdige dataene og systemenes tilgjengelighet og integritet. Det medfører lavere risiko for vesentlige kostnader som følge av forringelse eller bortfall av sentrale tjenester i fred, krise og væpnet konflikt. K7 kombinerer det statlige driftskonseptet i K3 med tjenestekjøpet i K4, for å etablere to lukkede skytjenester. Den statlige driftede skytjenesten gir høy grad av nasjonal kontroll som i K3, mens den lukkede skytjenesten som fremskaffes gjennom et tjenestekjøp gir middels grad av nasjonal kontroll. Siden de mest kritiske dataene håndteres i den statlige lukkede skytjenesten, vil virkningen på nasjonal kontroll i K7 ligge nært opp til den positive virkningen i K3. Konseptet rangeres likevel noe lavere enn K3 samlet sett, fordi noen beskyttelsesverdige data vil behandles i en skytjeneste levert av en kommersiell leverandør med noe lavere grad av nasjonal kontroll. Konsept 2 og 4 gir også positiv virkning på nasjonal kontroll, med hver sine fordeler og ulemper som gjør det vanskelig å skille den samlede virkningen. Utover nullalternativet er det K1 som gir lavest nytte med hensyn til nasjonal kontroll, med mange ulike løsninger anskaffet av hver enkelt virksomhet.

For virkningene knyttet til endret funksjonalitet og fleksibilitet er det konsept 4 som er nærmest nullalternativet. Stor samordning av innkjøp legger til rette for løsninger med stor skalerbarhet og et bredt tjenestetilbud. Konsept 2 og konsept 3 vil gi noe lavere funksjonalitet og fleksibilitet, men kommer bedre ut enn i konsept 1 som følge av større samordning av ressurser. K7 er den løsningen som kommer nest best ut med hensyn til endret funksjonalitet og fleksibilitet. Ettersom det er lagt til grunn at 2/3 av de beskyttelsesverdige dataene og systemene ligger i den delen av løsningen som tilsvarer K4 vil virkningene være nærmere vurderingene for K4 enn K3.

Tar vi i betraktning risiko knyttet til etterlevelse av krav er det mest krevende å sikre høy etterlevelse i konsept 1 der alle de 185 statlige virksomhetene selv må sørge for at kravene som stilles er overholdt. Det er lavest risiko i konsept 3 der staten selv tar ansvar for å drifte skyen og alle virksomhetene tar en del av denne løsningen. Større grad av samordning med en egen virksomhet rettet inn mot å anskaffe og følge opp et fåtall leverandører gir lavere risiko for manglende etterlevelse i konsept 4 enn i konsept 2. K7 vil ha en risiko tilsvarende et nivå mellom K3 og K4.

Gjennomføringsrisikoen knyttet til organisering er høyest i konsept 2 der 5-10 statlige virksomheter skal realisere konseptet og man er avhengig av en god samordning på tvers av statlig sektor for å få dette til. Gjennomføringsrisikoen er lavest i konsept 1 der man i stor grad fortsetter som i dag, men med et tydeligere regelverk.

Samlet sett er det krevende å rangere de ulike konseptene etter samfunnsøkonomisk lønnsomhet. De ikke-prissatte virkningene er potensielt svært store og med ulike fortegn. Det er likevel mulig å trekke noen entydige konklusjoner. Konsept 1 er rangert lavere enn konsept 4 på alle virkninger, både prissatte virkninger, virkninger av nasjonal kontroll og virkninger av endret funksjonalitet og fleksibilitet. Konsept 1 har noe lavere gjennomføringsrisiko, men gjennomføringsrisikoen knyttet til konsept 4 er relativt lav og konsept 4 rangeres bedre på risiko for manglende etterlevelse av kravene. Det innebærer at dersom det skal innføres strengere krav til nasjonal kontroll over beskyttelsesverdige data og systemer vil konsept 4 være et bedre alternativ enn konsept 1.

Samme vurdering gjelder for konsept 2. For alle virkninger er både konsept 4, konsept 3 og konsept 7 rangert likt eller høyere enn konsept 2. Det innebærer at alle disse konseptene

framstår som mer hensiktsmessige løsninger enn konsept 2. Denne konklusjonen styrkes ytterligere av at konsept 2 er vurdert til å ha vesentlig høyere risiko knyttet til gjennomføring og fordi usikkerhet knyttet til de prissatte virkningene er høyere.

Da står vi igjen med tre alternativer i tillegg til nullalternativet: konsept 3, konsept 4 og konsept 7. Disse tre konseptene er det vanskelig å gjøre en robust rangering mellom. Konsept 4 har vesentlig lavere kostnader og rangerer derfor høyere på prissatte virkninger. Konsept 4 rangeres også høyere med hensyn til virkninger av endret funksjonalitet og fleksibilitet. Konsept 3 har imidlertid større positive virkninger knyttet til nasjonal kontroll. Risiko knyttet til etterlevelse av krav er også lavere enn i konsept 4, mens gjennomføringsrisikoen er nokså lik. K7 ligger mellom disse to konseptene på alle parametere. Ettersom de ikke prissatte virkningene kan være svært store, men er svært krevende å kvantifisere, har vi ikke samfunnsøkonomifaglig grunnlag til å rangere de tre konseptene seg imellom.

Vi har heller ikke grunnlag for å konkludere hvorvidt et, to eller tre av disse konseptene er samfunnsøkonomisk lønnsomme sett opp mot nullalternativet. Alle tre alternativer innebærer vesentlige kostnadsøkninger fra nullalternativet. Nullalternativet vil også gi høyere funksjonalitet og fleksibilitet. På den annen side innebærer nullalternativet lav nasjonal kontroll og med det høyere risiko for tap eller forringelse av sentrale offentlige tjenester i fred, krise og væpnet konflikt. Det kan medføre store konsekvenser. Hvorvidt risikoreduksjonen, ved gjennomføringen av konsept 3, 4 eller 7 er tilstrekkelig stor til å forsvare kostnadsøkningen har vi imidlertid ikke grunnlag for å vurdere.

7.5.2 Anbefaling

Den samfunnsøkonomiske analysen viser at kostnadene som følger av økt grad av nasjonal kontroll for hele statsforvaltningen er relativt store. Manglende nasjonal kontroll kan imidlertid medføre store konsekvenser, særlig i en krise eller væpnet konflikt. Verdien av økt nasjonal kontroll og forskjeller i funksjonalitet og fleksibilitet er svært vanskelig å anslå og det er derfor krevende å vurdere den samlede samfunnsøkonomiske lønnsomheten av de ulike konseptene.

Hvilket konsept som bør gjennomføres blir derfor i all hovedsak et spørsmål om hvilken risiko for tap eller forringelse av sentrale tjenester man er villig til å akseptere. Med manglende grunnlag for å vurdere hvor stor denne risikoen er, er dette mer et spørsmål om politiske prioriteringer enn samfunnsøkonomifaglige vurderinger. Dersom hensynet til kostnader veier tyngre enn hensynet til nasjonal kontroll bør nullalternativet videreføres. Hvis hensynet til nasjonal kontroll vektlegges tyngst, bør konsept 3 velges. Aksepterer man noe høyere risiko for å redusere kostnader og prioritere funksjonalitet, framstår konsept 4 som det mest egnede konseptet. Konsept 3 og konsept 4 er imidlertid ikke å anse som rene alternativer til hverandre. De kan også kombineres, slik det er gjort i konsept 7-kombinasjonskonseptet, som er det konseptet som gir størst fleksibilitet til å balansere hensynene til nasjonal kontroll, kostnadseffektivitet og funksjonalitet.

Resultatene fra denne utredningen viser at statsforvaltningen håndterer betydelig mengder beskyttelsesverdige data. Utredningen viser imidlertid også at det kan være stor variasjon i hvor stort behovet for nasjonal kontroll over disse dataene og systemene er. Videre viser analysene vi har gjennomført at nasjonal kontroll er kostnadsdrivende. Det er derfor gode argumenter for at den beste løsningen kan være en delt skyløsning (K7).

Beskyttelsesverdige data med behov for høy grad av nasjonal kontroll, lagres og behandles i en lukket statlig sky (K3-delen). Andre beskyttelsesverdige data kan lagres og behandles i en lukket kommersiell sky (K4-delen) med middels grad av nasjonal kontroll. På denne måten kan valg av løsning tilpasses ut fra en konkret vurdering av hver enkelt virksomhets behov for sikkerhet og funksjonalitet. En slik kombinasjonsløsning vil kunne legge til rette for at graden av nasjonal kontroll er tilpasset behovet for beskyttelse av data og det enkelte system. Det kan gi en løsning som sikrer nasjonale sikkerhetsinteresser samtidig som kostnadene begrenses og behovet for funksjonalitet ivaretas.

Som en minimumstilnærming anbefaler vi at det gjøres et arbeid med å samle og klargjøre de kravene som må følges ved bruk av skytjenester i staten allerede i dag. Det vil gjøre det enklere for statlige virksomheter å velge riktige og trygge løsninger. Dette vil imidlertid ikke være tilstrekkelig til å sikre nasjonal kontroll over sentrale beskyttelsesverdige data og systemer.

Ut ifra en totalvurdering anbefales det derfor at konsept 7 - kombinasjonskonseptet tas med til videre planlegging. Selv om det ikke er tilstrekkelig grunnlag, per nå, til å fastslå at dette alternativet er det mest samfunnsøkonomisk lønnsomme, gir konsept 7 tilstrekkelig fleksibilitet til å finne en hensiktsmessig balansegang mellom nasjonal kontroll og behovet for kostnadseffektive og funksjonelle løsninger. Hvilke krav til nasjonal kontroll som stilles til de ulike deløsningene og hvilke data og systemer som bør plasseres hvor, kan vurderes nærmere når mer detaljert informasjon om de relevante dataene og systemene foreligger.

8 Føringer for forprosjektfasen

Sentral informasjon skal overleveres fra utredningsfasen til forprosjektfasen, slik at beslutningstaker kan legge nødvendige føringer for det videre arbeidet med prosjektet.

Dette kapittelet beskriver forhold som er vesentlige for en vellykket gjennomføring av prosjektet. Det omfatter arbeid frem til forprosjektfasen, gjennomføring av forprosjektet, og den videre realisering av et innføringsprosjekt.

Vi legger til grunn at K7 Kombinasjonskonseptet tas med videre i planleggingsarbeidet i neste fase og at det realiseres i tråd med anbefalingen i alternativanalysen.

8.1 Videreføring av utredningsprosjektet

Arbeidet har frem til nå vært organisert som et prosjekt ledet av NSM med Justis- og beredskapsdepartementet (JD) som prosjekteier. Arbeidet har involvert statsforvaltningen gjennom informasjonsinnhenting og bruk av en referansegruppe, og har vært utført i tett dialog med leverandørindustrien. Prosjektet har vært finansiert over NSMs regulære budsjett uten ekstra bevilgninger, og sektorene har stilt med ressurser til intervjuer, møter og deltakelse i referansegruppen.

I oppdragsbrevet fra JD fremgår det at arbeidet med forprosjektfasen skal startes opp med tanke på en ferdig gjennomført KS1 til juni 2023. Dette innebærer at eksisterende prosjektorganisasjon bør videreføres, men i noe redusert omfang, både for å sikre god samhandling med eksterne kvalitetssikrer og for å kunne gjennomføre nødvendige aktiviteter. For å sikre en fortløpende forankring med sentrale aktører i statsforvaltningen, bør også dialogen med referansegruppen videreføres.

KVU-arbeidet har vist at det er av stor betydning å arbeide videre med:

- 1 Igangsette og følge opp arbeidet med **tydeliggjøring av regelverket** knyttet til bruk av skyløsninger i statsforvaltningen (ref. innholdet i K1 og inkludere deler av konseptet i realiseringen av K3 og K4).
- 2 Konseptene K3 og K4 skal kunne skaleres etter behov, men det er likevel viktig å ha et godt bilde av **hvilke datavolum og omfang** man skal starte dimensjoneringen av løsningene for. Datavolum er den viktigste kostnadsdriveren for konseptene. Virksomhetene i statsforvaltningen skal ha oversikt over egne skjermingsverdige data, og det er nødvendig å følge opp virksomhetene ytterligere for å klargjøre omfanget av skjermingsverdige og øvrig beskyttelsesverdige data og systemer.
- 3 Fortsette arbeidet med å utpeke og klassifisere skjermingsverdige infrastrukturer og objekter og **godkjenne skjermingsverdige informasjonssystemer**. Dette er nærmere utdypet i kapittel 8.2.

De ovennevnte aktivitetene kan starte opp før forprosjektet igangsettes, men bør uansett gjennomføres i parallell med eller som del av forprosjektet og det videre arbeid med gjennomføringen av tiltaket.

8.2 Utdypende om skjermingsverdige informasjonssystemer

Det er avgjørende at verdier som er av betydning for nasjonale sikkerhetsinteresser utpekes og sikres i tråd med lovens krav. I henhold til sikkerhetsloven § 6-1 er et informasjonssystem skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner. Videre stilles det i sikkerhetsloven § 6-3 krav om at skjermingsverdige informasjonssystemer skal godkjennes av en godkjenningmyndighet. Dersom det kan skade grunnleggende nasjonale funksjoner om informasjonssystemet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse, skal informasjonssystemet i tillegg pekes ut som skjermingsverdig objekt eller infrastruktur etter sikkerhetsloven §§ 7-1 og 7-2. Det vil si at informasjonssystemer i en nasjonal skytjeneste som skal behandle skjermingsverdig ugradert informasjon eller i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner, vil kunne pekes ut som skjermingsverdige informasjonssystemer som skal godkjennes, eventuelt som en del av en skjermingsverdig infrastruktur pekt ut i henhold til sikkerhetsloven § 7-1. Skjermingsverdig objekt og infrastruktur klassifiseres VIKTIG, KRITISK eller MEGET KRITISK utfra skadefølgene for grunnleggende nasjonale funksjoner, jf. § 7-2.

Det er departementene som innenfor sitt ansvarsområde skal utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur, jf. sikkerhetsloven § 7-1 andre ledd.⁵³ Klassifiseringen skal bygge på en skadevurdering. Det er virksomheten som gjør skadevurderingen.⁵⁴

Prosessen frem til godkjenningen av et skjermingsverdig informasjonssystem er en planlagt og systematisk gjennomgang av om virksomheten har oppnådd et forsvarlig sikkerhetsnivå, jf. virksomhetssikkerhetsforskriften § 52. Det må videre påregnes at en nasjonal skytjeneste vil kunne inneholde skjermingsverdige informasjonssystemer som kan klassifiseres som MEGET KRITISK, som utgjør det høyeste klassifiseringsnivået. Eventuelt vil de skjermingsverdige informasjonssystemene kunne inngå i en skjermingsverdig infrastruktur som er klassifisert på samme nivå. Dette vil igjen medføre de strengeste kravene til beskyttelsestiltak og godkjenning.

Prosessen innebærer blant annet en detaljert systembeskrivelse, inkludert en beskrivelse av systemets funksjon og operative miljø.⁵⁵ I utviklingen av den tekniske løsningen er det derfor viktig at prosjektet tidlig går i dialog med godkjenningmyndigheten for å sikre at løsningen vil imøtekomme krav til godkjenning, og dermed kan benyttes for å behandle skjermingsverdig ugradert informasjon slik den er tiltenkt. Prosjektet bør også gå i dialog med fagmiljøet i NSM som utarbeider tekniske krav. NSM har utarbeidet en offentlig tilgjengelig veileder for godkjenning av informasjonssystem.

⁵³ Se også virksomhetssikkerhetsforskriften § 56 og NSMs håndbok i klassifisering

⁵⁴ Se også virksomhetssikkerhetsforskriften § 57 og NSMs håndbok i skadevurdering

⁵⁵ Se NSMs veileder for godkjenning av informasjonssystem, inkludert vedlegg 1 - Sikkerhetsgodkjenning som en del av utviklingsprosess

8.3 Eierstyring

En videreføring av tiltaket stiller en rekke krav til eierstyringen. Det vil bli en kompleks gjennomføring som berører alle departementssektorer, og som har grenseflater mot prosjekter og aktiviteter i flere av disse, både knyttet til etablering av skyløsninger, men også etablerte enheter som markedsplassen hos DFØ. Gjennomføringen av tiltaket vil således dekke et stort aktørbilde og behovet for involvering av disse kan være ulikt i ulike faser av gjennomføringen. Riktig involvering av virksomhetene er en viktig forutsetning for å lykkes.

Også forhold utenfor Norges grenser kan påvirke gjennomføringen. Det er av stor betydning at problemstillingene knyttet til nasjonal sikkerhet ivaretas på en tilfredsstillende måte i det videre arbeid. Utover nasjonale sikkerhetsinteresser må også informasjonssikkerhet i de statlige virksomhetene ivaretas. Prosjektet vil etablere en fellesløsning som i sin natur grenser inn mot den statlige IKT-koordineringsrollen til KDD.

Disse forholdene illustrerer at det stilles store krav til kompetanse i styringsrollen, og det vil være av stor betydning at prosjekteier innehar erfaring fra og kompetanse med å styre store, komplekse, tverrsektorielle IKT-programmer. Basert på relevante styringsproblemstillinger, som vi har illustrert noen av over, bør det gjøres en vurdering av hvor eierskapet til det videre arbeid med tiltaket bør plasseres.

Når eierskapet plasseres, bør man også hensynta at roller og ansvar kan justeres over tid, hvor det kan være en eier- og pådriver i forbindelse med planlegging og forberedelse frem til endelig beslutning om iverksettelse (etter KS1), mens eierstyringen i gjennomføringsfasen kan gjenspeile eierskapet til den nasjonale enheten som etableres eller får ansvaret. Det vil være en fordel at det er samme eier i forbindelse med anskaffelse, innføring og drift. Enheten som etableres eller får ansvaret for innføring og drift av en nasjonal skytjeneste bør ha en strategisk, tverrsektoriell rolle og høy kompetanse innen IKT-drift og -utvikling.

Vi anbefaler at tiltakseier så raskt som mulig legger en plan for det videre arbeidet med tydeliggjøring av regelverk for bruk av skyløsninger. Regelendringsprosessen med høringer må ofte gjennomføres parallelt med planleggingen av tiltaket, og være koordinert slik at forslaget til vedtak av budsjett og regelendring kommer samtidig til Stortinget.

8.4 Finansiering

Innføringen av en nasjonal sky er i hovedsak basert på et politisk initiativ og ønske fra sentrale myndigheter. For virksomhetene vil det å ta i bruk en slik løsning trolig innebære økte kostnader uten at de selv nødvendigvis opplever økt nasjonal kontroll som en nytte de får direkte glede av. Av den grunn kan det forventes at staten sentralt dekker alle planleggings- og etableringskostnader for den nasjonale skyløsningen. Vi legger således til grunn at staten finansierer etableringen av den nasjonale skyløsningen.

Når det gjelder virksomhetenes bruk av de etablerte skytjenestene som tilbys, legger vi til grunn at de selv må betale for de tjenestene som blir benyttet (brukerbetaling). Dette vil da i utgangspunktet dekke drift, forvaltning og videre tjenesteutvikling. Det er imidlertid nødvendig å avklare om det rettslige grunnlaget for dette er i tråd med de juridiske vurderingene av konseptene som er gjort i Vedlegg F, og rammebetingelsene knyttet til regelverk om offentlige anskaffelser og statsstøtte.

For mange virksomheter vil en nasjonal skyløsning innebære tilgang på en moderne og solid skytjeneste som møter deres krav på en god måte. For virksomhetene som ikke benytter en skyløsning for beskyttelsesverdige data, vil det være rimelig at de selv må finansiere kostnadene ved å migrere sine egne løsninger fra dagens etablerte løsning til den nye nasjonale skyløsningen. Dette vil da dekke migrering fra en egendriftet lokal løsning som ikke er skybasert. For virksomhetene som allerede benytter allmenne og/eller lukkede skyløsninger fra kommersielle leverandører, vil de få en merkostnad ved å flytte sine løsninger over til en nasjonal sky. Det er ikke åpenbart at det er rimelig at de skal dekke disse kostnadene med egne midler. Det som taler for at de skal finansiere overgangen selv, er at skyløsningen i utgangspunktet burde ha blitt etablert i henhold til gjeldende regler, mens et argument imot er at rammebetingelsene har endret seg og virksomheten dermed påføres en ekstrakostnad de ikke kunne ha forutsett på forhånd. Dette bør avklares i forprosjektfasen.

I tabellen under viser vi noen prinsipper og kriterier som finansieringsmodellen bør tilfredsstille. Disse bør bearbejdes videre i forprosjektet.

Tabell 8-1 Prinsipper og kriterier for finansieringsmodellen

Prinsipp	Kriterier
Finansieringsmodellen bør understøtte ønsket utvikling for konseptet	Finansieringsmodellen bør understøtte ønsket utvikling for bruk av skyløsninger i staten. Det innebærer at virksomhetene motiveres til å legge til rette for arbeidet med å realisere konseptet på en mest mulig hensiktsmessig måte.
Finansieringsmodellen bør gi insentiver og legge til rette for bred og effektiv implementering av konseptet	Nytteeffektene av konseptet avhenger av bred implementering hos et stort antall virksomheter. Finansieringsmodellen bør derfor legge til rette for at dette kan skje effektivt.
Finansieringsmodellen bør gi en riktig fordeling av kostnadene mellom de ulike aktørene i de ulike fasene og ta hensyn til aktørenes gevinster	En riktig fordeling innebærer at kostnadene som bæres av den enkelte aktør tar hensyn til gevinstrealiseringspotensialet hos denne. Dette vil være viktig for å gi samfunnsøkonomisk riktige insentiver.
Finansieringsmodellen bør være forståelig, transparent, stabil og målbar	Forståelig: Modellen må være forståelig for de involverte partene og ikke kreve for store ressurser å sette seg inn i. Transparent: Berørte parter må lett kunne skaffe seg informasjon om prinsippene og beregningene som ligger til grunn for kostnadsfordelingen i modellen. Stabil (forutsigbar): Modellen må være forutsigbar, hvilket innebærer at det ikke forekommer hyppige og uforutsigbare endringer i reglene for fastsettelsen eller størrelsen på aktørenes finansieringsbidrag.

Prinsipp	Kriterier
	Målbar: Fastsettelsen av den enkeltes finansieringsbidrag bør bygge på et datagrunnlag som kan aksepteres av partene og som rimelig lett kan innrapporteres og kontrolleres.
Finansieringsmodellen bør være enkel og effektiv å administrere	Finansieringsmodellen bør utformes på en måte som er enkel å etterleve og mulig å administrere effektivt.

Et viktig prinsipp som må avklares er hvorvidt bruk av de nasjonale skyløsningene skal være frivillig for virksomhetene, eller om de skal pålegges å benytte alt eller deler av disse. Dersom den nasjonale skyløsningen ikke eller i liten grad tas i bruk av virksomhetene, vil statsforvaltningen i praksis bevege seg i retning av konsept 1, reguleringskonseptet. Dette er ikke en utviklingsretning som er samfunnsøkonomisk ønskelig (ref. vurderingene i kap. 7).

Vi anbefaler derfor at nødvendige tiltak iverksettes for å hindre dette. Dersom staten ønsker økt nasjonal kontroll, bør man vurdere hvilke virkemidler som skal iverksettes for å sikre at løsningen tas i bruk. Dette kan bevege seg fra anbefalinger, føringer i digitaliseringsrundskrivet, insentiver for å ta den i bruk, til pålegg om bruk. Det kan åpnes for ulike tilnærminger avhengig av om det er skjermingsverdige eller beskyttelsesverdige data og systemer.

Det er en sammenheng mellom valg av finansieringsmodell, bruk av insentiver, krav til innføring og valg av tidsfrist. Realisering av en lukket statlig sky vil innebære betydelige investeringer og høye faste driftskostnader. Det er samfunnsøkonomisk uheldig å investere samfunnets midler uten å vite med tilstrekkelig sikkerhet om løsningen vil tas i bruk eller ikke. Innen andre samfunnsområder som veibygging, kulturbygg eller forsvarsmateriell vil det være utenkelig at dette ikke skulle tas i bruk. Det samme bør gjelde for IKT-løsninger. Forventet bruksomfang vil også påvirke statens posisjon ved forhandlingene om å inngå en leverandøravtale, selv om det uansett forutsettes en fleksibilitet i løsningen for å håndtere ulike datavolumer og bruksmønstre.

Det bør etter utredningens syn være en stor grad av forpliktelse om deltakelse fra virksomhetene før et såpass stort tiltak som en nasjonal sky kan igangsettes. Dette for å sikre en komplett innføring i hele statsforvaltningen som styrker kontrollen over nasjonale skjermingsverdige data. Vi anbefaler at det inngås en bindende avtale med virksomhetene i forprosjektfasen, når finansieringsmodell og øvrige forutsetninger er på plass. Samtidig bør det også i forprosjektfasen vurderes om det skal iverksettes et pålegg om obligatorisk deltakelse for de virksomhetene som tar i bruk skyløsninger for skjermings- og beskyttelsesverdige data og systemer.

8.5 Sentralt styringsdokument

Tiltaket vil, siden det legges opp til å realisere både K3 og K4, ha et skille mellom løsninger for skjermingsverdige og øvrige beskyttelsesverdige data, noe som vil stille ulike krav overfor aktuelle tilbydere. Anskaffelsesprosessene i hhv. K3- og K4-delen vil ha likheter, men også innebære forskjeller som rettferdiggjør å gjennomføre det hele som to parallelle prosesser, organisert i hvert sitt prosjekt. Et prosjekt for anskaffelse (K4-delen) vil fokusere på å inngå

en avtale med en leverandør som tar ansvar for leveranse av skytjenester til sluttbruker, mens et prosjekt for etablering av en lukket statlig sky (K3-delen) vil ha fokus på å inngå en avtale med en partner for å bistå i å etablere de tjenestene den statlige skyen selv skal tilby. Siden vi også anbefaler å gjennomføre et arbeid med tydeliggjøring av regelverket, og at det deretter vil være et behov for et prosjekt for innføring, gevinstplanlegging og -realisering, er det mye som tyder på at tiltaket bør organiseres som et program⁵⁶ med underliggende prosjekter.

Ved gjennomføring av et program med underliggende prosjekter er det behov for å utarbeide et sentralt styringsdokument (SSD) både for programmet og prosjektene da dette vil være ulike styringsobjekter hvor det stilles ulike krav til gjennomføringen.

For programmet bør det utarbeides et SSD med beskrivelser som dekker definisjon av programmet med tydelig avgrensning av innhold og rammer, et målbilde som dekker utviklingen gjennom flere faser, en overordnet tidsplan for gjennomføringen, en samlet kostnadsramme (P50) og ressursbehov, organisasjonsplan med enheter, overordnede roller og ansvar, samt hvordan en helhetlig nyttestyring og risikostyring skal gjennomføres.

Det er også viktig å beskrive prosjektrekkefølge, sammenheng og avhengighet mellom prosjektene i anskaffelses- og innføringsfasen, samt sentrale beslutnings- og leveransepunkter.

For prosjektene bør det utarbeides et SSD som gjenspeiler prosjektenes innhold. Struktur og innhold i et slikt styringsdokument for prosjekter er definert i statens prosjektmodell og Finansdepartementets rammeverk, men detaljeringen må tilpasses prosjektets egenart, risiko og vesentlighet. Det skal fremgå av dokumentet hvordan føringer for forprosjektfasen gitt i KVV, KS1 og øvrige rammebetingelser er blitt og vil bli håndtert. Generelt anbefales det at viktige elementer fra KVV-en videreføres og bearbeides i forprosjektet. I forprosjektet bør det gjøres en vurdering av om det er mest relevant å utarbeide et felles eller separat SSD for gjennomføringen av hhv. K3- og K4-delen.

Det er i kapittel 4 beskrevet områder hvor det bør utarbeides indikatorer for måloppnåelse. Disse bør benyttes som utgangspunkt for en konkretisering av effekt- og resultatmål under målkapittelet i SSD. Utover dette bør innholdet i kapittelet om føringer for forprosjektet og relevante utdrag fra KVV-en for øvrig benyttes som utgangspunkt for utarbeidelsen av utfyllende dokumentasjon i SSD knyttet til overordnede rammer, prosjektstrategi og prosjektstyringsbasis.

SSD for et prosjekt skal i utgangspunktet inneholde en beskrivelse av alle områdene som er inkludert i tabellen under. Program-SSDen bør også ta utgangspunkt i denne, men gjøre et selektivt utvalg av hva som håndteres på hhv. program- og prosjektnivå.

⁵⁶ En god praksis er Managing successful programmes (MSP) fra Axelos.

Tabell 8-2 Områder i SSD

Overordnede rammer	Prosjektstrategi	Prosjektstyringsbasis
Hensikt, krav og beskrivelse av konsept	Strategi for styring av usikkerhet	Arbeidsomfang, herunder endringsstyring
Prosjekts effekt- og resultatmål	Gjennomføringsstrategi	Prosjektnedbrytningsstruktur (PNS)
Kritiske suksessfaktorer	Kontraktstrategi	Kostnadsoverslag, budsjett og investeringsplan
Rammebetingelser, inkludert føringer for forprosjektfasen	Organisering og ansvarsdeling	Gevinstrealiseringsplan
Grensesnitt mot andre prosjekter		Tidsplan
		Intern kvalitetssikring

8.6 Organisering

8.6.1 Forprosjektet

Organisasjonen som skal videreføre arbeidet med å etablere en nasjonal skyløsning, bør i forprosjektfasen være tverrfaglig sammensatt, og som et minimum omfatte prosjektledelse, samfunnsøkonomi, strategi/forretningsutvikling, teknologi/arkitektur og jus. Det er viktig at prosjektet eller den nasjonale enheten som skal stå ansvarlig for anskaffelsen fremstår med et klart ansvar, stor myndighet og tydelig rolle overfor leverandørene som deltar i anskaffelsesprosessen.

Vi anbefaler å bruke den allerede etablerte referansegruppen og å involvere disse for å sikre at behovene og kravene til løsningene blir så godt samordnet som mulig. Dette gjelder både i forprosjektet og i senere faser av gjennomføringen.

8.6.2 Programmet

Dersom tiltaket organiseres som et program bør det etableres et programstyre med programeier som leder. Programmets omfang og den sektorovergripende styringsstrukturen kan gjøre det nødvendig å etablere et overordnet eier- og styringsnivå som sikrer formelle investeringsbeslutninger og som ivaretar overordnet strategi og prioriteringer, herunder prioritering og avgrensninger mot andre strategiske tiltak i sektorene.

Organisering, varigheten på programmet, sammenhengen mellom prosjektene og tidspunkt for overlevering til linjen, er avhengig av anbefalt gjennomføringsstrategi og hvilket ansvar programmet eventuelt skal ha i gevinstrealiseringen. Disse forholdene bør avklares i forprosjektet. I den sammenheng er det viktig å avklare ansvar og myndighet mellom program- og prosjektnivå.

8.7 Gjennomføring

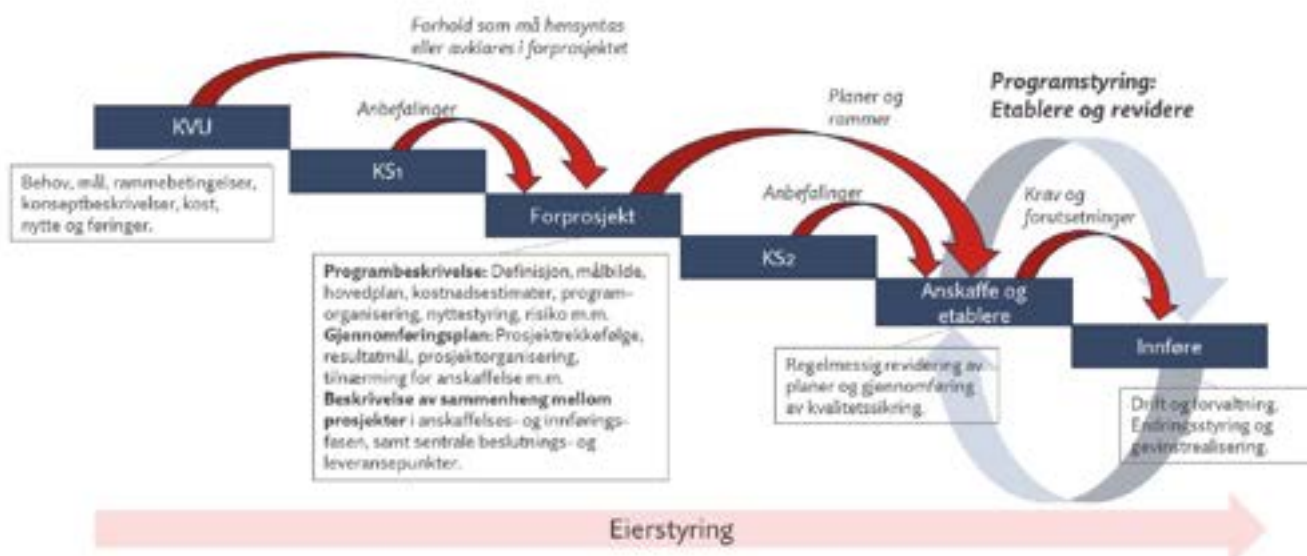
For å sikre faglige innspill og god forankring underveis i gjennomføringen, anbefaler vi at et bredt aktørbilde involveres i gjennomføring av tiltaket. I utgangspunktet vil det etter

utredningens vurdering være relativt generiske krav som stilles, basert på en basis tjenestekatalog over tjenester som kan etableres i løpet av relativt kort tid. Deretter vil det være en løpende tilpasning og videreutvikling av dette. Programmet vil ha et overordnet ansvar for å anskaffe tjenestene og etablere tjenestetilbudet, og vil på et egnet tidspunkt overlevere dette ansvaret til en linjeorganisasjon som viderefører arbeidet som en del av drift og forvaltning.

8.7.1 Faser i gjennomføringen

I kapittel 7.2 presenteres tidslinjen for gjennomføring av de aktuelle konseptene. Der forutsettes det at både K3- og K4-delen kan gjennomføres i løpet av 4 år fra oppstart av KS1. Denne rammen påvirkes av en rekke forhold: varighet på KS1, hvilket konsept som velges, hvilke forutsetninger eller føringer som følger med beslutningen, usikkerhet knyttet til varighet på KS2, juridiske avklaringer som skal gjennomføres, og hvilken konkret løsning som velges for å realisere K3-delen. Vi har av denne grunn ikke tegnet ut en tidslinje på nåværende tidspunkt, da det etter utredningens vurdering vil være en så stor usikkerhet knyttet til tidsplanen at den vil gi liten mening.

Gjennomføring av tiltaket vil dekke flere faser. Dette er illustrert i figuren under. Etter konseptvalget går man inn i forprosjektfasen hvor gjennomføringen av arbeidet planlegges og det utarbeides et styringsunderlag. En beslutning om å gå inn i en anskaffelses- og etableringsfase forutsetter at et betydelig og tilstrekkelig antall virksomheter forplikter seg eller pålegges av sitt departement til å ta i bruk løsningene. Etter anskaffelsen vil det være en fase for etablering av løsningen, før den settes i drift og innføres.



Figur 8-1 Faser i gjennomføringen

Varighetene som er indikert nedenfor er de samme som er lagt til grunn i kostnadskalkylen og er foreløpige og belagt med betydelig usikkerhet. I kap. 8.10 Suksessfaktorer er det beskrevet aktiviteter som kan redusere gjennomføringsrisiko og bidra til en raskere gjennomføring. Spesielt aktivitet 5, 6, 7 og 8 har mulighet for en raskere gjennomføring.

1. Ekstern kvalitetssikring (KS1) starter i begynnelsen av februar 2023 og har en estimert varighet til juni 2023.

2. Arbeidet med regelverk bør starte så raskt som mulig og vil trolig ha varighet ut forprosjektet.
3. Videreføring av utredningsprosjektet bør pågå frem til oppstart av forprosjektet og deretter bli en del av dette.
4. Beslutning om gjennomføring bør kunne fattes på regjeringsskonferansen høsten 2023.
5. Forprosjekt bør kunne starte opp høsten 2023 og vil trolig ha en varighet på opp mot 12 måneder, til sommer/høst 2024.
6. Ekstern kvalitetssikring (KS2) kan starte etter avsluttet forprosjekt, dvs. høsten 2024, og vil trolig ha en varighet på 3-4 måneder.
7. Gitt en gjennomføring som indikert over, vil man kunne starte arbeidet med å etablere en lukket, nasjonal sky på nyåret 2025. Vi legger til grunn at det vil ta 12 - 24 måneder, avhengig av valgt løsning. Etter utredningens vurdering innebærer dette bruk av kjent teknologi, og bør kunne gjennomføres på nærmere 12 enn 24 måneder.
8. Det bør være mulig å innføre deler av en nasjonal skyløsning i løpet av 2025, mens en komplett løsning kan komme på plass i løpet av 2026.

For å balansere risiko, kostnader og gevinster, samt håndtere endringer i rammebetingelser på en best mulig måte, bør forprosjektet ta stilling til hvilke prinsipper som bør ligge til grunn for videre arbeid i forprosjektfasen. Prinsippene kan eksempelvis ta utgangspunkt i det følgende:

- Dele opp gjennomføringen i mindre prosjekter
- Bygge på erfaring fra tilsvarende prosjekter
- Sikre kontroll på omfanget
- Gradvis innføring og løpende tjenesteutvikling

En overordnet anbefaling er at konseptet realiseres med trinnvis innføring og selvstendige og veldefinerte prosjekter som godkjennes hver for seg, men innenfor samme helhetlige styringsramme.

Planen for det videre arbeid bør detaljeres frem til forprosjektet starter, og deretter bli del av prosjektstyringsbasis i SSD.

8.7.2 Sentrale beslutninger

Tiltaket vil gå gjennom en rekke beslutningspunkter hvor det må besluttet om man skal gå videre, stanse gjennomføringen, eller endre strategi. Det bør i forprosjektet beskrives hvilke beslutninger som må fattes fra oppstart av forprosjektfasen til signering av kontrakt med en leverandør av skytjenester (K4-delen) og ferdigstillelse av etableringsfasen (K3-delen). Disse bør settes opp som milepæler med innbyrdes avhengighet.

Det bør tas følgende beslutninger før oppstart av forprosjektet:

- Beslutning om valg av konsept, gjennomføring og finansiering
- Beslutning om å starte opp arbeidet med å etablere / tydeliggjøre regelverket for bruk av skytjenester
- Beslutning om å videreføre utredningsprosjektet med mandat og rammer

Det vil etter forprosjektet være en rekke beslutningspunkter hvor det må fattes beslutninger om hvorvidt og i hvilken retning man vil gå videre. Det vil etter utredningens syn ikke være realistisk å gå videre med realiseringen dersom man ikke lykkes med å etablere en styrings- og finansieringsmodell som oppmuntrer og forplikter virksomhetene i tilstrekkelig grad til å ta i bruk den nasjonale skyløsningen. Gjennomføring betinger også at man, både for i K3- og K4-delen av programmet, lykkes med å tiltrekke seg relevante leverandører.

En viktig avklaring er knyttet til hvor mye gjenbruk av infrastruktur som lar seg realisere ved etablering av en lukket statlig sky. Dette vil både kunne påvirke løsningen, kostnader, fremdrift og samfunnsøkonomisk lønnsomhet.

Den samfunnsøkonomiske analysen viser at K3 begynner å gi gevinster fra omkring 2026. Det forventes at det vil ta opp til 10 år for virksomhetene å legge over nåværende systemer til skybaserte løsninger. I gjennomføringsstrategien bør det vurderes hvilke tiltak som er mulige å iverksette for å sikre en raskere innføring og gevinstrealisering.

Gjennomføringen av tiltaket vil måtte skje over flere år og strategien må derfor kunne håndtere endringer i politiske rammebetingelser og teknologiske og strukturelle endringer. Noen momenter knyttet til dette er:

- Politiske endringer kan innebære nye nasjonale rammebetingelser som gir nye føringer for betydningen av nasjonal kontroll, nye reguleringer fra EU (f.eks. knyttet til videreføring av Schrems II-dommen), eller nytt regelverk.
- Teknologiske endringer kan innebærer nye muligheter for å øke sikkerhetsnivået knyttet til integritet, konfidensialitet og tilgjengelighet.
- Strukturelle endringer kan innebærer nyetableringer av løsninger på norsk jord som imøtekommer krav om nasjonal kontroll på nye og forbedrede måter enn i dag.

8.7.3 Optimalisering av samfunnsøkonomisk lønnsomhet

Det må utarbeides en plan i forprosjektet for arbeidet med å optimalisere samfunnsøkonomisk lønnsomhet i senere faser. Denne planen må sees i sammenheng med tiltakene vi anbefaler i kapittel 8 Føringer for forprosjektfasen, planlagte tiltak for å optimalisere skyløsningene, samt endelig valg av drifts- og forvaltningsorganisasjon. Momentene under er hentet fra KVV-veilederen, og må i forprosjektet tilpasses realiseringen av besluttet konsept.

- Viktige elementer til et videre arbeid med en gevinstrealiseringsplan som omfatter tiltak for å realisere nyttesiden i prosjektet.
- Gjøre vurderinger av i hvilken grad nyttevirksomheter vil realiseres som effektivisering eller som kvalitetsheving og begrunn vurderingene.

- Anbefaling om styringsmessig fleksibilitet, herunder potensielle forenklinger og reduksjoner det kan jobbes videre med for å redusere kostnadsnivået.
- Når det er kjent og mulig, synliggjør forutsetninger og nødvendige tiltak for realisering av nytte og synliggjør sentrale risikoelementer for at nytten vil bli lavere enn det som er lagt til grunn i den samfunnsøkonomiske analysen. Dette er særlig relevant for prosjekter der nytten i stor grad skal realiseres i en annen styringslinje enn der hvor prosjektet ligger og kostnadene påløper.

Annet:

- Planen for forprosjektet bør sees i sammenheng med budsjettprosessen og det bør legges en plan for videre kvalitetssikring av prosjektet etter KS1.

8.8 Avhengigheter til andre prosjekter

Det er en sentral oppgave i et forprosjekt å videreutvikle oversikten over tilgrensende prosjekter, både med tanke på hvor de er i en beslutnings- og gjennomføringsprosess, hvilke data de omfatter, i hvilken grad de kan utvides til å dekke et større område, og hvor teknisk egnet de er til å bli integrert med eller være en del av en nasjonal skyløsning. Hensikten med dette er å ha oversikt over og kunne realisere mulige synergieffekter, samtidig som staten unngår investeringer i overlappende løsninger.

I Vedlegg A og Vedlegg I presenteres nasjonale og internasjonale prosjekter som kan ha innvirkning på realiseringen av en konkret nasjonal skyløsning. Det er viktig å følge disse prosjektene gjennom forprosjektfasen, sikre nødvendig dialog, og iverksette relevante tiltak basert på dette.

Betydningen av de omkringliggende prosjektene er forskjellig for hhv. K3- og K4-delen av K7. Siden K3-delen skal dekke skjermingsverdige data, mens K4-delen skal dekke andre beskyttelsesverdige data, vil muligheten for å oppnå synergieffekter og å unngå investeringer i overlappende løsninger i hovedsak gjelde for K3. K4-delen, som trolig vil håndtere det største datavolumet, kan skaleres opp og ned avhengig av bruksomfang uten at dette vil påvirke nytten av investeringer – det vil kun påvirke omfanget av tjenestekjøp. Dette vil ikke være tilfelle for K3-delen hvor en større grad av investeringer må gjennomføres uansett for å få skyløsningene og en nødvendig organisasjon operative. Deretter vil løsningen skaleres avhengig av hvor mye av de andre beskyttelsesverdige dataene som virksomhetene velger å lagre og behandle der.

8.9 Kontraktstrategi

Kontraktstrategi utgjør en sentral del av gjennomføringsstrategien. Den skal utarbeides i forprosjektet og oppsummere sentrale strategiske valg som vil påvirke risikoen i gjennomføringsprosjektet og muligheten til å realisere ønskede gevinster.

8.9.1 Forskjeller mellom konseptene

Konseptet som tas med videre til forprosjektet, har flere grunnleggende forskjeller mellom de to delene, som innebærer at tilnærmingen til bruk av leverandører og dermed hvilke typer kontrakter som skal inngås, kan avvike.

K3-delen innebærer at staten inngår flere avtaler, hvorav de viktigste er knyttet til:

- Leiekontrakt for tilgang til datasentre
- Anskaffelse av utstyr og programvare til utrustning av datasentrene og nødvendig datakommunikasjon
- Avtale med partnere som skal benyttes for å etablere og understøtte leveransen av skytjenestene
- Avtale om tilrettelegging for en sikkerhetskopi (evt. reserveløsning) utenfor Norge.

K4-delen innebærer at staten:

- Inngår avtale med partnere som skal levere skytjenester

8.9.2 Felles tilnærming

Anskaffelsesregelverket er særlig viktig for dette konseptet og det må i forprosjektet gjøres konkrete vurderinger av hvordan regelverket kommer til anvendelse for dette konseptet. Det vises til Vedlegg Juridiske vurderinger - Notat Haavind (del 2).

Vi anbefaler at forprosjektet gjennomfører en markedsdialog i forbindelse med utarbeidelse av konkurransegrunnlaget for blant annet å evaluere om kravene som stilles harmonerer med utviklingsretningen innen leverandørmarkedet.

Det bør bygges inn realopsjoner om fleksibilitet i kontrakten, med særskilt vekt på å kunne variere løsningen og avslutte tiltaket.

Det kan være nødvendig å utrede behovet for andre rettslige endringer, blant annet for å kunne pålegge virksomheter å ta i bruk løsningen.

I Vedlegg E Mulighetsstudien (basert på innholdet i Vedlegg F) påpekes det behov for nærmere juridiske avklaringer knyttet til begge konseptene. Dette må sees på i tillegg til innholdet i de to kapitlene under.

8.9.3 Tilnærming for lukket statlig sky (K3-del)



Avtale med partnere som skal benyttes for å etablere og understøtte leveransen av skytjenestene må etableres. Her vil mange av forholdene beskrevet under K4 gjelde, men med en vesentlig forskjell knyttet til ansvar, rolle og leveranser.

8.9.4 Tilnærming for lukket kommersiell sky (K4-del)

Det vil være viktig å gjøre en analyse av leverandørenes risikoeksponering og evne til å bære risiko, og å tilpasse kontraktsdokumentene i forhold til dette. Et element i dette vil

kunne være å ha et særlig høyt fokus på å vurdere aktuelle leverandørers kvalifikasjoner og ved å utforme gode insentivmekanismer i kontrakten(e).

Det vil være avgjørende i hvilket omfang skyløsningen kan anses som skjermingsverdig infrastruktur/informasjonsystem, og i hvilken grad dette innebærer at anskaffelsen kan sikkerhetsgraderes eller på annen måte bare kan utføres under særlige sikkerhetstiltak, slik at det kan gjøres unntak fra anskaffelsesregelverket (ref. Vedlegg C). Det må avklares om det er mulig at de statlige virksomhetene står fritt til å velge hvilken av de valgte leverandørene de skal inngå avtale med.

Det er et stort leverandørmarked for skytjenester. Oversikten i Vedlegg A knyttet til den utsendte RFI og bredden av leverandører som leverer skytjenester, underbygger utredningens forventning om at det vil være stor interesse for å inngå en avtale med staten om leveranse av skytjenester for beskyttelsesverdige data og informasjonssystemer.

Vi mener det vil være riktig at anskaffelsen baseres på to kategorier av krav. På den ene siden er det nødvendig med entydige krav knyttet til nasjonal kontroll som leverandørene må innfri. På den annen side anbefales det å benytte åpne behovsbeskrivelser, slik at leverandørene har rom for å presentere moderne løsninger på kundens behov, og også slik at det legges til rette for å videreutvikle løsningene etter at kontrakt er inngått.

Et annet forhold som vil være av stor betydning for i hvilken grad anskaffelsen vil kunne gi grunnlag for gevinstrealisering, er hvilke opsjoner på utvidelser som inkluderes i kontrakten. Dette kan være både opsjoner på utvidet funksjonalitet og på at løsningen kan tas i bruk av nye brukergrupper og andre virksomheter. Dersom kontrakten ikke inkluderer relevante opsjoner, for eksempel for nye brukergrupper, må det avklares om det er mulig på et senere tidspunkt å utvide bruken av løsningen til disse.

8.10 Suksessfaktorer

Kritiske suksessfaktorer bør gås gjennom og oppdateres ved oppstart av forprosjektet. Sammen med innholdet i usikkerhetsanalysen bør dette danne grunnlag for risikoanalysen som skal utarbeides i forprosjektet og benyttes under gjennomføringen av programmet med underliggende prosjekter.

Vi har identifisert noen sentrale suksessfaktorer med forslag til risikoreduserende tiltak i tabellen under. Disse vil også fungere som fallgruver dersom man «snur» innholdet i suksessfaktorene.

Tabell 8-3 Oversikt over kritiske suksessfaktorer

Identifiserte suksessfaktorer	Anbefalte tiltak
Aktiv eier- og programstyring (forprosjekt og gjennomføringsfasen)	• Klare rolle- og ansvarsbeskrivelser mellom involverte departementer og underliggende etater • Programmet bør rapportere til kun ett departement. • Klar oppdeling av helhetlig portefølje av tilgrensende programmer og prosjekter • Etablere styringsgruppe med hensiktsmessig ansvar og myndighet
Velfungerende finansieringsmodell	• Kartlegge og etablere prinsipper for finansieringsmodellen • Avklare kriterier for innføring; frivillighet kontra pålegg om

Tilstrekkelig grunnlag for gjennomføring	innføring • Sikre nødvendig forpliktelse hos aktørene • Realisering av konseptene forutsetter både tydeliggjøring av regelverk og nærmere vurdering av gjennomføringen opp mot: • Konkurranseregulering • Sikkerhetslovgivning • Annen lovgivning • Utredning og avklaring av nødvendig grunnlag for gjennomføringen må gjøres i forprosjektfasen
Kontraktstrategi som dekker anskaffelsen	• Valg av kontraktstrategi overfor leverandører, herunder inkludere opsjoner som gir mulighet for utvidelser både knyttet til funksjonalitet og nye brukergrupper/virksomheter • Dialog med potensielle leverandører • Sikre innovasjon i hele anskaffelsesperioden
God program- og prosjektstyring	• Gi program- og prosjektleder et klart og entydig mandat med tilhørende myndighet som er forankret og blir respektert • Sikre kapasitet, kompetanse og kontinuitet
Mengde data, systemer og deltakende virksomheter er tilstrekkelig	• Sikre bedre oversikt over mengde beskyttelsesverdig data og systemer • God interessenthåndtering der relevante innspill og synspunkter hensyntas, og andre sorteres bort på en hensiktsmessig måte • Gjøre løsningen attraktiv for virksomhetene • Godkjenning av tilstrekkelig antall skjermingsverdige systemer
Etablering av driftsorganisasjon med tilstrekkelig kompetanse	• Attraktive ansettelsesvilkår • Sikre kapasitet, kompetanse og kontinuitet
Gevinstrealiseringsplan og endringsledelse	• Klargjøre ansvar for gevinstrealisering gjennom en tydelig plan • Løpende oppdatering og videreutvikling av gevinstrealiseringsplanen • Gi de statlige virksomhetene ansvar for å realisere gevinstene innen sitt område