STORTINGET

Innst. 488 S

(2024–2025)

Innstilling fra kontroll- og konstitusjonskomiteen om sak om Program for felles IKT-tjenester i departementsfellesskapet

Vedlegg 1: Referat fra åpen høring

STORTINGET

Innst. 488 S

(2024–2025)

Innstilling til Stortinget
fra kontroll- og konstitusjonskomiteen

Innstilling fra kontroll- og konstitusjonskomiteen om sak om Program for felles IKT-tjenester i departementsfellesskapet

Til Stortinget

Bakgrunn

Program for felles IKT-løsninger i departementsfellesskapet er styrt av Digitaliserings- og forvaltningsdepartementet (DFD) og Forsvarsdepartementet (FD) i fellesskap, jf. Prop. 18 S (2022–2023).

I dag er det fire ulike IKT-plattformer i bruk i departementsfellesskapet: plattformene til FD/Statsministerens kontor (SMK), Justis- og beredskapsdepartementet (JD), Utenriksdepartementet (UD) og plattformen som benyttes av resten av departementene som ble driftet av Departementenes sikkerhets- og serviceorganisasjon (DSS). Fra 1. januar 2025 driftes de tre siste av Departementenes digitaliseringsorganisasjon (DIO). Dette er lite hensiktsmessig både fra et teknisk og økonomisk perspektiv. Det er svært dyrt og krevende å opprettholde og sikre tre ulike plattformer til samme høye standard. I tillegg øker angrepsflatene mot departementene når man har flere ulike plattformer.

Programmets mål er å bistå i å etablere en ny IKT-virksomhet og legge til rette for en felles digital plattform for applikasjoner og løsninger og for lagring og behandling av ugradert og skjermingsverdig ugradert informasjon. Plattformen vil tas i bruk av alle departementene, SMK og utenrikstjenesten og være særlig innrettet mot å ivareta digital sikkerhet tilpasset fremtidens trusselbilde. Programmet er organisert med en programleder og underliggende prosjekter. Det er etablert et programstyre som i dag består av DFD, FD, UD, JD og SMK. DIO og DSS er observatører i programstyret.

Arbeidet med å samle departementenes IKT-miljøer og IKT-løsninger har pågått i flere år. Det ble utarbeidet en konseptvalgutredning i 2017. I 2021 ble det startet et forprosjekt. Dette ledet fram til program for felles IKT-tjenester i departementsfellesskapet, som ble kvalitetssikret (KS2) i 2022. Mot slutten av 2022 fastsatte Stortinget en kostnadsramme på 1,4 mrd. kroner inkl. mva., jf. behandlingen av Prop. 18 S (2022–2023). Målbildet ved oppstart av programmet var å etablere en ny felles IKT-plattform gjennom anskaffelse i markedet. Den nye plattformen skulle i hovedsak være basert på en privat skyløsning levert av en tredjepart. De tidligere IKT-miljøene skulle samles i et nytt forvaltningsorgan underlagt det daværende Kommunal- og distriktsdepartementet.

Plattformen som ble driftet av DSS, ble utsatt for et svært alvorlig dataangrep sommeren 2023. Dette medførte en usikkerhet og et ytterligere behov for å snarest mulig få etablert en ny felles IKT-plattform.

Etter dataangrepet mot IKT-plattformen til DSS sommeren 2023 var ikke dette målbildet lenger mulig å gjennomføre. Programmet ble derfor nødt til å utrede en ny løsning som var gjenstand for ekstern kvalitetssikring sommeren 2024. Stortinget fastsatte høsten 2024 ny kostnadsramme på 2,24 mrd. kroner inkl. mva., jf. behandlingen av FDs Prop. 1. S (2024–2025). Endringen i kostnadsrammen skyldtes i hovedsak dataangrepet 2023.

Departementene ble 21. oktober 2024 varslet av DSS om at samlet forbruk av rammeavtale for konsulentbruk på IKT-området hadde oversteget maksimal

økonomisk ramme på 600 mill. kroner. For denne rammeavtalen mottok DSS statusrapporter fra leverandøren hver sjette måned. Som følge av høyt uttak på avtalen mellom rapporteringstidspunktene ble det ikke tidsnok oppdaget at avtalen ville bli oversteget i løpet av høsten 2024. DSS hadde på dette tidspunktet allerede satt i gang et arbeid for å få på plass en ny rammeavtale med forventet signering innen mars 2025. Arbeidet med inngåelse av ny rammeavtale ble intensivert så langt det var praktisk mulig.

Ny avtale ble signert av DIO 25. januar 2025. Ansvaret for avtalen ble flyttet fra DSS til DIO da IKT-miljøet til DSS ble en del av DIO ved DIOs opprettelse 1. januar 2025.

Etter at DSS og departementene som brukte avtalen, fikk kjennskap til overforbruk av avtalen, ble det iverksatt tiltak for å redusere bruken av avtalen til et absolutt minimum. Departementene og DSS så seg imidlertid nødt til å videreføre konsulentoppgaver som var helt nødvendige for å opprettholde driften og sikkerheten på IKT-plattformene til departementene. Det ble også vurdert som nødvendig å opprettholde et minimumsnivå av aktivitet i utviklingsprosjektene, slik at disse ikke skulle stoppe opp.

Det ble satt i gang flere kompenserende tiltak for at overforbruk på felles rammeavtaler ikke skulle skje igjen:

- I den nye rammeavtalen for konsulentmegling plikter leverandøren hver måned å sende DIO en rapport over hvor mye som er fakturert totalt under rammeavtalen.
- I tillegg stilles det krav til leverandøren om en digital kundeportal som skal gi tilgang til informasjon og tjenester og ha rapporteringsmuligheter som skal gi oversikt over aktive avrop på avtalen m.m.
- DSS skal gå gjennom og vurdere kontraktsoppfølgingen av fellesavtaler og skal foreslå eventuelle forbedringstiltak til DFD. Dette er et oppdrag gitt i tildelingsbrev for 2025.

Komiteens behandling av saken

På bakgrunn av oppslag i media startet komiteen undersøkelser i saken 11. februar 2025 ved å sende brev til digitaliserings- og forvaltningsministeren med spørsmål om rammeavtaler i staten og fikk svar 18. februar 2025. Komiteen sendte oppfølgingsspørsmål i brev av 4. og 25. mars 2025 og fikk svar hhv. 14. mars og 1. april 2025. Korrespondansen følger som vedlegg til innstillingen.

Komiteen vedtok i møte 8. april 2025 å åpne sak om program for felles IKT-tjenester i departementsfellesskapet, jf. Stortingets forretningsorden § 15 første ledd andre punktum.

Åpen kontrollhøring 12. mai 2025

Som ledd i behandlingen av saken gjennomførte komiteen en åpen kontrollhøring mandag 12. mai 2025. Komiteen besluttet at høringen skulle omhandle – men ikke begrense seg til – følgende problemstillinger:

- Hvordan ble hensynet til sikkerhet vektlagt i forbindelse med byttet av plattform for felles IKT-løsning i 2023?
- Har program for felles IKT-løsninger for departementsfellesskapet vært forvarlig styrt i forbindelse med endringen av målbildet?
- Hvordan er utsiktene til at prosjektet etter endringene kan realiseres i tide innenfor fastsatt økonomisk ramme?

Følgende ble invitert og møtte til høringen:

- Digitaliserings- og forvaltningsminister Karianne O. Tung
- Forsvarsminister Tore O. Sandvik
- Tidligere kommunal- og distriktsminister og tidligere forsvarsminister Bjørn Arild Gram
- Tidligere kommunal- og distriktsminister Sigbjørn Gjelsvik
- Direktør for Departementenes sikkerhets- og serviceorganisasjon Torgeir Swensson Strøm
- Direktør for Departementenes digitaliseringsorganisasjon Anders Aagaard Sørby.

Stenografisk referat fra høringen følger som vedlegg til innstillingen.

Innhenting av dokumentasjon vedr. faglig grunnlag

Komiteen sendte 16. mai 2025 brev til digitaliserings- og forvaltningsministeren og ba om å få oversendt dokumentasjonen vedrørende det faglige grunnlaget for veivalgene i programmet, herunder for skifte av målbildet vinteren 2023. Digitaliserings- og forvaltningsministeren oversendte den etterspurte dokumentasjonen 22. mai 2025.

Dokumentasjonen gir en vesentlig innsikt i teknisk innretning og vurderinger knyttet til IKT-systemene til departementsfellesskapet. Hvis informasjonen blir kjent for uvedkommende, vil dette kunne bidra til å lette straffbare handlinger slik som etterretningsvirksomhet. Dokumentene er derfor unntatt offentlighet med hjemmel i offentleglova § 24 tredje ledd.

Korrespondansen med statsråden, som inneholder en oversikt over den oversendte dokumentasjonen, følger som vedlegg til innstillingen.

Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Kari Henriksen, Frode Jacobsen og Kirsti Leirtrø, fra Høyre, lederen Peter Frølich og Svein Harberg, fra Senterpartiet, Eivind Drivenes og Willfred Nordlund, fra Fremskrittspartiet, Carl I. Hagen, fra Sosialistisk Venstreparti, Audun Lysbakken, fra Rødt, Seher Aydar, og fra Venstre, Naomi Ichihara Røkkum, viser til at utgangspunktet for saken var to oppslag i Aftenposten hhv. 4. og 5. februar 2025 om programmet for felles IKT-løsning for departementsfellesskapet. De to oppslagene hadde følgende overskrifter:

«– Toppbyråkrater vraket gjenbruk. Nytt datasystem: 2,2 milliarder.
– Sprengte konsulentavtale med 130 millioner kroner.»

Komiteen viser videre til at medieomtalen førte til at komiteen 11. februar 2025 sendte et brev til digitaliserings- og forvaltningsminister Karianne Oldernes Tung med to spørsmål om rammeavtalene for konsulentbruk. Brevet ble besvart 18. februar 2025 og senere fulgt opp med nye brev fra komiteen hhv. 4. og 25. mars 2025 og svar fra statsråden hhv. 14. mars og 1. april 2025.

Komiteen har konsentrert seg om tre hovedspørsmål:

1. Kostnader til eksterne konsulenter.
2. Informasjon til Stortinget om endringer i utviklingsarbeidet med IKT-plattformen.
3. Sikkerhetsvurderinger ved beslutninger om endringer i utviklingsarbeidet.

Komiteen viser til at den på bakgrunn av informasjonen i saken besluttet å åpne sak om IKT-plattform for departementsfellesskapet 8. april 2025 og avholde en åpen høring om saken 12. mai 2025.

Komiteen besluttet å legge følgende problemstillinger til grunn for å belyse saken i høringen:

– Hvordan ble hensynet til sikkerhet vektlagt i forbindelse med byttet av plattform for felles IKT-løsning i 2023?
– Har program for felles IKT-løsninger for departementsfellesskapet vært forsvarlig styrt i forbindelse med endringen av målbildet?
– Hvordan er utsiktene til at prosjektet etter endringene kan realiseres i tide innenfor fastsatt økonomisk ramme?

Disse tre problemstillingene var ikke til hinder for at andre relaterte problemstillinger kunne bli løftet i høringen.

Bakgrunn

Komiteen legger til grunn at det under regjeringen Solberg i 2017 ble gjennomført en konseptvalgutredning for IKT-løsning for departementsfellesskapet, samt at det våren 2021 ble startet et forprosjekt.

Komiteen legger også til grunn at dette ledet frem til et program for felles IKT-tjenester i departementsfellesskapet, som så ble kvalitetssikret i en KS2-prosess høsten 2021 og våren 2022.

I høringen uttalte statsråd Karianne O. Tung:

«Så endret man jo det målbildet. Man gikk fra FDs tonivåplattform mot høsten 2021 og tok en beslutning om å gå til privat lukket sky. Man arbeidet så med forprosjektet og gjorde det klart for ekstern kvalitetssikring våren 2022.»

Komiteen legger videre til grunn at planen i en periode var å bruke FDs tonivåplattform. Komiteen oppfatter også at det på dette stadiet var noe Nasjonal sikkerhetsmyndighet (NSM) ut fra sikkerhetshensyn vurderte var en mulig løsning.

Komiteens medlemmer fra Høyre og Venstre understreker at FDs tonivåplattform fortsatt er i daglig bruk av Forsvarsdepartementet og Statsministerens kontor, samt at den er sikkerhetssertifisert av Nasjonal sikkerhetsmyndighet (NSM).

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser til at tidligere forsvarsminister Gram sa følgende i høringen:

«Målbildet ved oppstart av programmet var å etablere en ny felles IKT-plattform gjennom anskaffelse i markedet. Den nye plattformen skulle i hovedsak være basert på en privat skyløsning levert av en tredjepart. De tidligere IKT-miljøene skulle samles i et nytt forvaltningsorgan underlagt det daværende Kommunal- og distriktsdepartementet. Ekstern kvalitetssikrer ga tilbakemelding om at valgt målbilde kunne være hensiktsmessig, men de ba oss om å vurdere å etablere en ny plattform med gjenbruk av komponenter fra Depnet/U.»

Videre viser disse medlemmer til det statsråd Tung sa:

«Så endret man jo det målbildet. Man gikk fra FDs tonivåplattform mot høsten 2021 og tok en beslutning om å gå til privat lukket sky. Man arbeidet så med forprosjektet og gjorde det klart for ekstern kvalitetssikring våren 2022.»

Slik det framstår for disse medlemmer, ble en kvalitetssikring påbegynt av regjeringen Solberg våren 2021. Den ble imidlertid stoppet da ekstern kvalitetssikrer mente at styringsdokumentene som forelå, ikke tilfredsstilte kravene for KS2, og at det dermed ikke var grunnlag for videre kvalitetssikring. Disse medlem-

mer viser til det departementsråd i Forsvarsdepartementet sa i høringen for å belyse hvordan dette ble oppfattet:

«Den eksterne kvalitetssikringen og starten på den, som egentlig ble anbefalt stoppet av en ekstern leverandør, var egentlig startskuddet for å begynne å vurdere om dette var en riktig vei videre. Så det var der vridningen mot en privat sky istedenfor FDs tonivåplattform egentlig startet.»

Disse medlemmer ser det slik at det departementsråd Hermansen svarte i høringen, illustrerer hvorfor man ikke gikk videre med FDs tonivåløsning:

«Det vi så da vi begynte å jobbe med å realisere den prinsippbeslutningen som var tatt tidligere, var at med en gang man skal ha med andre departementer som har helt andre grensesnitt – utenrikstjenesten med hundre utenriksstasjoner, Finansdepartementet med tunge makromodeller, osv. – ville det være ekstremt vanskelig og kostnadskrevende og innebære enormt mye 'one-off', altså særløsninger, for å kunne få det til å fungere. Det var nok også det som preget litt den første runden med ekstern kvalitetssikring, hvor ekstern kvalitetssikrer sa at grunnlaget ikke var godt nok for å gå videre. Dette var i 2020–2021. Da så vi at skal vi lage en plattform som møter de målsettingene – altså både sikker, effektiv og kostnadsforsvarlig drift – kunne ikke det bygges på FDs opprinnelige tonivåplattform. Derfor gikk man til Stortinget med endringsproposisjonen i 2022 og anbefalte at man brukte FDs plattform mot det graderte, men lagde en ny, ugradert plattform som skulle sikkerhetsgodkjennes, basert på en kommersiell leveranse fra leverandører. Så det er årsaken til at man gikk vekk fra det opprinnelige.»

Disse medlemmer viser til Prop. 18 S (2022–2023), hvor det står:

«Programmet legg til rette for ei felles løysing som handterer ugradert, ugradert skjermingsverdig og begrensa informasjon. Begrensa informasjon vil bli levert frå Forsvarsdepartementet si plattform. Ugradert og skjermingsverdig ugradert vil bli levert frå den nye verksemda sin plattform. Den nye plattforma vil bli basert på sky-teknologi, i hovudsak som ei privat, lukka løysning. Ein såkalla to-nivåklient for sikker og effektiv behandling av gradert og ugradert informasjon er under utvikling.»

Slik disse medlemmer ser det, er dette en klargjøring av at målbildet er endret fra en strategi som utelukkende baserer seg på FDs tonivåløsning. Det kommer klart fram at FDs løsning skal brukes mot det graderte, og at det lages en ny, ugradert plattform (sikkerhetsgodkjent) basert på kommersielle leveranser, slik det kommer fram av sitatet av departementsråd Hermansen over.

Komiteen merker seg at vurderingen så sent som i 2023 tilsa at det tekniske målbildet kunne nås gjennom delvis gjenbruk av eksisterende plattformer. Komiteen forstår videre at denne vurderingen senere ble endret som følge av IKT-angrepet sommeren 2023, og at beslutningen ble omgjort til at man måtte etablere en helt ny plattform for å sikre en felles, sikker og effektiv infrastruktur basert på én plattform.

Komiteen forstår svarene som ble gitt i høringen, slik at denne plattformen skal være felles for de ulike løsningene, som så skal tilpasses ulike behov for sikkerhet og gradering for forskjellige departementer og virksomheter.

Komiteen merker seg digitaliserings- og forvaltningsminister Karianne O. Tungs overordnede beskrivelse av arbeidet med ny felles IKT-plattform i kontrollhøringen 12. mai 2025:

«Programmet har eksistert over flere år, men fram til 2021 var arbeidet preget av interne uenigheter og lite framgang. Etter 2021 har vi hatt stram styring, og det har blitt oppnådd to viktige milepæler i prosjektet. Det første er at vi har etablert en ny virksomhet som samler de tidligere IKT-miljøene. […] Vi jobber nå med å ferdigstille den andre delen, nemlig å etablere en ny, felles IKT-plattform.»

Informasjon til Stortinget

Komiteen forstår det dithen at det har vært et omforent mål på tvers av de politiske skillelinjer å legge til rette for en felles digital plattform til bruk for alle departementer.

Komiteen oppfatter det som avklart at arbeidet med å utvikle en ny, felles IKT-plattform for departementsfellesskapet endret mål underveis i prosessen.

Slik digitaliserings- og forvaltningsministeren beskriver det, skjedde dette på to stadier: Hhv. som følge av KS2-prosessen vinteren 2022 og etter det alvorlige dataangrepet sommeren 2023.

I brev fra digitaliserings- og forvaltningsministeren 1. april 2025 står det:

«I forprosjektet som forelå på dette tidspunktet, var det lagt til grunn at departementene skulle ta i bruk FDs IKT-plattform. Kvalitetssikringen som ble påbegynt under forrige regjering våren 2021 ble stoppet. Ekstern kvalitetssikrer mente at styringsdokumentene som forelå ikke tilfredsstilte kravene for KS2, og at det derfor ikke var grunnlag for videre kvalitetssikring. I stedet ble det planlagt et tidsløp med sikte på å ha utarbeidet et ferdig forprosjekt innen utgangen av 2021. Det var i forbindelse med sluttføringen av dette reviderte forprosjektet – vinteren 2021–2022 – at FD og daværende Kommunal- og distriktsdepartementet (KDD) la til grunn at departementenes framtidige IKT-plattform skulle basere seg på en privat lukket skyløsning levert fra en tredjepart. Utviklingen på IKT-området og kartlegginger av departementenes behov for digitale tjenester og applikasjoner, gjorde det nødvendig å se på alternativer til plattformer som ikke ville legge like store begrensninger på brukerne som FDs plattform ville gjøre. Vurderingene var at FDs plattform måtte ha et høyt sikkerhetsnivå og -løsninger, siden den også skulle behandle lavgradert (BEGRENSET) informasjon. Dette ville kreve at man måtte være meget restriktiv med

hvilke applikasjoner og tjenester som kunne legges på FDs plattform. Mesteparten av informasjonen som departementene håndterer, og applikasjonene de bruker for å behandle den, krever ikke et like høyt sikkerhetsnivå som FDs plattform har.»

Komiteen legger til grunn at regjeringen på dette stadiet, altså fra våren 2022 og frem til sommeren 2023, ikke lenger baserte seg på FDs tonivåløsning, men en kombinasjon hvor også DSS' løsninger skulle inngå.

Komiteens medlemmer fra Høyre, Fremskrittspartiet, Rødt og Venstre kan ikke se at Stortinget på noe tidspunkt ble tydelig informert om denne nye vurderingen, hvor DSS' plattform ble lagt til grunn som felles plattform.

Komiteen merker seg at digitaliserings- og forvaltningsministeren viser til informasjon i Prop. 18 S (2022–2023) fra Forsvarsdepartementet, hvor regjeringen beskriver arbeidet med den nye felles IKT-plattformen. Komiteen kan imidlertid ikke se at informasjonen som gis her, gjør det klart for Stortinget at arbeidet har endret karakter, og at premissene om å bygge på FDs tonivåløsning fra da arbeidet ble igangsatt, er blitt endret fra regjeringens side.

Komiteens medlemmer fra Høyre og Fremskrittspartiet finner det kritikkverdig at Stortinget ikke ble gjort uttrykkelig oppmerksom på at premissene for arbeidet var nye.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser til at målbildet for oppstart av programmet var å etablere en ny felles IKT-plattform gjennom anskaffelser i markedet. Videre ble Stortinget informert i Prop. 18 S (2022–2023), som er sitert ovenfor, om at plattformen skulle baseres på en privat lukket skyløsning. Utenriks- og forsvarskomiteen hadde under behandlingen av Prop. 18 S (2022–2023) ingen merknader.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet, Sosialistisk Venstreparti, Rødt og Venstre, mener det er for tidlig å konkludere med om regjeringens valg av privat skyløsning framfor bruk av egne systemer var godt nok utredet, og om informasjonen til Stortinget var tilstrekkelig. Flertallet viser til at Riksrevisjonen har varslet en undersøkelse av det ureglementerte merforbruket av privat konsulenthjelp knyttet til IKT-prosjektet. Flertallet mener dette er kjernen i saken, og antar at undersøkelsen også vil kunne gi innsikt i om prosess og beslutninger i forkant av de økonomiske overskridelsene har vært forsvarlige. Flertallet understreker at komiteens høring har belyst saken på en nyttig måte, men mener grunnlaget for å konkludere er for tynt før Riksrevisjonens undersøkelse er gjennomført.

Komiteen legger til grunn at det omfattende dataangrepet i juli 2023 fikk store følger også for vurderinger knyttet til ny felles IKT-plattform for departementsfellesskapet. Det vises til svar fra digitaliserings- og forvaltningsministeren 18. februar 2025:

«Programmets tekniske målbilde var å videreutvikle IKT-plattformen som ble driftet av DSS. Etter dataangrepet mot IKT-plattformen til DSS sommeren 2023, var ikke dette målbildet lenger mulig å gjennomføre. Programmet ble derfor nødt til å utrede en ny løsning som var gjenstand for ekstern kvalitetssikring sommeren 2024. Stortinget fastsatte høsten 2024 ny kostnadsramme på 2,24 mrd. kroner inkl. mva., jf. behandlingen av FDs Prop. 1. S (2024–2025). Endringen i kostnadsrammen skyldtes i hovedsak dataangrepet 2023.»

I høringen 12. mai 2025 uttalte tidligere kommunal- og distriktsminister Sigbjørn Gjelsvik:

«Planen var å informere Stortinget om desse endringane i målbildet hausten 2023. Så langt kom vi aldri, på grunn av angrepet mot IKT-plattforma Depnet/U sommaren 2023. I juli 2023 oppdaga vi at ein avansert og ressurssterk trusselaktør hadde kome seg inn på e-postserverar på Depnet/U via den dåverande løysinga for synkronisering av e-post til tilsette sine mobile einingar.»

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser til at tidligere kommunal- og distriktsminister Gjelsvik i fortsettelsen av ovenstående sitat sa følgende:

«Denne løysinga er ein kommersiell programvare som vert brukt av mange verksemder globalt. Sikkerheitshòlet trusselaktøren utnytta, var ei såkalla nulldagssårbarheit. Utan å gå inn på tekniske forhold betyr ei nulldagssårbarheit at ein trusselaktør har identifisert og utnytta eit svakt punkt før leverandøren er kjend med det. Sårbarheiter av denne typen er nærmast umogleg å beskytte seg mot. Sikkerheitshòlet som vart oppdaga av oss, og som ramma fleire andre verksemder i verda, vart raskt tetta av programvareleverandøren. Som følgje av at trusselaktøren hadde kome seg inn på e-postserverane på Depnet/U, vart serverane kompromitterte. Før eg gjer nærmare greie for handteringa og oppfølginga av dataangrepet, vil eg understreke at eg ved to anledningar sommaren 2023 informerte Stortinget om dette på eigna måte.»

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet vil tilføye at Stortinget ble informert på egnet vis sommeren 2023 og i Prop. 1 S (2023–2024) fra både FD og KDD.

Digitaliserings- og forvaltningsministeren uttalte i høringen følgende om dette:

«Det gjorde at man igjen endret målbildet: først fra FDs tonivåplattform til privat lukket sky, og deretter til å ha privat lukket sky, men også med gjenbruk av komponenter fra Depnet/U. Det skulle man jo informere Stortinget om i Prop. 1 S for 2022–2023, etter et eksternt kontrollpunkt, som også hadde gått gjennom ekstern kvalitetssikrer, men da kom dataangrepet, som gjorde at Depnet/Us plattform ble kompromittert.»

På spørsmål fra representanten Carl I. Hagen om hvem som tok beslutningene, om å endre løsninger, svarte tidligere statsråd Bjørn Arild Gram:

«Det er jo den enkelte statsråd som på sine områder er konstitusjonelt ansvarlig, men du forankrer ting i regjering. I denne saken er det to statsråder som har vært ansvarlige for saksfeltet. Det er forsvarsministeren hele veien, og det er kommunal- og distriktsministeren, senere digitaliserings- og forvaltningsministeren, etter at departementet ble delt.»

På spørsmål fra representanten Audun Lysbakken om hvem som tok beslutningene og hvilket beslutningsgrunnlag som lå til grunn, svarte tidligere kommunal- og distriktsminister Sigbjørn Gjelsvik:

«Før dataangrepet kom det ein rapport frå ekstern kvalitetssikrar, som skulle vere grunnlag for dei vurderingane som skulle gjerast vidare i programmet, med forankring i regjeringa. Når det gjeld vurderingane som vart gjorde etter dataangrepet, har eg vist til nokre av dei prosessane som vart sette i gang mens eg var statsråd.»

Komiteens medlemmer fra Høyre og Fremskrittspartiet kan ikke se at høringen brakte på det rene når, hvordan og av hvem beslutningen om bytte av plattformløsning ble fattet. Disse medlemmer fastslår imidlertid at både skriftlige svar fra digitaliserings- og forvaltningsministeren og høringen brakte på det rene at beslutningen er blitt fattet på regjeringsnivå.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser til tidligere forsvarsminister Gram for klargjøring av hvordan beslutning om bytte av plattformløsning ble fattet:

«Det er departementene som er konstitusjonelt ansvarlige, og statsrådene som tar beslutningene, men alle viktige beslutninger, milepæler og veivalg i programmet er forankret i regjering.»

Videre viser disse medlemmer til tidligere forsvarsminister Grams utdyping av hvem som hadde ansvar og tok beslutninger i prosjektet, på et spørsmål fra Carl I. Hagen om hvilken statsråd som la saken fram for regjeringen. Gram sa:

«I denne saken er det to statsråder som har vært ansvarlige for saksfeltet. Det er forsvarsministeren hele veien, og det er kommunal- og distrikts ministeren, senere digitaliserings- og forvaltningsministeren, etter at departementet ble delt.»

I brev til komiteen 1. april 2025 skriver statsråd Tung også:

«Før FD og KDD rakk å informere Stortinget om det endrede målbildet ved å delvis gjenbruke enkeltkomponenter fra Depnet/U, istedenfor å anskaffe en helt ny plattform, ble Depnet/U utsatt for et dataangrep. Dataangrepet skjedde sommeren 2023 ved at en avansert og ressurssterk trusselaktør utnyttet en såkalt nulldagssårbarhet i den gamle løsningen for synkronisering av e-post på mobile enheter.»

Komiteens medlemmer fra Høyre og Fremskrittspartiet kan ikke se at denne endringen tilsier at det ble mindre viktig å informere Stortinget om de nye vurderingene regjeringen hadde gjort seg. Disse medlemmer kan heller ikke se at en så vidt omfattende endring er blitt tydelig kommunisert til Stortinget. Disse medlemmer finner dette kritikkverdig.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet mener det er godtgjort at vurderinger som er gjort underveis i prosjektet, har blitt kommunisert til Stortinget, jf. Forsvarsdepartementets Prop. 1 S (2023–2024) s. 70–71:

«Stortinget har ved behandlingen av Innst. 110 S (2022–2023) til Prop. 18 S (2022–2023) vedtatt at FD og KDD kan iverksette Program for Felles IKT-tjenester med en kostnadsramme på 1 392 mill. 2023-kroner inkl. mva (1 141 mill. 2023- kroner eks. mva) for programmets Endringstrinn 1 og 2 (1. januar 2021–30. mars 2025). Programmet er planlagt ferdigstilt i slutten av 2025. I programmet er det blant annet lagt til grunn at DSS' plattform delvis skal kunne gjenbrukes. Som følge av dataangrepet mot DSS' plattform sommeren 2023 vil programmet også vurdere alternative handlingsalternativer som innebærer etablering av helt ny plattform og mulig forsering av etablering av plattformen til første halvår 2024. På grunn av dette kan det være aktuelt å replanlegge deler av programmet. Den foreslåtte rammen for 2024 er derfor noe usikker.»

Økonomi

Komiteen mener det er klarlagt at DSS ikke har hatt tilstrekkelig kontroll med bruken av konsulenter i arbeidet med ny IKT-plattform, og viser til svar fra digitaliserings- og forvaltningsministeren 18. februar 2025:

«Departementene ble 21. oktober 2024 varslet av DSS, om at samlet forbruk av rammeavtale for konsulentbruk på IKT-området hadde oversteget maksimal økonomisk ramme på 600 mill. kroner. For denne rammeavtalen mottok DSS statusrapporter fra leverandøren hver 6. måned. Som følge av høyt uttak på avtalen mellom rapporteringstidspunktene ble det ikke tidsnok oppdaget at avtalen ville bli oversteget i løpet av høsten 2024. DSS hadde på dette tidspunktet allerede satt i gang et arbeid for å få på plass en ny rammeavtale med forventet signering innen mars 2025. Arbeidet

med inngåelse av ny rammeavtale ble intensivert så langt det var praktisk mulig. Ny avtale ble signert av DIO 25. januar 2025. [...] Umiddelbart etter at DSS og departementene som brukte avtalen fikk kjennskap til overforbruk av avtalen, ble det iverksatt tiltak for å redusere bruken av avtalen til et absolutt minimum. Departementene og DSS så seg imidlertid nødt til å videreføre konsulentoppgaver som var helt nødvendig for å opprettholde driften og sikkerheten på IKT-plattformene til departementene. Det ble også vurdert som nødvendig å opprettholde et minimumsnivå av aktivitet i utviklingsprosjektene slik at disse ikke skulle stoppe opp.»

Komiteens medlemmer fra Høyre, Fremskrittspartiet, Rødt og Venstre mener det er tydelig at DSS ikke hadde oversikt og kontroll med bruken av konsulenter. Disse medlemmer mener det også er tydelig at endringen i programmet ikke førte til økt årvåkenhet og oppfølging av konsulentbruken. Disse medlemmer mener det også er tydelig at kontrollmekanismene i oppfølgingen ikke var tilstrekkelig gode.

Komiteens medlemmer fra Høyre og Fremskrittspartiet finner dette kritikkverdig.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser til digitaliserings- og forvaltningsministerens svar i høringen:

«Jeg tror det er viktig at vi her skiller mellom arbeidet med IKT-plattformen og det som er kjent som emagine-avtalen, som Lysbakken er inne på.

Emagine-avtalen er en felles rammeavtale for bruk av konsulenttjenester innenfor IKT-området, altså en rammeavtale for IKT-tjenester som alle departementene kan benytte seg av. Utenriksdepartementet, Justisdepartementet – mange departementer har benyttet seg av denne avtalen. Den hadde en maksimal ramme på 600 mill. kr., og i høst ble det oppdaget at grensen for denne rammeavtalen var nådd. Man hadde også samlet sett gått over 600 mill. kr.

Med en gang vi fikk kjennskap til den overskridelsen, reduserte vi bruken til et absolutt minimum, så langt vi fikk det til uten at det skulle gå ut over sikkerheten til de IKT-tjenestene vi skulle utføre. Man startet umiddelbart arbeidet med å lage en ny rammeavtale for å ha den ut på anbud. Konkurransen ble kunngjort i starten av november 2024, og vi fikk en ny kontrakt i slutten av januar 2025.

Det er uheldig at det skjedde, og vi har gjort en rekke tiltak etter at vi oppdaget at denne rammeavtalen ble overgått, for å unngå at det skjer igjen. For det første har vi overført ansvaret for rammeavtalen på IKT-konsulentformidling fra DSS til DIO, siden DIO ble opprettet fra 1. januar. Vi har stilt krav til bedre internkontroll for å oppdage, for at dette ikke skal skje, og for å følge opp. Tidligere i denne rammeavtalen hadde man rapportering fra leverandør hver sjette måned. Vi har stilt krav om at man skal ha månedlige rapporteringer, nettopp for å unngå at dette skjer igjen.»

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet, Sosialistisk Venstreparti, Rødt og Venstre, viser til at kontroll med konsulentbruken etter alt å dømme vil være et helt sentralt spørsmål i den undersøkelsen som Riksrevisjonen har varslet. Flertallet mener derfor det er naturlig å vente med å ta stilling til spørsmålet om kritikk og graden av eventuell kritikk til undersøkelsen foreligger.

Sikkerhet

Digitaliserings- og forvaltningsminister Karianne O. Tung begrunnet i høringen programmet for felles IKT-tjenester i departementsfellesskapet slik:

«Programmet skal sørge for å oppnå to overordnede ting, for det første en ny, sikker og moderne IKT-plattform for Statsministerens kontor, alle departementene, Norges utenriksstasjoner, Departementenes digitaliseringsorganisjon, DIO, og Departementenes sikkerhets- og serviceorganisasjon, DSS. For det andre skal man etablere en ny, felles organisasjon som samler IKT-kompetansen i departementene.»

Komiteen registrerer at det tross stor ressursbruk og forsinkelser ennå ikke er lyktes med å få på plass en ny, felles IKT-plattform for departementsfellesskapet. Komiteen registrerer videre at det per 2025 ikke er en felles organisasjon for arbeidet med IKT-plattform, men to nye etater, nemlig Statens graderte plattformtjenester underlagt Forsvarsdepartementet og Departementenes digitaliseringsorganisasjon (DIO) underlagt Digitaliserings- og forvaltningsdepartementet.

I brev fra digitaliserings- og forvaltningsministeren 1. april 2025 skriver statsråden følgende om endringen bort fra FDs tonivåplattform:

«FD og DFD vurderte at det ikke var behov for å gjennomføre en egen sikkerhetsvurdering av Depnet/U, som følge av endret målbilde til å gjenbruke enkeltkomponenter fra denne plattformen. Dette fordi vi hadde et godt nok informasjonsgrunnlag om Depnet/U. Nasjonal sikkerhetsmyndighet (NSM) gjennomførte en penetrasjonstest1 av Depnet/U i 2022. Penetrasjonstesten ga gode tilbakemeldinger, og på bakgrunn av dette vurderte FD og DFD at det ikke var behov for en ny sikkerhetsvurdering av Depnet/U.»

I høringen uttalte tidligere statsråd Bjørn Arild Gram:

«La meg si noen ord om sikkerhetsvurderingene som ble foretatt i denne perioden. Nasjonal sikkerhetsmyndighet gjennomførte i 2022 en inntrengningstest av Depnet/U. Dette var en test av sikkerheten og sårbarheten til datasystemet gjennom planlagte og forhåndsbestilte angrep. Testen ga gode tilbakemeldinger på sikkerhetstilstanden til Depnet/U. Den bekreftet at det var mulig og sikkert å gjenbruke komponenter fra plattformen i den nye felles IKT-plattformen. Mot slutten av 2022 startet vi også et nødvendig oppgraderingsarbeid på komponenter i Depnet/U. Oppgraderingsarbeidet på Depnet/U, som startet opp i slutten av 2022, økte sik-

kerhetsnivået ytterligere og sørget for økt levetid på komponentene som ble vurdert å gjenbruke. Som følge av dette var det ikke behov for å gjennomføre en ny sikkerhetsvurdering av Depnet/U våren 2023. Det var uansett en forutsetning at ny felles IKT-plattform skulle godkjennes av Nasjonal sikkerhetsmyndighet. En annen viktig forutsetning for sikkerheten var at informasjon som er gradert i henhold til sikkerhetsloven, skulle lagres og behandles gjennom Forsvarsdepartementets IKT-plattformer. På grunn av dataangrepet mot Depnet/U sommeren 2023 måtte vi replanlegge målbildet for ny felles IKT-plattform. Vi gjennomførte sikkerhetsvurderinger av Depnet/U og vurderinger av handlingsalternativer på kort sikt. Tidligere kommunal- og distriktsminister vil redegjøre nærmere for håndtering og oppfølging av selve dataangrepet. Sikkerhetsvurderingene som ble gjennomført av tilstanden til Depnet/U etter dataangrepet, resulterte i at vi ikke lenger hadde tillit til komponentene som var tenkt gjenbrukt i ny felles IKT-plattform.»

Tidligere kommunalminister Sigbjørn Gjelsvik bekrefter det samme bildet og sa i høringen følgende:

«Våren 2023 gjennomførte vi det fyrste kontrollpunktet av programmet med ekstern kvalitetssikring. Målbildet som då vart kvalitetssikra, var ein ny felles IKT-plattform med gjenbruk av enkelte komponentar frå plattforma Depnet/U. Som Gram var inne på i sitt innlegg, vurderte både departementa og ekstern kvalitetssikrar våren 2023 at ei ny felles IKT-plattform med gjenbruk av nokre komponentar frå Depnet/U ville vere ein farbar veg, med tanke på både sikkerheit og økonomi.»

Representanten Frode Jacobsen stilte spørsmål ved hvilke sikkerhetsvurderinger som ble gjort da man gikk bort fra FDs tonivåløsning, og spurte bl.a. om følgende:

«Ved å gå bort fra FD II la man ikke sikkerheten bort, men ut fra hva Hermansen sa tidligere, var det ikke like hensiktsmessig å legge seg på samme sikkerhetsnivå på hele linja her som man ville gjort på FD II. Var det en vurdering man også fikk faglig støtte til fra NSM?»

Tidligere statsråd Bjørn Arild Gram svarte:

«Det var definitivt faglig anbefalt. I hvor stor grad NSM var inne i vurderingene da, klarer ikke jeg å svare på, men det var forutsatt at NSM skulle godkjenne løsningen til slutt. NSM skulle ha en rolle med tanke på løsningen vi skulle ende med. Det var en prosess – husk at vi gikk inn i et forprosjekt som så skulle kvalitetssikres. Det er mange steg her, og vi var fortsatt ikke der at beslutningen skulle tas. Det ble fremmet for Stortinget et år etterpå, etter at prosessen var tatt videre. Det har skjedd ting etter det igjen, som har gjort at vi har måttet planlagt på nytt.»

Komiteens medlemmer fra Høyre og Fremskrittspartiet finner at de praktiske følgene av dataangrepet sommeren 2023 viser at sikkerhetsvurderingene ikke har vært tilstrekkelig gjennomtenkte og holdbare i møte med virkeligheten. Disse medlemmer mener dette tyder på svake – og i ettertid feilaktige – vurderinger da regjeringen i forbindelse med KS2-prosessen valgte å endre målbildet for arbeidet. Disse medlemmer mener dette både har forsinket arbeidet og gitt økte kostnader, samt ikke gitt departementsfellesskapet en ny og tilstrekkelig sikker løsning.

Disse medlemmer finner dette kritikkverdig.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet vil understreke at komiteen har liten innsikt i hvilke bakenforliggende sikkerhetsvurderinger som er gjort, all den tid komiteen ikke ønsket en lukket høring hvor disse kunne blitt utdypet.

For øvrig viser disse medlemmer til at tidligere statsråd Gram og statsråd Tung har redegjort for de sikkerhetsmessige vurderingene. Disse medlemmer mener den samlede vurderingen av sikkerhet, inkludert forutsetningen om godkjenning av NSM, er og har vært tilstrekkelig.

Disse medlemmer vil også vise til at angrepet sommeren 2023 var, slik tidligere kommunalminister Gjelsvik forklarte i høringen, et angrep fra en avansert og ressurssterk aktør som utnyttet en såkalt nulldagssårbarhet, som er så godt som umulig å beskytte seg mot. Angrepet rammet for øvrig flere land, sikkerhetshullet ble oppdaget av DSS, og leverandøren fikk tettet hullet på bakgrunn av den informasjonen som ble gitt av DSS.

Videre mener disse medlemmer at det fra alle hold har blitt påpekt at det var nødvendig å gå bort fra prinsippvedtaket som ble gjort av den daværende regjeringen Solberg om å bygge på FDs totrinnsmodell, og ikke minst ble dette stoppet av en ekstern kvalitetssikrer som regjeringen Solberg selv bestilte. Målet om å etablere en ny IKT-virksomhet og legge til rette for en felles digital plattform som skal tas i bruk av alle departementene og være innrettet mot å ivareta digital sikkerhet, vil sikre oss et framtidig moderne og effektivt IKT-system.

Videre viser disse medlemmer til at det kom fram i høringen, som svar på spørsmål fra representanten Kirsti Leirtrø, at saken handler om mer enn regjeringens saksbehandlingssystem. Representanten Leirtrø spurte om sammenhengen mellom langtidsplanen for forsvarssektoren og digitaliseringsstrategien. Digitaliserings- og forvaltningsminister Tung svarte følgende:

«Vi har jo satt som ambisjon at Norge skal bli det mest digitaliserte landet innen 2030, og den ambisjonen skal også gjelde offentlig forvaltning. Jeg synes forhistorien her – med fire IKT-miljøer hvor UD og utenriksstasjonene har sitt eget, Justisdepartementet har sitt eget, DSS har hatt sitt eget og FD og SMK har hatt sitt eget – egentlig eksemplifiserer hvor viktig det er å arbeide med å sørge for moderne digitale verktøy, sånn at man også får en moderne og digital forvaltning. Det er nettopp denne organiseringen som egentlig har hindret at man kan jobbe effektivt nok i årene som har vært, og

som beskriver hvor viktig det er å få på plass denne plattformen, for at vi skal kunne nyttiggjøre oss nye teknologier, som KI, automatisering og maskinlæring, også i årene framover. Det er det ene punktet om hvorfor det er viktig med den felles IKT-plattformen, og så handler det – som forsvarsministeren er inne på – om sikkerhet. Vi lever i en verden der de digitale truslene øker for hver dag. Digital svindel er nå større på verdensmarkedet enn narkotikahandel. Det viser hvor viktig det er hele tiden å jobbe med sikkerhet i systemene. Å gå fra fire IKT-miljøer, hvor vi er sårbare og ineffektive, til ett felles IKT-miljø vil bidra til å øke sikkerheten i departementsfellesskapet og er en viktig milepæl for oss. Sikkerhet og modernisering av forvaltningen er viktige stikkord i arbeidet med felles IKT-plattform.»

Disse medlemmer mener statsråd Tungs svar også belyser et annet viktig poeng: at offentlig forvaltning får et sterkere og mer kompetent digitaliseringsmiljø, noe disse medlemmer mener er viktig i møte med en verden i rivende teknologisk utvikling.

Disse medlemmer vil også vise til representanten Jacobsen, som i høringen viste til at det har vært flere IKT-prosjekter i offentlig forvaltning som har vært utsatt for kritikk av kontroll- og konstitusjonskomiteen gjennom tidene. Disse medlemmer mener svaret til forsvarsminister Sandvik belyser et vesentlig poeng i arbeidet med ny IKT-plattform: at det hele tiden har vært jaktet på løsninger som skal sikre at man ikke har en utdatert modell i det den er ferdig, men tvert imot en modell som holder tritt med teknologiutviklingen:

«Jeg tenkte jeg ville legge til noe. Det kan jo godt tenkes man kommer tilbake hit, men nettopp disse kontrollfunksjonene er viktige. Det er derfor man har laget statens prosjektmodell, og det er derfor man har hatt denne grundige gjennomgangen – at man har både KS2, man har flere kontrollpunkter, og man har en fleksibel måte å gjøre det på for å kunne tilpasse seg virkeligheten, så man ikke ender opp med et utdatert system den dagen man innfører det. For her er det et teknologikappløp, der det også er kommersielle selskaper som er i lead på teknologiutviklingen, samtidig som vi må sikre at vi har nasjonal kunnskap og kunnskap internt i forvaltningen for å kunne skjerme ting som ikke vil passe seg å ha ut i rene kommersielle løsninger. Jeg synes nettopp denne kontrollfunksjonen understrekes av at det er viktig å ha denne utviklingen framover, og jeg synes statsråd Tung også har redegjort veldig godt for at dette følges veldig godt opp.»

Komiteens medlemmer fra Høyre og Fremskrittspartiet registrerer for det første at statsrådene ved flere anledninger trekker frem at angrepet skjedde i regi av en avansert og ressurssterk aktør. Med tanke på at dette er datasystemet til Norges regjering, og at vi er i en svært spent sikkerhetspolitisk situasjon, måtte det være å forvente at avanserte og ressurssterke aktører ville søke å utnytte enhver sårbarhet.

Disse medlemmer viser videre til at regjeringen før datainnbruddet fikk en helt konkret advarsel fra ekstern kvalitetssikrer om risikoen knyttet til gjenbruk av eksisterende ugradert nettverk. Høringen har ikke avdekket at statsrådene i regjeringen Støre foretok seg noe basert på denne advarselen, og at det snarere virker som statsrådene fortsatt – og tross de store negative konsekvensene av innbruddet – er tilfredse med valgene som ble tatt. Det vises til supplerende analyse fra A-2 Norge AS 26. april 2023, hvor tilråding 4 på side 18 lyder:

«Sikre kontroll over om infrastruktur som er benyttet for lagring og behandling av ikke-skjermingsverdige data oppgraderes til å bli benyttet for løsninger med et høyere sikkerhetsnivå.»

Disse medlemmer viser også til at det i høringen og oversendte dokumenter klart fremkommer at det er nivåforskjell på sikkerheten i FDs tonivåplattform og den løsningen regjeringen Støre valgte. Høringen har ikke avdekket at statsrådene foretok seg noe for å utfordre sikkerhetsnivået i den valgte løsningen, selv om det understrekes at prosjektet styres svært tett fra politisk ledelse.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet mener målet for etableringen av plattformen er å ha et fornuftig sikkerhetsnivå tilpasset verdiene som skal beskyttes. Målet er ikke å ha høyest mulig sikkerhetsnivå. FDs tonivåplattform har et sikkerhetsnivå som ville satt store begrensninger for effektiviteten og samhandlingen til departementene. Det høye sikkerhetsnivået skyldes sammenkoblingen mot lavgradert, et hensyn man ikke trenger å ta med seg i utviklingen av en plattform for behandling av ugradert skjermingsverdig og ugradert informasjon. Høyres og Fremskrittspartiets merknad om at statsrådene ikke utfordret sikkerhetsnivået i den valgte løsningen, bygger på en feil vurdering om at sikkerhetsnivået på FDs tonivåplattform var det riktige nivået for behandling av ugradert skjermingsverdig og ugradert informasjon hos departementene. Det kom tydelig fram i høringen at det valgte tekniske målbildet innebærer at FDs plattform vil bli benyttet for informasjon som er gradert begrenset. Sikkerhetskravene for skjermingsverdig ugradert informasjon vil settes slik at plattformen kan godkjennes av NSM. Disse medlemmer viser til at Hermansen sa følgende under høringen:

«Da så vi at skal vi lage en plattform som møter de målsettingene – altså både sikker, effektiv og kostnadsforsvarlig drift – kunne ikke det bygges på FDs opprinnelige tonivåplattform. Derfor gikk man til Stortinget med endringsproposisjonen i 2022 og anbefalte at man brukte FDs plattform mot det graderte, men lagde en ny, ugradert plattform som skulle sikkerhetsgodkjennes, basert på en kommersiell leveranse fra leverandører. Så det er årsaken til at man gikk vekk fra det opprinnelige.»

Disse medlemmer viser videre til at Gram uttalte følgende under høringen:

«Her var det mulig å få sikre skyløsninger på norsk jord, med norske krav og norsk sikkerhet, sikkerhetskrav som vi selv stilte, sikkerhetsklareringer og så videre, som gjorde at du fikk de rette. Du fikk sikre løsninger og samtidig fleksible og hensiktsmessige løsninger som gjorde at departementene fikk dekket behovene sine. Det graderte skulle fortsatt leveres av Forsvarets plattformer.»

Videre viser disse medlemmer til følgende sitat fra Pettersen fra høringen:

«Som Hermansen var innom, er dette et marked som har vært i utvikling. Og det vi har sett, er at de store selskapene på skyteknologi og datasenter tilpasser løsninger mer og mer til nasjonale sikkerhetskrav. Det vi gjør i Norge, i vårt program, er likt tilsvarende vurderinger som gjøres i andre land. Vi har ulike kjøremiljøer basert på en verdivurdering av informasjonen. Det sikreste kjøremiljøet som gjelder ugradert, er en skjermingsverdig ugradert plattform, slik vi legger opp til. Den skal sikkerhetsgodkjennes, sammen med hele plattformen, av Nasjonal sikkerhetsmyndighet, men hvor vi bruker markedet som har oppdatert informasjon, stordriftsfordeler og erfaring med drift i en helt annen størrelsesorden enn det vi kunne klare å levere.»

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet, Sosialistisk Venstreparti, Rødt og Venstre, viser til sine tidligere merknader og vil avvente Riksrevisjonens undersøkelse før konklusjoner i saken trekkes.

Komiteens tilråding

Komiteen har for øvrig ingen merknader, viser til saken og rår Stortinget til å gjøre følgende

vedtak:

Innst. 488 S (2024–2025) – Innstilling fra kontroll- og konstitusjonskomiteen om sak om Program for felles IKT-tjenester i departementsfellesskapet – vedlegges protokollen.

Oslo, i kontroll- og konstitusjonskomiteen, den 27. mai 2025

Peter Frølich

leder og ordfører

VEDLEGG 1

Referat
fra åpen høring i kontroll- og konstitusjonskomiteen

Program for felles IKT-tjenester i departementsfellesskapet

Høring 12. mai 2025 kl. 09:00

Åpen høring i kontroll- og konstitusjonskomiteen mandag den 12. mai 2025 kl. 9

Møteleder: Peter Frølich (H) (komiteens leder)

Sak:

Program for felles IKT-tjenester i departementsfellesskapet

Møtelederen: Da er klokken 9, og vi kan lukke dørene. Jeg ønsker velkommen til denne kontrollhøringen i regi av kontroll- og konstitusjonskomiteen. Høringen vil handle om initiativsaken som er opprettet i kontrollkomiteen om felles IKT-tjenester i departementsfellesskapet.

Kontrollkomiteen startet undersøkelser i saken 11. februar 2025. Bakgrunnen var da oppslag i Aftenposten 3. og 5. februar om programmet for felles IKT-løsning for departementsfellesskapet. I komiteens møte 8. april 2025 ble det besluttet å åpne en såkalt initiativsak og avholde en kontrollhøring som ledd i behandlingen av den.

Komiteen har besluttet at høringen skal omhandle, men ikke begrense seg til følgende problemstillinger:

- Hvordan ble hensyn til sikkerhet vektlagt i forbindelse med byttet av plattform for felles IKT-løsninger i 2023?
- Har programmet for felles IKT-løsninger for departementsfellesskapet vært forsvarlig styrt i forbindelse med endringen av målbildet?
- Hvordan er utsiktene til at prosjektet etter endringene kan realiseres i tide, innenfor fastsatt økonomisk ramme?

Følgende personer møter til høring i dag:

- digitaliserings- og forvaltningsminister Karianne Oldernes Tung
- forsvarsminister Tore O. Sandvik
- tidligere kommunal- og distriktsminister og tidligere forsvarsminister Bjørn Arild Gram
- tidligere kommunal- og distriktsminister Sigbjørn Gjelsvik
- direktør for Departementenes sikkerhets- og serviceorganisasjon Torgeir Swensson Strøm
- direktør for Departementenes digitaliseringsorganisasjon Anders Aagaard Sørby

De prosedyrene som er fastsatt i reglementet for kontrollhøringer, vil bli fulgt. Jeg minner for ordens skyld om at dette er en åpen høring, og at komiteen kun kan motta taushetsbelagte opplysninger for lukkede dører. Dersom et av komiteens spørsmål ikke kan besvares uten å røpe opplysninger som er underlagt taushetsplikt, skal den inviterte gjøre komiteen oppmerksom på det. Under høringen må også komiteens medlemmer huske på å ikke gjengi eller vise til opplysninger som er underlagt lov- eller instruksfestet taushetsplikt.

Det er opplyst om at det i løpet av dagen kan bli nødvendig å avholde en egen, lukket kontrollhøring i etterkant av denne åpne høringen. Dersom det skal gjøres, vil den selvfølgelig bli holdt i et gradert møterom her på Stortinget, og oppstart blir i så fall kl. 15. Komiteen vil i løpet av høringen ta stilling til om det er behov for en lukket høring eller ikke, og selvfølgelig gi beskjed til de inviterte så fort det lar seg gjøre.

Jeg minner også om at det blir tatt referat fra høringen, og det vil følge som vedlegg til komiteens innstilling i saken. Det er også viktig for referentene at alle inviterte husker å bruke mikrofonen og skru den av og på til riktig tid.

Høring med direktør Departementenes sikkerhets- og serviceorganisasjon Torgeir Swensson Strøm og direktør Departementenes digitaliseringsorganisasjon Anders Aagaard Sørby

Møtelederen: Da er vi klare til å starte med den første bolken, og jeg ønsker velkommen til direktør for Departementenes sikkerhets- og serviceorganisasjon Torgeir Swensson Strøm. Du har med deg en bisitter, assisterende direktør Thomas Bettum. Velkommen til deg også.

Jeg vil også ønske velkommen til direktør for Departementenes digitaliseringsorganisasjon Anders Aagaard Sørby. Du har med deg en bisitter, avdelingsdirektør for virksomhetsutvikling Unni Anette Johnsrud. Velkommen.

Hver av dere får først inntil 10 minutter til en innledning. Etter innledningene starter komiteens utspørring. Da er det først saksordfører, som er meg i dette tilfellet, som får 10 minutter til spørsmål. Deretter får alle partigruppene som er representert, inntil 5 minutter til sine spørsmål. Så blir det en åpen runde fra komiteen til oppklarende spørsmål, og til slutt får dere muligheten til noen avsluttende bemerkninger hvis dere ønsker det.

Så er det sånn i utspørringen at det kan oppleves slik at komitémedlemmene kanskje er litt pågående eller avbryter eller noe sånt. Det er ikke for å være uhøflige, men det er i så fall for å komme til bunns i kjernen av de spørsmålene som komiteen ønsker svar på, innenfor den begrensede tiden vi har.

Da gir vi først ordet til direktør for Departementenes sikkerhets- og serviceorganisasjon, DSS, Torgeir Swensson Strøm. Du har 10 minutter til din innledning. Vær så god.

Torgeir Swensson Strøm: Takk for det, komitéleder.

Programmet for felles IKT-tjenester har vært og er en viktig aktivitet i departementsfellesskapet. Å etablere en ny digital plattform med digitale løsninger som legger til rette for økt sikkerhet og økt samhandling mellom departementene, er avgjørende for at departementene skal kunne ivareta sine kjerneoppgaver og grunnleggende funksjoner.

Jeg vil takke kontroll- og konstitusjonskomiteen for at jeg får komme hit i dag og bidra til å svare på de tre problemstillingene knyttet til sikkerhetshensyn ved beslutning om bytte av plattform i 2023, styringen av programmet og de videre utsiktene i programmet.

Samfunnsmålet for program felles IKT-tjenester er at Statsministerens kontor, alle departementene, Norges utenriksstasjoner og DSS skal ha en sikker, kostnadseffektiv og funksjonell behandling og deling av digital informasjon internt og eksternt. De tre effektmålene er:

- Informasjonssikkerheten er styrket og i henhold til regelverket.
- IKT-tjenestene i departementsfellesskapet er effektive, brukervennlige og imøtekommer brukernes behov.
- Drift og forvaltning av IKT-tjenester har høy effektivitet og er i samsvar med beste praksis.

Målene vil også omfatte Departementenes digitaliseringsorganisasjon, DIO, nå som DIO er etablert.

Når jeg i dagens høring bruker begrepet «endret målbilde», er det knyttet til endringer i det tekniske målbildet som dreier seg om design og valg av plattformløsning som best støtter opp under samfunnsmålet og effektmålene for programmet.

Jeg har vært direktør for Departementenes sikkerhets- og serviceorganisasjon, DSS, siden 1. november 2023. DSS' hovedoppgave er å levere sikre og effektive fellestjenester til departementene, Statsministerens kontor og DIO. Tjenestene skal leveres med riktig kvalitet og til riktig tid. DSS organiserer et bredt og velfungerende tjenestetilbud og skal gi råd til Digitaliserings- og forvaltningsdepartementet om utviklingen av tjenestene. DSS og DIO samarbeider nå tett om tjenesteleveranser til departementsfellesskapet hver dag.

Tjenesteleveransene til DSS er delt opp i fire hovedområder: vakt-, resepsjons-, og sikkerhetstjenester, HR-tjenester, fasilitetstjenester og anskaffelses- og oversettelsestjenester. Tjenesteleveransene reguleres gjennom tjenestebeskrivelser.

Da jeg tiltrådte som direktør for DSS 1. november 2023, og fram til 31. desember 2024, lå ansvaret for drift og forvaltning av dagens felles IKT-plattform, heretter kalt Depnet/U, i DSS. Depnet/U ble benyttet av samtlige departementer med unntak av Utenriksdepartementet, Justis- og beredskapsdepartementet og Forsvarsdepartementet. Statsministerens kontor benytter også Forsvarsdepartementets plattform. I tillegg til drift og forvaltning av Depnet/U leverte DSS et bredt spekter av digitale informasjons- og samhandlingstjenester som understøttet departementenes arbeidsprosesser.

Sentrale prioriteringer innenfor de digitale tjenestene etter at jeg tiltrådte, har bl.a. vært å følge opp etterarbeidet etter dataangrepet sommeren 2023 og DSS' bidrag i program for felles IKT-tjenester. Som en del av dette har omstillingsprosessen knyttet til opprettelsen av og overføringen av ansatte til DIO stått sentralt. Ansvaret for DSS' digitale tjenester ble overført til DIO 1. januar 2025.

Som direktør i DSS har jeg vært en del av programstyret i programmet for felles IKT-tjenester. Programstyret er et rådgivende organ for programeierne – Digitaliserings- og forvaltningsdepartementet og Forsvarsdepartementet – som eier og styrer programmet i fellesskap.

Programstyret består av representanter på toppledernivå i embetsverket. Programstyret ledes av Forsvarsdepartementet og Digitaliserings- og forvaltningsdepartementet som programeiere, og er ellers representert med deltakelse fra Utenriksdepartementet, Justis- og beredskapsdepartementet, Statsministerens kontor, DSS og DIO.

Styret møtes en gang i måneden og har ekstraordinære møter som ved behov initieres av enten programmet eller programeierne. Programstyrets rolle er å gi råd om viktige strategiske valg og programmets prosesser og å identifisere risikoer og tiltak i programmet. Det er programeierne som tar de endelige beslutningene innenfor rammen av de avklaringer som skjer i regjeringen, og de fullmakter som er gitt av Stortinget.

Min rolle i programstyret har særlig vært å bygge på DSS' erfaring og kompetanse med drift og forvaltning av IKT-løsninger for departementene og tydeliggjøre DSS' vurderinger knyttet til programmets strategier og veivalg, sett fra mitt ståsted. Jeg har arbeidet for å styrke samhandlingen mellom DSS, DIO og programmet på relevante områder, slik at de ulike aktørene skulle trekke i samme retning.

Et viktig ansvar har vært å legge til rette for konsolideringen av IKT-virksomhetene, og særlig å sikre en vellykket overføring av DSS' digitale tjenester til DIO. Denne overføringen var en viktig milepæl som la grunnlaget for å samle departementenes IKT-ressurser under én felles virksomhet. Å samle de digitale ressursene i ett miljø er sentralt for å forenkle driften, styrke sikkerheten og legge til rette for modernisering av de digitale tjenestene framover på én felles plattform.

Kontroll- og konstitusjonskomiteen ønsker å få belyst tre hovedspørsmål i denne høringen.

Spørsmålet om hvordan hensyn til sikkerhet ble vektlagt ved beslutningen om bytte av plattform i 2023,

tolker jeg til å gjelde endringen av det tekniske målbildet for ny, felles plattform som ble besluttet etter dataangrepet i 2023. Beslutningen ligger til programeierne, men gjennom deltakelsen i programstyret er jeg kjent med at hensynet til sikkerhet var en avgjørende faktor.

Når det gjelder spørsmålet om hvorvidt programmet har vært forsvarlig styrt i forbindelse med endringen av målbildet, er min vurdering at programmet har vært styrt på en god måte. Programmet er underlagt statens prosjektmodell og følger anerkjent programmetodikk. Programmet er også blitt fulgt opp gjennom flere eksterne kvalitetssikringer som omfatter både KS2 og såkalte kontrollpunkter.

Det er etablert en egen styringsstruktur for programmet. Beslutninger om endringer i målbildet er blitt tatt av eierne, Forsvarsdepartementet og det tidligere Kommunal- og distriktsdepartementet, nå Digitaliserings- og forvaltningsdepartementet, etter forutgående behandling i programstyret.

Til spørsmålet om hvorvidt prosjektet kan realiseres i tide og innenfor fastsatt økonomisk ramme, viser jeg til at programmet har lagt opp til trinnvis gjennomføring fram til 2027, med kontraktsigneringer i 2025, testing av løsningen høsten 2025, og overgang til ny plattform i 2026–2027.

Det foreligger et tett styrings- og kontrollregime som skal bidra til at programmet leverer i tråd med rammen som nå er satt. Etter min vurdering er det god styring på programmet, og det gjøres fortløpende vurderinger av og rapporteres på risikoer og usikkerhet som kan være knyttet til framdriften eller måloppnåelsen i programmet.

Med dette avslutter jeg min innledning og stiller meg til disposisjon for å svare på komiteens spørsmål.

Møtelederen: Tusen takk skal du ha.

Spørsmålene kommer ganske snart, men først gir jeg ordet til direktøren for Departementenes digitaliseringsorganisasjon, Anders Aagaard Sørby, som også har 10 minutter til sin innledning. Vær så god.

Anders Aagaard Sørby: Takk for det, komitéleder.

Takk for invitasjonen til denne høringen om program for felles IKT-tjenester i departementsfelleskapet.

Jeg ble utnevnt til direktør i departementenes nye digitaliseringsorganisasjon, med kortnavn DIO, av Kongen i statsråd 15. desember 2023. Den 1. januar 2025 ble DIO operativt som ordinært forvaltningsorgan underlagt Digitaliserings- og forvaltningsdepartementet.

DIO har ansvar for å levere sikre og effektive digitale fellestjenester med riktig kvalitet til Statsministerens kontor, alle departementene, Norges utenriksstasjoner, Departementenes sikkerhets- og serviceorganisasjon og 22. juli-senteret. Gitt min korte periode som direktør for DIO må jeg ta forbehold om at jeg ikke har informasjon om alle detaljer og historikk knyttet til program for felles IKT.

Jeg tiltrådte stillingen 1. mars 2024 og var da midlertidig ansatt i Digitaliserings- og forvaltningsdepartementet, som hadde det formelle ansvaret for DIOs etablering. Gjennom 2024 jobbet vi med å etablere DIO som organisasjon. Mitt hovedansvar var å sørge for at DIO ble bemannet med rett kompetanse fra de avgivende virksomhetene, som var DSS, Justis- og beredskapsdepartementet og Utenriksdepartementet. I dette arbeidet samarbeidet jeg tett med direktør i DSS og de tre IKT-lederne i avgivende virksomheter. Jeg fikk støtte i arbeidet fra prosjektet for organisering og ansvar i programmet for felles IKT, som bisto departementet i etableringen av DIO. Fra mars 2024 deltok jeg også som observatør i programmets styremøter for å få god innsikt i status, styrets anbefalinger og eierdepartementenes beslutninger.

DIO ble operativ i henhold til plan fra 1. januar 2025 og overtok da leveranseansvaret for departementenes ugraderte digitale fellestjenester. Jeg har nå ledet DIO i litt over fire måneder. Inntil en ny og felles digital plattform er etablert, vil vi videreføre sikker og stabil drift av dagens tre plattformer med samme kvalitet som tidligere.

På samme tidspunkt som DIO ble operativt, kom en ny etat på plass under Forsvarsdepartementet. Statens graderte plattformtjenester overtok ansvaret for digitale tjenester på gradert nivå. Det er dermed to IKT-leverandører i departementsfellesskapet som må samarbeide tett framover.

Formålet med opprettelsen av DIO er å styrke sikkerheten i departementenes digitale løsninger og forbedre departementenes evne til samordning og samarbeid. Den ustabile verdenssituasjonen, det digitale trusselbildet og kravene i den nye sikkerhetsloven gjør at departementene bør bli enda bedre rustet til å håndtere dataangrep og kriser. Den nasjonale sikkerhetsstrategien som regjeringen la frem den 8. mai, peker i samme retning.

Samtidig står departementsfellesskapet overfor stadig mer komplekse og sektorovergripende samfunnsutfordringer. Dette krever at departementene tenker nytt rundt hvordan de samhandler og deler data på tvers. Den nasjonale digitaliseringsstrategien Fremtidens digitale Norge peker på digitalisering som et strategisk virkemiddel for å løse dette.

I 2023 ble det gjennomført en omfattende behovskartlegging for hele departmentsfellesskapet. Den peker på flere digitale utfordringer i de ansattes arbeidshverdag. La meg kort oppsummere:

– Departementene jobber på fire ulike digitale plattformer med forskjellige fagsystemer og samhand-

lingsløsninger. For departementsansatte medfører dette mye tid og ressurser på tungvinn og manuell oppgaveløsning. Dette hemmer også samhandlingen på tvers av departementene, og med underliggende etater og andre aktører.
- Fra et driftsperspektiv er ulike plattformer økonomisk og ressursmessig svært krevende å videreutvikle, drifte og forvalte.
- Flere plattformer innebærer også flere mulige angrepsflater for trusselaktørene.

For å møte digitaliseringsstrategiens mål om et taktskifte i offentlig sektor må departementene ha én felles, sikker, effektiv og fremtidsrettet infrastruktur. Denne må legge til rette for å ta i bruk mer moderne teknologi som gjør det enklere å jobbe smartere og samhandle sømløst.

Etableringen av DIO er et viktig organisatorisk grep for å lykkes med digitalisering i departementsfellesskapet. Ved å samle ressurser og kompetanse i robuste fagmiljøer kan vi holde tritt med den teknologiske utviklingen og levere mer kostnadseffektive, helhetlige løsninger av høy kvalitet for fellesskapet. Et mer samlet ansvar for departementenes digitale tjenester øker også evnen til koordinering og samvirke i beredskaps- og krisesituasjoner.

Gjennom DIO er det etablert felles prioritering, styring og ledelse av departementenes digitale tjenester. Med dette utløses en større kraft til å lykkes med helhetlig og strategisk digitalisering.

Komiteen ønsker svar på tre hovedspørsmål i denne høringen. Komiteens første spørsmål omhandler vurderinger og beslutninger som ble foretatt før min tiltredelse. Jeg kan dermed ikke bidra med ytterligere informasjon utover direktør Strøms tidligere redegjørelse.

Jeg ønsker imidlertid å dele mine vurderinger knyttet til de to neste spørsmålene: Til spørsmålet om programmet har vært forsvarlig styrt i forbindelse med endringen av målbildet, viser jeg til innlegget til direktør i DSS og stiller meg bak hans vurderinger av at programmet har en hensiktsmessig styring. Programmet følger anbefalt metodikk for styring av store statlige programmer, med tydelig avklart myndighet og ansvar mellom programleder, programstyret og programmets eiere.

Programmet er delt opp i tre endringstrinn. Det gjennomføres kontrollpunkter med ekstern kvalitetssikring for å få en kritisk, uavhengig gjennomgang av planer og mål før neste endringstrinn kan starte opp.

Utviklingsarbeidet innen hvert endringstrinn gjennomføres med en smidig tilnærming. Dette innebærer at arbeidet deles opp i korte iterative faser, med trinnvise leveranser. Hver fase avsluttes med en intern kvalitetssikring og vurdering av eventuelle justeringer. Dette gir etter min mening økt fleksibilitet til å tilpasse programmet ved endringer i behov.

Programstyret er sammensatt av representanter fra de sentrale interessentene for programmets leveranser. Jeg har selv deltatt i programstyret, først som observatør i 2024 og senere som ordinært programstyremedlem fra 1. januar 2025. Jeg opplever at det har blitt fremlagt gjennomarbeidede vurderinger til programstyret.

I 2023 var det lagt til grunn at det tekniske målbildet kunne realiseres gjennom delvis gjenbruk av eksisterende plattformer. Som følge av hendelsen sommeren samme år måtte programmets gjennomføringsstrategi endres, og det er nå basert på anskaffelse og etablering av en helt ny plattform. Med nytt kontrollpunkt i 2024 støttet ekstern kvalitetssikrer denne tilnærmingen. Basert på min innsikt virker dette fornuftig.

Jeg ønsker også å dele mine vurderinger av om programmets prosjekt vil kunne realiseres i tide og innenfor økonomisk ramme. Programmet har en faseinndelt gjennomføringsplan som jeg mener vil bidra til leveranser innen definert omfang, tid, kvalitet og kostnad. Arbeidet med å anskaffe og etablere en felles digital plattform er en prioritert utviklingsoppgave også i DIO. Vi bidrar med dedikerte fagressurser til programmet, og fremover vil vi bruke enda flere ressurser på dette arbeidet. Slik skal vi bidra både til å sikre tilstrekkelig kvalitet og til å bygge kompetanse i DIO, som forberedelse til fremtidig eierskap, forvaltning og drift av den nye plattformen. DIO, programmet og programeierne har god dialog om dette, bl.a. i ukentlige møter der programleder rapporterer status.

Programmet skal levere en felles digital infrastruktur, med DIO som ansvarlig totalleverandør. Formålet med DIO er vanskelig å realisere uten én felles plattform til å bygge sikre og fremtidsrettede tjenester på. Jeg ser derfor frem til en felles plattform som gjør det mulig å utløse gevinster innen sikkerhet, effektivitet og kvalitet i departementenes oppgaveløsing og enklere drift av tjenestene. Vi i DIO er parat til å ta leveranseansvaret for den nye plattformen når den suksessivt blir klar for bruk fra 2026.

Med dette avslutter jeg min innledning og stiller meg til disposisjon for å svare på komiteens spørsmål. Takk

Møtelederen: Tusen takk for innledningen. Vi går over til komiteens utspørring. Det er jeg som starter, med saksordførerens 10 minutter.

Spørsmålene vil primært rettes til direktøren for DSS, men det er selvfølgelig mulig også for deg å hoppe inn og svare, hvis det er mer relevant, og hvis du føler at du sitter med relevante svar på spørsmålene.

Vi må starte med utgangspunktet for at dette ble en interessant sak for deler av kontrollkomiteen. Det skyldes at det var lagt en strategisk plan fra tidligere regjering om at departementene skulle migrere over til For-

svarsdepartementets tonivåsystem. Bak det lå det beslutninger og vurderinger som bygde på sikkerhetsbetraktninger: at sikkerheten i et system som var bygd på DSS, ikke var tilstrekkelig, og at det kunne være risiko for f.eks. hacking, noe som igjen ville være både utfordrende og ikke minst kostbart hvis skulle skje.

Så skjer det altså noe i 2023. Dette er mine betraktninger, men det blir brukt et fremmedord eller «konsulentord»: et endret målbilde. Vi blir opplyst om at målbildet blir endret, som jeg forstår har en nærmere forklaring. Det endrede målbildet innebærer i realiteten at man går tilbake på den tidligere strategiske planen – slik oppfattes det i alle fall herfra – og at man fortsetter på tanken om å bygge på deler av et DSS-system som har klare, identifiserte risikoer og svakheter.

Hvem er det som tar den beslutningen? Jeg tror vi må begynne med det. Helt konkret: Hvem tar beslutningen om dette endrede målbildet, som, etter komitéleders oppfatning, er å skifte ut en tidligere fastlagt plan om at dette skulles migreres til Forsvarsdepartementets, FDs, tonivåløsning?

Torgeir Swensson Strøm: Jeg startet i DSS den 1. november 2023, altså etter dataangrepet. Jeg er kjent med noen av vurderingene som er gjort tidligere, men jeg kan ikke svare for det som er gjort veldig tidlig, altså før 2023. Det som ble lagt til grunn i forbindelse med dataangrepet og den endringen som kom etter dataangrepet, var at man gjorde omfattende analyser for å finne ut hva som var den beste løsningen. Tilliten til Depnet/U-løsningen var redusert etter angrepet, og det gjorde at man måtte gjennomgå hva man skulle gjøre. Det var en omfattende og dyptgripende prosess, og mange spørsmål ble stilt i den sammenhengen.

Møtelederen: For å være helt tydelig: Den bekymringen eksisterte jo også på et tidligere tidspunkt. Derfor ble det lagt en plan fra høyere hold om at man skulle migrere til Forsvarsdepartementets tonivåløsning. Det var det som var identifisert som en god løsning. Så skjer endringene i dette målbildet likevel, uten tilstrekkelige sikkerhetsvurderinger av hvordan det ville gå, ser det ut til – og så skjer det man fryktet. Det er derfor vi bare prøver å finne ut hvem det er som sitter med ansvaret og som foretar denne endringen av målbildet. Du har nevnt programeiere og programstyre, og at det er der det formelt sett er forankret, men går det an å være mer spesifikk? Hvem er det som tar beslutningen?

Torgeir Swensson Strøm: Jeg klarer ikke å være mer spesifikk når det gjelder det som har gått forut for min tid i DSS. Det klarer jeg ikke å gi deg veldig konkret. All erfaring er at når det gjelder hvordan strukturen i styringen fungerer, er det eierne, altså i dag Digitaliserings- og forvaltningsdepartementet, DFD, og Forsvarsdepartementet som tar de beslutningene.

Møtelederen: Vi får sikkert anledning til å spørre mer om dette senere i høringen.

Jeg vil gå over til sikkerhetsvurderingene. Vi har i brev fått opplyst at det ikke forelå konkrete sikkerhetsvurderinger knyttet til endringene av dette målbildet, men ble det fra DSS' side gjort noen betraktninger om hvorvidt sikkerheten var bedre i det ene eller andre systemet? Ble det gjort noen slike vurderinger i det hele tatt i forbindelse med endringen av målbildet?

Torgeir Swensson Strøm: I forbindelse med endringen som skjedde etter dataangrepet, ble det gjort vurderinger i DSS og av eksterne parter, noe som gjorde at vi hadde et godt grunnlag å stå på og vurdere ut ifra.

Møtelederen: I dag driftes departementene på fire ulike plattformer – stemmer det?

Torgeir Swensson Strøm: Det stemmer.

Møtelederen: Er alle enige om at det er tungvint og noe man bør gå vekk fra?

Torgeir Swensson Strøm: Ja.

Møtelederen: I det opplegget som det er lagt opp til nå, er det også lagt opp til mange forskjellige kjøremiljøer, som er et uttrykk som brukes. Man skal ha skjermingsverdig ugradert informasjon i privat sky i norske datasenter. Man skal ha ugradert informasjon delvis i offentlig sky og delvis i et eget datasenter, og så skal man ha graderte løsninger som skal leveres for seg, av statens graderte plattformtjenester. Hvis jeg har telt riktig, er vi da oppe i fire forskjellige kjøremønstre. For meg høres det egentlig ut som om man går fra å mene at fire ulike plattformer er komplisert, til at det fortsatt vil være veldig komplisert, og at man er oppe i iallfall fire ulike kjøremiljøer.

Hvordan ser dere på kompleksiteten i dette? Er det egentlig en forbedring?

Torgeir Swensson Strøm: Jeg vil si at det er en forbedring. Det man gjør, er å bygge en felles plattform som – litt enkelt beskrevet ut fra en økonoms hode – er en felles grunnmur som alt står på, og så innreder man den i ulike miljøer. Årsaken til at man gjør det, er å sikre at man har en felles mur rundt, og så har man ulike muligheter til tilgang, f.eks. en del og et kjøremiljø som kan kobles direkte ut på nettet og hente ut de mulighetene som ligger i det. Hvis man lager en for rigid mur rundt, klarer man ikke å ha løsninger som klarer å koble seg på det som er på utsiden. Det enkleste her er å lage en mur og bare kutte linjen ut til internett. Da er man helt iso-

lert, og man er helt trygg. Ved å ha fire ulike kjøremiljøer, har man fleksibiliteten imellom.

Det er viktig å si at teknologien utvikler seg hele tiden – det er en rivende fart på utsiden av statssystemet, hvor man hele tiden lager nye muligheter. Det er det man prøver å utnytte for å få en moderne plattform som har bygd inn alle de mulighetene som nå ligger inne, og den funksjonaliteten man kan få ved å ha en slik løsning. Jeg er trygg på at dette er en bedre, mer effektiv og sikrere måte å gjøre det på enn å ha fire ulike plattformer med helt ulikt oppsett.

Møtelederen: Hvis man skulle kjørt på denne opprinnelige planen med å ha det samlet i FDs tonivåsystem, ville vi i hvert fall hatt betydelig færre angrepspunkter – vil ikke det stemme? Nå blir det i alle fall fire forskjellige angrepspunkter. Er ikke det en sårbarhet i seg selv?

Torgeir Swensson Strøm: Det at man har én felles plattform, er det som sikrer at man har en så sikker løsning som mulig – vurdert ut fra at man har færre angrepspunkter. Hvorvidt man har FDs plattform eller denne plattformen som man nå planlegger for, dreier seg om fleksibiliteten. FDs tonivåløsning er altså mindre fleksibel enn denne løsningen som det nå planlegges for.

Møtelederen: Jeg bare noterte meg en ting du sa i et tidligere svar om når det ble gjort sikkerhetsvurderinger for DSS. Du sa at det ble gjort sikkerhetsvurderinger etter hackingen.

Torgeir Swensson Strøm: Ja, etter angrepet sommeren 2023.

Møtelederen: Det komiteen er interessert i, eller i hvert fall komitélederen er interessert i – jeg får snakke for meg selv – er hvorfor det ikke gjøres vurderinger ved endringen av målbildet. Man går vekk fra et system nettopp fordi man mener det er fare for hacking, man mener at det er usikkert, og så gjøres det en endring av målbildet tilbake igjen til det presumptivt usikre systemet. Hvorfor gjøres det ikke en sikkerhetsvurdering ved endringen av målbildet, slik at man i det minste får klarlagt risikoen?

Torgeir Swensson Strøm: Jeg mener det gjøres en sikkerhetsvurdering. Da er det litt viktig å si at det etter angrepet gjøres en sikkerhetsvurdering av ulike parter knyttet opp mot Depnet/U-plattformen …

Møtelederen: Ja, det har vi oppfattet … men ved endringen av målbildet, altså en tid før hackingen, hvorfor foretas det ikke sikkerhetsvurderinger knyttet til at målbildet endres? Det var jo hele grunnen i utgangspunktet til at man ønsket å gå for FDs tonivåsystem. Så endrer målbildet seg av noen som vi skal finne ut hvem er, men det foretas, så vidt jeg kan oppfatte, ingen sikkerhetsvurdering i den forbindelse. Det er det jeg spør om: Hvorfor skjer ikke det?

Torgeir Swensson Strøm: Jeg kom inn 1. november 2023, og det er grunnlaget for mine svar.

Møtelederen: Vi skal videre på talerlisten, og ordet går til Arbeiderpartiet. Frode Jacobsen har 5 minutter til sine spørsmål.

Frode Jacobsen (A): Jeg har bare lyst til å følge opp det komitélederen spurte om nå, litt til. Den planen som forrige regjering hadde utarbeidet, var det slik at den ville vært trygg og sikker å kjøre videre på etter angrepet, eller ble det gjort grundige vurderinger som tilsa at det særlig av sikkerhetsmessige hensyn var helt nødvendig å endre det som lå der?

Torgeir Swensson Strøm: Etter angrepet var tilliten til plattformen Depnet/U svekket. Det ble gjort sikkerhetsvurderinger knyttet til om vi kunne stole på denne plattformen etter at det hadde vært angrep. Det ble gjort en rekke tiltak for å sikre den plattformen så godt som mulig samtidig som man vurderte hva vi burde gjøre videre framover, altså i et langsiktig perspektiv. Det ene er det kortsiktige som ble gjort på Depnet/U-plattformen, og så var det vurderingen videre framover: Hva er det vi nå skal gjøre for å lage en ny plattform som kan fungere så godt som mulig for departementsfellesskapet?

Frode Jacobsen (A): Vi har også sett diskusjonen om kostnader her. Den nye løsningen koster mye penger. Kan du si noe om hvilke vurderinger som er gjort, og hvordan man arbeider for å gjøre dette så billig som mulig? Det er vel ikke bare å gå i butikken og kjøpe en løsning for departementene, men summen er veldig høy.

Torgeir Swensson Strøm: Summen er høy, det er jeg enig i i den forstand at det er mange kroner, men det er også en veldig omfattende og kompleks løsning man skal bygge. Det gjør at man har hatt omfattende gjennomganger for å beregne hva dette antakelig vil koste, og det grunnlaget som programmet og programstyret har fått i den sammenheng, er etter min vurdering et godt grunnlag for å kunne vurdere og legge fram for Stortinget det som nå er lagt inn som rammen for programmet.

Frode Jacobsen (A): Så litt om styringen av prosjektet. Nå sitter dere som prosjekteiere, men det styres av

Forsvarsdepartementet og Digitaliserings- og forvaltningsdepartementet. Kan du si noe om hvordan du opplever styringen fra departementene – er de tett på og aktivt med, eller forholder de seg passive?

Torgeir Swensson Strøm: Jeg vil si at begge departementene absolutt er tett på, og det synliggjøres kanskje tydeligst gjennom programstyret, og deltakelsen i programstyret er fra toppnivå i departementene. Det vil jeg si – de involverer seg absolutt i det som legges fram av ulike saker fra programmet og programleder.

Frode Jacobsen (A): Vi ser i mediene at bl.a. ansatte i UD har kommet med noen advarsler og sagt at UDs løsning kan brukes. Vi har sett at noen mener Forsvarsdepartementets løsning kan brukes. Har dere fått noen advarsler underveis fra ansatte, fra IKT-miljøer, som dere ikke har tatt inn over dere eller i tilstrekkelig grad tatt på alvor, eller – advarsler høres litt farlig ut – er det kommet innsigelser og bekymringsinnspill som dere ikke har tatt seriøst?

Torgeir Swensson Strøm: Ikke som jeg er kjent med. Det er alltid en diskusjon, og det gjøres risikovurderinger, og det er en diskusjon i programstyret knyttet til det som legges fram fra programmet og fra programleder. Men det er ingen varsler jeg kjenner til som ligger her som gjør at vi burde valgt noe annet.

Frode Jacobsen (A): Har du noe å legge til, Sørby?

Anders Aagard Sørby: Jeg vil gjerne legge noe til fra DIOs perspektiv. Nå er de vurderingene om gjenbruk av ulike plattformer vurderinger som ble gjort før min tid og før jeg tiltrådte, men det som er viktig fra et DIO-perspektiv, er at vi kan gjenbruke vår evne og vår kompetanse til å levere plattformer til de ulike departementene, også Utenriksdepartementet og spesielt utenriksstasjonene. Derfor bruker vi nå ansatte fra DIO som har spesialistkompetanse, også inn mot å levere tjenester til Utenriksdepartementet, inn i programmet for felles IKT-tjenester, slik at vi sikrer denne kompetansen i det videre arbeidet.

Møtelederen: Da er vi ferdig med spørsmål fra Arbeiderpartiet.

Vi går videre til Senterpartiet. Jeg gir ordet til Eivind Drivenes.

Eivind Drivenes (Sp): Jeg vil tilbake til perioden før målbildet ble endret. Ble det gjort en tilstrekkelig vurdering av sikkerheten og faren for hacking før det? Var det en tilstrekkelig vurdering av sikkerheten i prosjektet og av de forskjellige løsningene? Så kom hackingen, og da så en at en hadde gjort en for dårlig jobb. Er det noe i det?

Torgeir Swensson Strøm: Jeg vil si at i hvert fall med min kunnskap – og igjen må jeg si at jeg kom inn 1. november 2023 – og med de vurderingene jeg har sett, og det som ble gjort etter angrepet, var de vurderingene absolutt gode med hensyn til det å si noe om sikkerhet. Sikkerhet var en klart viktig faktor som ble vurdert i sammenhengen, så det vil jeg si er gjort med god kvalitet.

Eivind Drivenes (Sp): Men var det egentlig et sjokk for prosjektet da hackingen skjedde?

Torgeir Swensson Strøm: Det var nok et sjokk for mange, også ut over programmet. Jeg jobbet i et departement på den tiden, og det var en stor sak. Det må også sies at det var en såkalt nulldagshendelse, så det var ingen som kunne gjøre noe eller visste noe om at det var noen hull i den løsningen vi brukte, Depnet/U-løsningen. Det er viktig å ha for seg at det var en nulldagshendelse, og at det var så å si umulig å vite hvordan det angrepet skulle gå. Det var gjort vurderinger også – det var en inntrengningstest på den Depnet/U-løsningen før sommeren 2023 – så vi hadde ikke noen tegn som jeg kjenner til, på at dette ikke var en god nok løsning.

Eivind Drivenes (Sp): Da det ble gjort vedtak om endret målbilde, var det en stor diskusjon om å endre målbildet, eller var det samstemmighet? Hvordan var det i styringsgruppen?

Torgeir Swensson Strøm: Det var en diskusjon, og det ble lagt fram ulike alternativer. Det var en diskusjon i gruppen. Jeg kom inn 1. november 2023, og vi fikk en del av materialet etterpå. Da var det en helhetsvurdering knyttet til de mulige ulike alternativene, som ble godt diskutert i programstyret.

Eivind Drivenes (Sp): Der var det stor enighet om målbildeendringen?

Torgeir Swensson Strøm: Målbildet man endte opp med, oppfatter jeg at det var god enighet om, og så er det jo et råd som blir gitt. Jeg oppfatter ikke at det var noen store uenigheter i gruppen rundt det.

Eivind Drivenes (Sp): Takk. Da har jeg ikke flere spørsmål.

Møtelederen: Da går vi videre fra Senterpartiet til Fremskrittspartiet og Carl Ivar Hagen.

Carl I. Hagen (FrP): Takk skal du ha, komitéleder.

Jeg vil gjerne først spørre om dette med at programstyret er et rådgivende organ. Er det noen av rådene fra programstyret som ikke er fulgt opp av eierne?

Torgeir Swensson Strøm: Ikke meg bekjent.

Carl I. Hagen (FrP): Derfor kan vi også si at programstyret har en vesentlig og kanskje helt avgjørende innflytelse, selv om det formelt er råd?

Torgeir Swensson Strøm: Jeg har ikke oversikt over alle saker og råd som er gitt, og jeg kom som sagt inn 1. november, men jeg har ikke noen oppfatning av, eller sitter med noe grunnlag for å kunne si, at rådene etter diskusjonen i programstyret ikke har vært fulgt.

Carl I. Hagen (FrP): Det er departementene som er eiere og fatter beslutninger. Fattes de beslutningene av statsrådene, eller er det departementsrådene som treffer beslutninger? Det er jo mennesker som treffer beslutninger, ikke et eller annet annet som omtales som et departement. Er det departementsrådene eller statsrådene som fatter beslutninger?

Torgeir Swensson Strøm: Det kan ikke jeg svare på. Det må stilles til noen i departementet. Jeg kjenner ikke til hvordan det blir gjort inne i departementet.

Carl I. Hagen (FrP): Ok.

Det snakkes også om at dere har hatt eksterne kvalitetssikrere. Hvem er det?

Torgeir Swensson Strøm: Det er ulike konsulentmiljøer som har vært hentet inn for å gi tilbakemelding, og også etater i staten som har oppgaver av den typen.

Carl I. Hagen (FrP): Så det er også private konsulentfirmaer inne som kvalitetssikrere?

Torgeir Swensson Strøm: Det er det.

Carl I. Hagen (FrP): Det ble også snakket om en programleder. Hvem er det?

Torgeir Swensson Strøm: Programlederen er Erik Johannesen.

Carl I. Hagen (FrP): Så programmet har også en organisasjon med en leder?

Torgeir Swensson Strøm: Absolutt.

Carl I. Hagen (FrP): Rapporterer han til programstyret?

Torgeir Swensson Strøm: Han rapporterer til departementet og er ansatt i departementet.

Carl I. Hagen (FrP): Til departementet, ikke til styret.

Dere snakker om trusselaktører. Kan dere si hvem det er? Vet vi noe om det, eller er det sånt dere ikke kan si i en åpen høring?

Torgeir Swensson Strøm: Jeg kan ikke si noe rundt det. Opplysningene rundt dette er graderte.

Carl I. Hagen (FrP): Mener dere to at programmet nå går i henhold til planer og er innenfor rammene – at det egentlig ikke er noen grunn for komiteen til å engasjere seg noe særlig, og at alt går etter planene – eller er det store utfordringer og også eventuelle overskridelser av de økonomiske rammene?

Anders Aagaard Sørby: Som jeg nevnte i min innledning, har programmet nå lagt planer for det videre arbeidet, som vi er godt kjent med. Det er et komplekst arbeid vi står overfor – og når jeg sier «vi», snakker jeg om departementsfellesskapet – for å realisere de IKT-tjenestene vi nå har behov for å få på plass, inklusiv denne felles IKT-plattformen.

Min vurdering av de planene som foreligger nå, med trinnvis utvikling og overgang til én felles plattform som gradvis skal ta over fra de øvrige, er at de er gode.

Når det gjelder kostnadsspørsmålet, er det slik at vi nærmere sommeren får inn oppdaterte priser, slik at programmet kan gjøre oppdaterte estimater over gjenstående arbeid, og vi får kvalitetssikret de tallene som per nå foreligger.

Carl I. Hagen (FrP): Har Strøm noe å si i tillegg?

Torgeir Swensson Strøm: Nei, jeg er enig med direktøren i DIO. Jeg føler at det er en god styring av programmet, og at vi nå er inne i en prosess hvor vi får tilbudene fra leverandørene og kan vurdere kostnadsrammen mye mer konkret, fordi man sitter med faktiske tilbud å vurdere ut fra. Det gjør at du kan si noen ting om dette er innenfor den ...

Carl I. Hagen (FrP): Til selve overgangen fra de fire plattformene til én ny, felles: Når man skifter, er det ofte utfordringer og problemer. Er dere også fornøyd med det dere har sett gjennom – at det er i rute, at gjennomføringsfasen skal gå greit?

Anders Aagaard Sørby: Jeg skal være forsiktig med å si at det vil gå greit, men de planene som ligger for det kompliserte arbeidet vi står overfor, mener jeg er gode og lar seg realisere. Den planen fordrer også at vi i DIO engasjeres og engasjerer oss sterkt i arbeidet, da vi som den samlede totalleverandøren av digitale IKT-tjenester til departementsfellesskapet bl.a. skal ivareta dialog-

en med departementene. Det er komplekst, men vi har gode planer.

Møtelederen: Da går vi videre til SV og Audun Lysbakken – 5 minutter.

Audun Lysbakken (SV): Takk.

Jeg overlater til dere å vurdere hvem som skal svare på mine spørsmål, så lenge dere ikke svarer på det samme.

Formelt sett er det departementene som eier som tar de store beslutningene, men hvem er det som styrer dette prosjektet i praksis, i det daglige? Er det departementsansatte, deres ansatte eller de private konsulentene?

Anders Aagaard Sørby: Jeg tillater meg å svare. Programmet er organisert slik at vi har en programleder. Programlederen er ansatt i Forsvarsdepartementet. Programlederen rapporterer både til eierne i ukentlige statusmøter – hvor jeg også deltar, som direktør for DIO – og til programstyret i om lag månedlige møter.

Audun Lysbakken (SV): Hvis man fra eiersiden er så tett på, hvordan er det da mulig å miste så kontroll over pengebruken på private konsulenter? Nå har det kommet fram at til tross for at DSS varslet om at man hadde passert det som ville være brudd på anskaffelsesreglementet, har man fortsatt å leie inn konsulenter. Tyder ikke det på at konsulentene har stor kontroll og eiersiden liten kontroll?

Torgeir Swensson Strøm: Jeg er ikke enig i at det sier at man ikke har kontroll. Når det gjelder overskridelsen, er det en DSS-sak, og det må jeg ta ansvaret for og beklage at ble en overskridelse. Det var det DSS som burde hatt kontroll på, og det har egentlig ikke noe med programmet som sådan å gjøre.

Audun Lysbakken (SV): Kan du bare forklare hvordan det kunne skje?

Torgeir Swensson Strøm: Det skyldes ulike forhold. Det viktigste er at når man har en avtale sånn som denne er formet, er det laget et tak. Den går også ut på tid, så det var et siste tidspunkt for når avtalen skulle brukes, men her gikk man i taket. Det dreide seg om at man i en fase i programmet bl.a. trengte mer kapasitet. Da ble denne avtalen brukt, og så overskred man den.

Vi har i ettertid analysert hvordan dette kunne skje, og her er det også en sak hvor Riksrevisjonen er inne i bildet. Ut fra mitt ståsted hadde vi ikke god nok kontroll på forbruket på avtalen. Det henger bl.a. sammen med at vi hadde et opplegg med seksmåneders kontrollpunkter, hvor vi fikk tilbakemelding fra leverandøren hver sjette måned på hvordan forbruket var. Der glapp det, egentlig.

Audun Lysbakken (SV): Kan du forstå at det tolkes som at disse konsulentene har jobbet på egen hånd med liten grad av kontroll?

Torgeir Swensson Strøm: Jeg er ikke enig i den beskrivelsen. Her er det to ting som er helt atskilt: Når det gjelder avtalen og det som skjedde i forbindelse med avtalen, er det en sak som DSS må ta ansvaret for – altså det som dreier seg om avtaleforvaltningen – mens det som dreier seg om bruk av konsulenter i programmet, er en helt annen sak.

Audun Lysbakken (SV): Hvorfor blir antallet innleide høyere og høyere i dette programmet – langt høyere enn opprinnelig forutsatt?

Torgeir Swensson Strøm: Jeg kan ikke svare for bruken av konsulenter i programmet. Det jeg kan svare for, og som jeg også var inne i en vurdering av, er avdelingen i DSS som nå er overført til DIO. Den hadde egentlig kapasitet og kompetanse til å drifte Depnet/U, men ingen vesentlig kompetanse til å drive et stort og komplekst prosjekt eller program som skifte av plattform er. I den sammenheng var man ute og prøvde å få tak i kompetanse i DSS til å bruke inn i programmet. Gjennom det slipper man å leie inn, men når man ikke klarte å hente inn personer som var fast ansatt i DSS, måtte man leie inn for å ha den kapasiteten og den spisskompetansen som trengs i programmet. Vi lånte ut personer fra DSS til programmet, og vi erstattet dem med innleie av konsulenter i DSS for at vi skulle ha personer som var fast ansatt i staten til å delta inn i programmet.

Utgangspunktet her er at man den gangen ikke hadde kapasitet og kompetanse i – skal vi si – staten og DSS til å ivareta en så stor og kompleks operasjon som skifte av plattform er. Da må en basere seg på innleie av konsulenter som kan ha en spisskompetanse på enkelte områder, og som vil bidra inn med kapasitet.

Møtelederen: Da går vi videre til Naomi Røkkum fra Venstre, som har 5 minutter.

Naomi Ichihara Røkkum (V): Tusen takk. Mange spørsmål er allerede dekket, men jeg fortsetter litt der SV slapp, med spørsmål knyttet til kostnader. Hva var årsaken til at kostnadsoverskridelsene ble oppdaget i oktober? Var det denne seksmånedersrutinen som du snakket om?

Torgeir Swensson Strøm: Ja, vi fikk tall fra leverandøren som viste at vi var over grensen på 600 mill. kr.

Naomi Ichihara Røkkum (V): Hva slags type økonomisk rapportering har det vært i programstyret? Dere har jo møter ganske ofte.

Torgeir Swensson Strøm: Programstyret rapporterer på selve programmet. Som sagt er det ikke noen sammenheng mellom avtalen som sådan og den rapporteringen og det opplegget som er for styringen inn i programmet.

Naomi Ichihara Røkkum (V): Hvor er det økonomien rapporteres til, slik at man fortløpende kunne ha avdekket kostnadsbruken?

Torgeir Swensson Strøm: Avtalen er som sagt DSS' avtale. Det er mange parter som kan gjøre avrop på avtalen, og flere departementer bruker den. Det er en generell fellesavtale på tvers av alle departementene. Det rapporteres ikke inn i programmet på bruken av den avtalen i seg selv.

Naomi Ichihara Røkkum (V): Burde den typen kostnadsbruk ha vært rapportert inn?

Torgeir Swensson Strøm: Nei, den strukturen er på en måte rettet inn mot DSS, så det er DSS som må ta det ansvaret, med tanke på forvaltningen av avtalen generelt. Det kan ikke legges inn i programmet som noe ansvar for programmet.

Naomi Ichihara Røkkum (V): Du nevnte at dette ikke var godt nok styrt. Hvilke tiltak har dere gjort for at det ikke skal skje framover? Vi er nok enige om at vi trenger et godt IKT-system, men vi trenger heller ikke akkurat en kostnadsoverskridelse framover, og da er det noe med å kunne ha økonomisk kontroll også fortløpende, ikke bare en gang i halvåret.

Torgeir Swensson Strøm: Da er det viktig med rammen for programmet, og man er innenfor styringsrammen som er satt der. Det er veldig viktig å skille dette, for det er ingen sammenheng mellom den avtalen og det som foregår i programmet. Det er viktig å ha med seg.

Det er gjort ulike tiltak, og vi har også fått pålegg gjennom tildelingsbrevet for 2025 om å gjøre ulike vurderinger og tiltak i DSS, også med hensyn til den nye avtalen som nå er inngått med en leverandør, hvor vi har endret kontrollregimet og oppfølgingsregimet. Vi har strammet opp avtaleforvaltningen med tanke på både den avtalen og andre avtaler som vi har på helt andre områder i DSS.

Naomi Ichihara Røkkum (V): Hvor ofte er økonomikontrollen og -rapporteringen framover?

Torgeir Swensson Strøm: For avtalen som dreier seg om konsulentinnleie, er det nå hver måned. Det har gått fra hver sjette måned til hver måned.

Naomi Ichihara Røkkum (V): Og det handles på den rapporteringen, så det ikke bare er en nikk-og-smil-øvelse?

Torgeir Swensson Strøm: Den handles det på, det kan jeg garantere deg.

Møtelederen: Da har vi vært gjennom alle partiene i komiteen og de fem minuttene de har til disposisjon.

Nå er det en åpen runde for oppklaringsspørsmål. Vi kan starte med Kirsti Leirtrø fra Arbeiderpartiet.

Kirsti Leirtrø (A): Takk for det. Jeg har to spørsmål. Det er litt vanskelig å få svar på det som har skjedd før 2023, har jeg forstått, men jeg vil likevel forsøke. I 2011 kom den første utredningen om behovet for å få samordnet alle departementene, og i 2018 ble det besluttet. I 2019 foregår det en hacking, og det blir en reetablering i 2021. Dette er hendelsesforløpet. Strøm svarer her at de kortsiktige løsningene etter hackingen var å få begrenset skadevirksomheten, nær sagt. Jeg har likevel et spørsmål om vurderingene rundt de langsiktige løsningene: Var det det som var grunnen til behovet for å omorganisere?

Jeg lurer også på om det ble tatt noen grep med hensyn til det det blir spurt om om konsulentbistand, altså ekstern konsulentbistand kontra det å ha det i egen organisasjon, utover det å stramme inn på avtaleverket.

Torgeir Swensson Strøm: Det er ulike deler i det spørsmålet. Til innstramming i konsulentbruken: Når programmet er satt opp, har man lett etter kapasitet i DSS og i de andre organisasjonene som nå på en måte er en del av DIO, altså Justisdepartementet og Utenriksdepartementet. Man klarer å ta ut og bruke kapasitet som er eller var i de organisasjonene, for å bistå inn i programmet – det er gjort – og etter mitt skjønn har man brukt de personene så langt man klarer. Men når behovet er til stede for en spesiell kompetanse eller ekstra kapasitet, er det det som er grunnlaget for det omfanget av konsulentbruken.

Jeg føler og oppfatter at den konsulentbruken skyldes at man ikke har hatt tilstrekkelig kapasitet i DSS, Justisdepartementet eller Utenriksdepartementet til å bidra inn. Det er ikke sånn at man bare har leid inn fordi man synes det er fint og flott – overhodet ikke. Det er et viktig poeng, tenker jeg. Det var én del av det du spurte om.

Når det gjelder den langsiktige vurderingen: Angrepet var sommeren 2023. Da ble Depnet/U-plattformen angrepet. Etter det var det kortsiktige tiltak for å håndte-

re det på Depnet/U-plattformen, og så i programmet. De kortsiktige tiltakene var det DSS som sto for. Det var de tiltakene man gjorde veldig konkret. I tillegg til det måtte programmet gå inn og se og vurdere om det var behov for noe annet, gitt at Depnet/U-plattformen hadde redusert tillit som en følge av angrepet.

I den vurderingen av ulike scenarioer og hvordan man skulle gå videre, oppfatter jeg at det var en god vurdering av det som var mulige alternativer, som gjorde at man endte med den løsningen man nå går inn for, og den plattformløsningen man går inn for i dag.

Anders Aagaard Sørby: Jeg vil gjerne legge til noe rundt dette med konsulentbruk. Igjen kan jeg ikke gå for langt tilbake i tid, men fra mitt perspektiv ser jeg helt klart at det er krevende å frigjøre tilstrekkelig egne internt ansatte til et så stort utviklingsarbeid som det som nå foregår. Fra mitt perspektiv har det vært viktig at vi i DIO i perioden fra nyttår og fram til nå – og ikke minst i tiden framover – kan supplere bruken av eksterne konsulenter med våre egne ansatte. Det er egentlig av to hovedårsaker. Det ene handler om at vi må benytte vår spisskompetanse til å levere IKT-tjenester til departementsfellesskapet og supplere konsulentkompetansen med det, ikke minst for gradvis å bygge oss kompetanse på det vi skal ta over eierskap til og forvaltning av framover.

Per i dag har DIO om lag 20 egne faste ansatte som bistår i programmet i ulike prosentsatser. Vi jobber nå for å forberede hvordan vi kan øke dette antallet i den fasen programmet går inn i nå, som er en gjennomføringsfase der vi faktisk skal bygge den nye felles plattformen.

Møtelederen: Da er Audun Lysbakken neste på listen.

Audun Lysbakken (SV): Det er nevnt flere ganger hva slags sikkerhetsvurderinger som er gjort rundt spørsmålet om hvorvidt det var mulig med gjenbruk av systemer, systemer som har blitt kompromittert gjennom dette angrepet i 2023, og det har også vært spørsmål om gjenbruk av UDs system. Kan dere si noe mer om karakteren til de vurderingene? Er det gjort en utredning av gjenbruksspørsmålet, f.eks.? Og i så fall, hvor?

Anders Aagaard Sørby: Nå var ikke jeg en del av de vurderingene som ble foretatt, eller den prosessen som ledet opp til de beslutningene som ble tatt når det gjelder gjenbruk av bl.a. UDs plattform. Jeg hadde heller ikke detaljkunnskap om hvordan status på UDs plattform var før jeg overtok ansvaret fra nyttår. Samtidig er det viktig for meg å få fram at det er flere egenskaper ved den tidligere UD-plattformen som det er viktig å kunne gjenskape i det videre arbeidet.

Audun Lysbakken (SV): Jeg tror jeg avbryter deg der. Det er greit med den argumentasjonen, men jeg er egentlig ute etter å komme til bunns i hvordan beslutningen ble tatt, for dere har henvist til vurderingen flere ganger. Rent formelt: Hvordan ble den vurderingen tatt? Ble det f.eks. gjort en skriftlig utredning? Finnes den noe sted? Var det primært fra konsulentsiden denne vurderingen kom? Beskriv prosessen.

Torgeir Swensson Strøm: Jeg tror ikke jeg klarer å svare deg godt på det spørsmålet. Her er det programmet som legger det fram. Programlederen legger det fram i programstyret. Som sagt har jeg ikke vært inne lenger enn fra 1. november 2023, men det er vurderinger som ble gjort, og som ble lagt fram i programstyret, som er grunnlaget for de rådene som kommer videre. Det er ikke en utredning som blir satt ut til et fagmiljø et eller annet sted. Det er programmet som gjør de vurderingene, med dialog inn mot f.eks. DSS.

Audun Lysbakken (SV): Greit. Siden det er henvist til vurderingen flere ganger, tror jeg det er rimelig at komiteen får mulighet til å se hvordan den vurderingen er gjort. Hvis dere ikke kan svare på det, er det jo mulig at vi kan få det skriftlig i etterkant – en beskrivelse av den prosessen og hvordan den vurderingen ble gjort.

Møtelederen: Det kan vi ordne i en etterfølgende korrespondanse med de inviterte.

Vi går til Carl I. Hagen.

Carl I. Hagen (FrP): Det er flere som nå har tatt opp bruken av konsulenter. Er det rammeavtaler med ulike konsulentfirmaer, hvor det altså er de som er leverandører som rapporterer til dere om hvor mange konsulenttimer som er benyttet? Det ble vel sagt at det var leverandøren som varslet om at man gikk over denne grensen på 600 mill. kr. Betyr det at det er leverandørene som selv styrer, får etterspurt tjenester fra ulike departementer og rapporterer inn hvor mange timer som er benyttet? Hvordan er det systemet?

Torgeir Swensson Strøm: Det systemet er at DSS har inngått én felles avtale for kjøp av konsulenter innenfor et spekter av konsulenttjenester. Den avtalen ligger der og er tilgjengelig for alle departementene. De kan gjøre avrop på den avtalen. Det departementene gjør, er å si at de nå trenger sånn kapasitet og sånn kompetanse. Så er det den leverandøren som har den avtalen, som går ut og har en oversikt over hvilke konsulenter som har denne kompetansen, og som da kan tilbys

til den prisen som ligger i avtalen som er etablert med DSS.

DSS eller det departementet som gjør avrop, synliggjør et behov, og så får man et tilbud tilbake igjen fra den leverandøren om at vi kan tilby dette, gitt den kravspesifikasjonen dere har kommet med. Det er ikke vi som i utgangspunktet styrer hvilke konsulenter vi skal ha inn. Det er en kravspesifikasjon som forteller hva det er vi har behov for akkurat nå, og så er det mange avrop på den avtalen. Ulike departementer har avrop på den. Før DIO ble etablert, hadde vi også avtale i DSS, hvor vi har gjort avrop på den avtalen.

Carl I. Hagen (FrP): Er det én avtale med ett firma, eller er det flere forskjellige? Og det andre er: Når departementene da foretar et avrop, er det departementet som får regningen for det, eller er det på fellessystemet?

Torgeir Swensson Strøm: Nei, det er departementet som får regningen, og som betaler den.

Carl I. Hagen (FrP): Ok. Det er ikke slik at departementene kan foreta avrop som betales av noen andre? De får for det de bruker?

Torgeir Swensson Strøm: Ja.

Carl I. Hagen (FrP): Det er bra.

Er det én avtale med mange firmaer, og hvordan inngås de? Er det anbud med disse avtalene?

Torgeir Swensson Strøm: Det er det som er litt spesielt med denne avtalen. Det er en såkalt megleravtale, så det er en konsulentmegler. Det er ett firma som har avtaler med ulike konsulentmiljøer, så vi bare forespør megleren: Vi trenger denne kapasiteten og denne kompetansen, kan dere gi oss et tilbud på det? Prisene er lagt i den fellesavtalen allerede, så de tilbyr på de prisene som ligger i fellesavtalen. Det er en megleravtale, og det er noe annet enn enkeltavtaler med enkeltfirmaer.

Møtelederen: Da har jeg tegnet meg selv. Vi må tilbake igjen til dette endrede målbildet. Den tidligere regjeringen hadde altså skåret gjennom og sagt at man skulle migrere over til FDs tonivåløsning. Det var tatt en avgjørelse om at det var det sikreste, basert på sikkerhetsbetraktninger. Så skjer det et regjeringsskifte, og så går tiden, og så oppfatter jeg klart og tydelig at det skjer en eller annen form for reversering. Man går vekk fra FDs tonivåløsning og går tilbake igjen til tanken om å bygge på et annet system. Det er en stor, ganske fundamental avgjørelse for dette prosjektet.

Det er formelt påpekt hvor avgjørelsene tas, osv., men selv om du ikke vet svaret på det, som du har sagt tidligere: Er det naturlig for komiteen å legge til grunn at en så stor avgjørelse som dette gjøres i tett samspill med den politiske ledelsen i de involverte departementene, og at man har ryggdekning i departementets øverste ledelse når man tar en så stor og viktig beslutning både sikkerhetsmessig og kostnadsmessig?

Torgeir Swensson Strøm: Som jeg har svart tidligere, oppfatter jeg at departementene, altså de to eierdepartementene, er veldig tett koblet på, men jeg kjenner heller ikke til dialogen som er inne i de to departementene mellom embetsverk og politisk ledelse knyttet til saken. Jeg har ingen indikasjoner på at de ikke snakker sammen, men jeg kan ikke gi deg et konkret svar. Det må de etterfølgende partene, eller innkalte, si noe om.

Møtelederen: Helt naturlig. Det er egentlig bare for å høre, kan du si, litt betraktninger og forventninger og hvordan dere opplever det fra deres posisjon, men jeg forstår selvfølgelig at det formelt er vanskelig for dere å gi svar på nøyaktig hva som har skjedd på departementssiden.

Kan jeg da spørre om noe annet? Det er sagt fra statsråden i denne sakens forbindelse at de har en stram styring av prosjektet. En stram styring av prosjektet vil vel også si at man er tett involvert i en så viktig avgjørelse som å endre fra FD II-nivået og til et helt annet system. Er det riktig for oss å kunne legge til grunn?

Torgeir Swensson Strøm: Ja, jeg vil si at det er en stram og god styring av programmet. Så er det, som bl.a. direktøren i DIO nevnte, ukentlige møter, det er månedlige programstyremøter, og det er også møter som blir gjort med basis i, skal vi si, ekstraordinære saker som ønskes tatt opp. Jeg føler at det her er en veldig god styring på programmet generelt. Men jeg klarer ikke å gi svar på hva som foregår inne i departementet, og hvordan dette blir gjort inne i departementet.

Møtelederen: Vi har litt ekstra tid, så Naomi Ichihara Røkkum har tegnet seg.

Naomi Ichihara Røkkum (V): Dere har nevnt balansevurderingen mellom bruk av interne ressurser og eksterne konsulenter, og vi fikk et godt svar, føler jeg, på det som gjelder det framtidige. Men kunne dere ha sagt litt om hvilke vurderinger som ble gjort rundt den balansen, både innledningsvis, før man igangsatte og underveis på ulike tidspunkt, i og med at dette er noe dere har vært klar over over tid?

Torgeir Swensson Strøm: Jeg kan svare litt for det jeg har vært inne i selv, og særlig da vinteren og våren 2024, hvor programmet er på for å få kapasitet fra DSS til å bruke inn i programmet som kompetanse. Vi måtte si: Beklager, her klarer vi ikke å avgi ressurser. Vi kunne

bl.a. ikke gjøre det av driftshensyn, for vi hadde en plattform vi skulle drive, og vi kunne ikke avgi de folkene inn i programmet for at de skulle drive med planlegging knyttet opp mot det framtidige. Det vi gjorde da – og så får Anders svare for det som ligger der i dag – var at vi ga ressurser til programmet, og så leide vi inn konsulenter for å drifte Depnet/U-løsningen, som vi hadde ansvaret for. Så her har det vært nøye vurderinger, vil jeg si – i hvert fall var det det i DSS – når det gjelder hva slags nivå vi klarer oss på, hva vi kan avgi av kapasitet til programmet, og når må vi si: Vi kan ikke avgi mer, for da er vi redd for driften av Depnet/U-plattformen.

Naomi Ichihara Røkkum (V): Kunne man hatt en prosjektansatt? Én ting er den personal- og kompetansemessige siden av det, men ble det også gjort en kostnadsavveining av å ha noen som er fast ansatt, enten det er frigjøring av andre ressurser fra andre steder, eller det f.eks. er en prosjektansatt f.eks. som får dedikert oppgaver knyttet til dette, som tross alt er et ganske stort prosjekt?

Torgeir Swensson Strøm: I første rekke: Det jeg har vært inne i, er en vurdering av hva vi klarer å avgi av kapasitet. Jeg og DSS har sagt at ok, hvis vi får erstattet med en innleid, altså at vi får ressurser å hente inn, da kan vi avgi en fast ansatt som jobbet i DSS, som en ressurs til programmet.

Anders Aasgaard Sørby: Jeg vil gjerne legge til fra mitt perspektiv: Fra DIO er det nå fire ansatte som over en lengre periode, også før DIOs etablering, er frigjort og jobber i programmet med leveranseoppgaver der, i tillegg til 20 ansatte som er med på mindre eller større basis. Det er vurderinger som er gjort i de tidligere fasene, og som vi viderefører i DIO.

Naomi Ichihara Røkkum (V): Da kan jeg spørre litt banalt: Hadde det vært billigere å ha en fast ansatt, noen som har bestillerkompetanse, enn å ta inn disse konsulentene?

Anders Aasgaard Sørby: Det er alltid en avveining av hva man skal ansette i våre etater kontra hva vi skal leie inn. Fra DIOs perspektiv ser jeg at vi ikke har den spisskompetansen som vi trenger, og det vil være uhensiktsmessig å bygge opp så mye kapasitet i vår linjeorganisasjon for å drive et så stort utviklingsarbeid på siden av våre oppgaver. Fremover nå har vi et arbeid for å etablere en sourcingstrategi som skal svare på og være en veiledning for oss når det gjelder hva slags kapasitet og kompetanse vi skal ha i vår driftsorganisasjon, og hva slags kapasitet vi skal kjøpe i markedet.

Møtelederen: Vi rekker et kort spørsmål fra Eivind Drivenes.

Eivind Drivenes (Sp): Takk, leder. Nå stilte Venstres representant mange gode spørsmål, og det er noe i samme rekken: Var egen kapasitet og kompetanse inn i prosjektet overvurdert? Var det en overvurdering av det i tidlig fase?

Torgeir Swensson Strøm: Jeg har ikke noe grunnlag for å svare deg på det. Jeg har ikke vært inne i de vurderingene, men det har hele tiden vært gjort en vurdering, og programmet har hele tiden etterspurt kapasitet og kompetanse fra linjeorganisasjonen i de tre enhetene som har vært inne her, altså DSS, Justisdepartementets IKT-enhet og UDs IKT-enhet. Altså har man etter mitt skjønn så langt som mulig prøvd å få kapasitet og kompetanse. Så har vi som har jobbet i linjen – jeg får si for DSS sin del, da – avgitt så langt vi klarer, til vi ikke har turt å gå lenger med å avgi folk med tanke på driftingen av den plattformen. Det er det som på en måte er hovedutfordringen, og har vært det i DSS: å sikre at vi i tillegg har en god drift av den plattformen, som departementene er avhengige av hver eneste dag.

Møtelederen: Da er vi kommet til den siste delen, som er muligheten for de inviterte til å si noen avsluttende ord, hvis det er ønskelig. Dere har opptil 5 minutter hver, hvis dere ønsker det.

Anders Aasgaard Sørby: Takk for det, komitéleder. Jeg ønsker kort å oppsummere min redegjørelse for komiteen.

Selv etter hendelsen i 2023 er målet for programmet uendret, nemlig det å sikre at Statsministerens kontor, alle departementene, Norges utenriksstasjoner, DSS og 22. juli-senteret får én felles og sikker digital plattform for moderne teknologi, noe som vil styrke departementsfellesskapets evne til å løse sitt samfunnsoppdrag.

Vi har også snakket om disse ulike kjøremiljøene. Vi har i dag fire ulike plattformer som det er svært komplekst å foreta drift og forvaltning av. Det å bygge én felles plattform, som vi nå gjør, er en riktig utvikling. Den plattformen som vi nå bygger, vil ha ulike bestanddeler, såkalte kjøremiljøer, nært knyttet sammen i én felles plattform, som gjør det mulig for DIO i fremtiden å sikre en helhetlig drift og forvaltning av den plattformen.

Etableringen av den nye plattformen er en forutsetning for at vi i DIO skal kunne lykkes i rollen som Departementenes digitaliseringsorganisasjon, og bidrag til programmets videre arbeid har derfor en høy prioritet hos meg. Takk.

Møtelederen: Tusen takk.

Torgeir Swensson Strøm: Jeg har ingen ytterligere kommentarer utover det som direktøren i DIO sa. Min vurdering, litt sånn overordnet, er at vi trenger en felles plattform å bygge på videre i framtiden for at dette skal fungere på en god måte for departementene.

Møtelederen: Da takker jeg på vegne av kontrollkomiteen for at dere tok dere tid til å møte opp her. Vi samles igjen kl. 10.40.

Høringen ble avbrutt kl. 10.21.

Høringen ble gjenopptatt kl. 10.40

Høring med tidligere kommunal- og distriktsminister og tidligere forsvarsminister Bjørn Arild Gram, og tidligere kommunal- og distriktsminister Sigbjørn Gjelsvik

Møtelederen: Da er klokken 10.40, og vi er klare til å starte opp igjen. Det er en glede for meg som leder av komiteen å ønske velkommen til tidligere kommunal- og distriktsminister og tidligere forsvarsminister Bjørn Arild Gram. Du har med deg en bisitter, departementsråd i Forsvarsdepartementet Frede Hermansen. Jeg vil også ønske velkommen til tidligere kommunal- og distriktsminister Sigbjørn Gjelsvik. Du har med deg en bisitter, ekspedisjonssjef i Digitaliserings- og forvaltningsdepartementet Jan Olav Pettersen. Velkommen til dere alle.

Dere kjenner opplegget. Hver får 10 minutter til innledning, og deretter starter komiteens utspørring. Saksordfører får 10 minutter til spørsmål, og så får partigruppene inntil 5 minutter til sine spørsmål. Så blir det en åpen runde på 15 minutter til oppklarende spørsmål, og til slutt får dere muligheten til å si noen korte oppsummerende ord. Jeg minner for ordens skyld om at dette er en åpen høring, og at hvis det er behov for å gi taushetsbelagte opplysninger, må det skje for lukkede dører.

Jeg tror rett og slett vi går rett på sak. Bjørn Arild Gram har 10 minutter til innledning – ordet er ditt.

Bjørn Arild Gram: Takk for det, leder. Utgangspunktet for denne høringen er program for felles IKT-tjenester for departementsfellesskapet, som jeg heretter kaller programmet. Ansvaret for programmet er delt mellom digitaliserings- og forvaltningsministeren, tidligere kalt kommunal- og distriktsminister, og forsvarsministeren. Jeg hadde ansvaret for programmet da jeg var kommunal- og distriksminister fra oktober 2021 til april 2022, og senere som forsvarsminister fra april 2022 til februar i år.

Bakgrunnen for at programmet ble etablert, var at det i departementsfellesskapet eksisterte fire ulike IKT-organisasjoner, med sine egne IKT-plattformer. Forsvarsdepartementet, Justis- og beredskapsdepartementet og Utenriksdepartementet hadde alle egne IKT-organisasjoner. De øvrige departementene benyttet IKT-plattformen som på det tidspunktet var driftet av Departementenes sikkerhets- og serviceorganisasjon, DSS, men som nå driftes av Departementenes digitaliseringsorganisasjon, DIO. Jeg vil heretter kalle denne IKT-plattformen for Depnet/U.

Jeg er glad for at vi gjennom etableringen av programmet endelig har klart å etablere en mer kraftfull innsats for å samle IKT-miljøene og sørge for at departementsfellesskapet får en sikker, kostnadseffektiv og moderne IKT-plattform. Dette er et stort og komplisert arbeid. Det var derfor viktig at arbeidet ble gjennomført og styrt etter anerkjent prosjektmetodikk og i tråd med statens prosjektmodell.

Digitaliserings- og forvaltningsdepartementet og Forsvarsdepartementet eier og styrer programmet i fellesskap. Den øverste administrative ledelsen i de to departementene følger programmet tett. Lederen av programmet er ansatt i Forsvarsdepartementet. Som en del av styringen er det etablert et programstyre. Formålet med programstyret er å gi råd til eierne og sørge for at styringen av programmet er godt forankret. Programstyret består, i tillegg til av representanter fra ledelsen i eierdepartementene, av representanter fra ledelsen i Utenriksdepartementet, Justis- og beredskapsdepartementet og Statsministerens kontor. I tillegg deltar direktørene for Departementenes sikkerhets- og serviceorganisasjon og Departementenes digitaliseringsorganisasjon. Programstyret har gitt oss mulighet til å drøfte vanskelige problemstillinger og sørge for at programmets målbilde ivaretar behovene i departementsfellesskapet på en god måte. Programstyremøtene avholdes månedlig. I tillegg har også eierdepartementene ukentlige oppfølgingsmøter med programledelsen.

Den politiske styringen av programmet foregår i ordinær dialog mellom embetsverk og politisk ledelse i de respektive departementene. Alle viktige saker skal behandles i regjeringen. Det har vi fulgt opp i styringen av dette programmet.

Store statlige prosjekter skal i henhold til statens prosjektmodell være gjenstand for ekstern kvalitetssikring. Etter ferdig forprosjekt skal det gjennomføres en ekstern kvalitetssikring, en såkalt KS2, før kostnadsrammen legges fram for Stortinget. Dette var noe av det første vi satte i gang etter at jeg tiltrådte som statsråd i oktober 2021. I KS2-rapporten fra våren 2022 støttet ekstern kvalitetssikrer innretningen til programmet og ga klarsignal til oppstart. Kvalitetssikreren anbefalte at det ble

gjennomført ytterligere kvalitetssikringer i såkalte kontrollpunkter underveis. Dette er fulgt opp. Basert på anbefalingene fra kvalitetssikringen fremmet regjeringen forslag for Stortinget om en kostnadsramme på om lag 1,4 mrd. kr. Kostnadsrammen ble vedtatt av Stortinget gjennom behandlingen av Innst. 110 S for 2022–2023 i desember 2022. Det var i forbindelse med nysalderingen.

Målbildet ved oppstart av programmet var å etablere en ny felles IKT-plattform gjennom anskaffelse i markedet. Den nye plattformen skulle i hovedsak være basert på en privat skyløsning levert av en tredjepart. De tidligere IKT-miljøene skulle samles i et nytt forvaltningsorgan underlagt det daværende Kommunal- og distriktsdepartementet. Ekstern kvalitetssikrer ga tilbakemelding om at valgt målbilde kunne være hensiktsmessig, men de ba oss om å vurdere å etablere en ny plattform med gjenbruk av komponenter fra Depnet/U. Vi vurderte dette i den videre gjennomføringen og kom frem til at en ny felles IKT-plattform med gjenbruk av enkelte komponenter fra Depnet/U ville være en farbar vei, både sikkerhetsmessig og økonomisk. Våren 2023 ble justert målbilde med gjenbruk lagt fram for ekstern kvalitetssikring. Dette var første kontrollpunkt. Ekstern kvalitetssikrer ga støtte til det nye målbildet og la til grunn at dette ville gi lavere kostnader i etablerings- og migreringsfasen.

La meg si noen ord om sikkerhetsvurderingene som ble foretatt i denne perioden. Nasjonal sikkerhetsmyndighet gjennomførte i 2022 en inntrengningstest av Depnet/U. Dette var en test av sikkerheten og sårbarheten til datasystemet gjennom planlagte og forhåndsbestilte angrep. Testen ga gode tilbakemeldinger på sikkerhetstilstanden til Depnet/U. Den bekreftet at det var mulig og sikkert å gjenbruke komponenter fra plattformen i den nye felles IKT-plattformen. Mot slutten av 2022 startet vi også et nødvendig oppgraderingsarbeid på komponenter i Depnet/U. Oppgraderingsarbeidet på Depnet/U, som startet opp i slutten av 2022, økte sikkerhetsnivået ytterligere og sørget for økt levetid på komponentene som det ble vurdert å gjenbruke. Som følge av dette var det ikke behov for å gjennomføre en ny sikkerhetsvurdering av Depnet/U våren 2023. Det var uansett en forutsetning at ny felles IKT-plattform skulle godkjennes av Nasjonal sikkerhetsmyndighet. En annen viktig forutsetning for sikkerheten var at informasjon som er gradert i henhold til sikkerhetsloven, skulle lagres og behandles gjennom Forsvarsdepartementets IKT-plattformer.

På grunn av dataangrepet mot Depnet/U sommeren 2023 måtte vi replanlegge målbildet for ny felles IKT-plattform. Vi gjennomførte sikkerhetsvurderinger av Depnet/U og vurderinger av handlingsalternativer på kort sikt. Tidligere kommunal- og distriktsminister vil redegjøre nærmere for håndtering og oppfølging av selve dataangrepet. Sikkerhetsvurderingene som ble gjennomført av tilstanden til Depnet/U etter dataangrepet, resulterte i at vi ikke lenger hadde tillit til komponentene som var tenkt gjenbrukt i ny felles IKT-plattform. Nærmere beskrivelser av disse vurderingene må eventuelt tas i en lukket del.

Det nye målbildet etter dataangrepet er å etablere en ny felles IKT-plattform gjennom anskaffelse i markedet. Den nye plattformen vil være en hybrid løsning, hvor det etableres tre kjøremiljøer for behandling av informasjon med ulik verdi: ett kjøremiljø for ugradert skjermingsverdig, ett kjøremiljø for ugradert og ett kjøremiljø for bruk av offentlige skytjenester. Dette er ikke det samme som helt atskilte løsninger, slik som vi har i dag, og som Nasjonal sikkerhetsmyndighet har advart mot.

Det er viktig at departementenes verdier sikres på riktig nivå, og at vi ikke skaper unødvendige begrensninger for oss selv. Det er nettopp dette en ny felles IKT-plattform vil gi oss. De ulike sikkerhetsnivåene gjør at vi kan sikre verdiene våre på en hensiktsmessig måte, samtidig som vi får tilgang på effektive og moderne digitale verktøy. Takk så langt, leder.

Møtelederen: Tusen takk selv. Da går vi videre til tidligere kommunal- og distriktsminister Sigbjørn Gjelsvik, som også har 10 minutter til sin innledning – vær så god.

Sigbjørn Gjelsvik: Takk for det, leiar. Eg tiltredde som kommunal- og distriktsminister i april 2022 og hadde den statsrådsposten fram til oktober 2023. I den perioden hadde eg saman med tidlegare forsvarsminister Gram ansvaret for Program for felles IKT-tenester til departementsfellesskapa.

Innleiingsvis vil eg seie at eg sluttar meg til det Gram har sagt om den perioden eg har innsikt i og kan svare for, altså den perioden eg sat som statsråd. I den perioden var programmet under god styring frå dei to ansvarlege departementa, og eg vil òg framheve at samarbeidet mellom dei to departementa var svært godt.

Føremålet med programmet er å etablere ei felles, sikker, kostnadseffektiv og moderne IKT-plattform for departementa. Drift av fire ulike IKT-plattformar er lite hensiktsmessig. Det er ikkje kostnadseffektivt, og det skapar utfordringar for den digitale samhandlinga mellom departementa. Nasjonal sikkerheitsmyndigheit og andre sikkerheitsekspertar har òg understreka at fire ulike plattformar gjev fleire angrepsmoglegheiter for aktørar som ønskjer å skade våre interesser.

I den vidare delen av innlegget mitt vil eg fokusere på kva vi la til grunn for programmet i perioden rett før

dataangrepet mot plattforma Depnet/U sommaren 2023, og handteringa og oppfølginga av dataangrepet i 2023.

Våren 2023 gjennomførte vi det fyrste kontrollpunktet av programmet med ekstern kvalitetssikring. Målbildet som då vart kvalitetssikra, var ein ny felles IKT-plattform med gjenbruk av enkelte komponentar frå plattforma Depnet/U. Som Gram var inne på i sitt innlegg, vurderte både departementa og ekstern kvalitetssikrar våren 2023 at ei ny felles IKT-plattform med gjenbruk av nokre komponentar frå Depnet/U ville vere ein farbar veg, med tanke på både sikkerheit og økonomi.

Planen var å informere Stortinget om desse endringane i målbildet hausten 2023. Så langt kom vi aldri på grunn av angrepet mot IKT-plattforma Depnet/U sommaren 2023. I juli 2023 oppdaga vi at ein avansert og ressurssterk trusselaktør hadde kome seg inn på e-postserverar på Depnet/U via den dåverande løysinga for synkronisering av e-post til tilsette sine mobile einingar.

Denne løysinga er ein kommersiell programvare som vert brukt av mange verksemder globalt. Sikkerheitshòlet trusselaktøren utnytta, var ei såkalla nulldagssårbarheit. Utan å gå inn på tekniske forhold betyr ei nulldagssårbarheit at ein trusselaktør har identifisert og utnytta eit svakt punkt før leverandøren er kjend med det. Sårbarheiter av denne typen er nærmast umogleg å beskytte seg mot.

Sikkerheitshòlet som vart oppdaga av oss, og som ramma fleire andre verksemder i verda, vart raskt tetta av programvareleverandøren. Som følgje av at trusselaktøren hadde kome seg inn på e-postserverane på Depnet/U, vart serverane kompromitterte.

Før eg gjer nærmare greie for handteringa og oppfølginga av dataangrepet, vil eg understreke at eg ved to anledningar sommaren 2023 informerte Stortinget om dette på eigna måte.

Under og rett etter dataangrepet gjekk mykje av tida til å handtere hendinga og gjennomføre risikoreduserande tiltak. Dei kompromitterte serverane for e-post vart tekne ned, og det vart raskt etablert ei ny e-postløysing for departementa. Dette var eit særs viktig arbeid for å sikre at departementa hadde gode kommunikasjonsløysingar.

Som eit risikoreduserande tiltak overførte vi ikkje gamle e-postar til den nye e-postløysinga. Det vart òg innført fleire sikkerheitstiltak på Depnet/U, slik som auka overvaking av plattforma. Vi endra òg rutinane våre for saksbehandling, slik at vi i større grad behandla saker og prosessar på nasjonalt avgrensa plattform. Alle desse tiltaka har bidrege til å redusere restrisikoen ved å fortsetje å bruke Depnet/U og gjer at det er akseptabelt å nytte plattforma vidare, fram til ny felles IKT-plattform er etablert.

Som ein del av oppfølginga etter dataangrepet hausten 2023 gjennomførte vi i samarbeid med våre sikkerheitsleverandørar og Nasjonal sikkerheitsmyndigheit fleire sikkerheitsvurderingar av tilstanden til Depnet/U. Dette var for å undersøkje sikkerheitstilstanden til plattforma samt tilliten til komponentane som var planlagt gjenbrukte i ny felles IKT-plattform. I tillegg vurderte vi om det var mogleg raskt å etablere ei midlertidig plattform som varetok dei mest sentrale funksjonane til departementa fram til ny og fullt funksjonell felles IKT-plattform var ferdig etablert. Resultatet av desse vurderingane vart ikkje klare før etter at eg fråtredde som kommunal- og distriktsminister i oktober 2023.

Med det avsluttar eg mi innleiing og stiller meg til disposisjon for å svare på spørsmåla til komiteen.

Møtelederen: Tusen hjertelig takk for det.

Jeg starter med saksordførerens spørsmål, som er på 10 minutter.

Vi må egentlig skru tiden tilbake igjen til da den forrige regjeringen styrte, hvor det ble tatt en beslutning – forankret på politisk nivå i regjeringen – om å migrere departementenes systemer til Forsvarsdepartementets systemer, altså FD II-nivå. Det var en beslutning basert på bl.a. sikkerhetsbetraktninger, faren for hacking og den type ting.

Det skjer en prosess, som beskrives i brevet: Det skulle migreres til FD II-nivå-plattform. I arbeidet ble en full migrering til FD II-nivå vurdert som uhensiktsmessig.

Så foretas altså denne store, ganske fundamentalt viktige beslutningen om å endre målbildet og gå tilbake igjen til det som handler om å bygge videre på DSS-systemet, altså det som ser ut som en reversering av en beslutning om å gå over på FD-systemer. Hvem tok den beslutningen? Jeg tror jeg går til Gram først.

Bjørn Arild Gram: Det er korrekt at man besluttet å gå bort fra den tiltenkte modellen med å bygge på Forsvarsdepartementets tonivåplattform. Forrige regjering hadde påbegynt en kvalitetssikring våren 2021, men den ble også stoppet, for ekstern kvalitetssikrer mente at styringsdokumentene som forelå, ikke tilfredsstilte kravene for KS2, og at det ikke var grunnlag for videre kvalitetssikring. Så jobbet man videre utover høsten 2021 med å ta arbeidet videre og sluttføre et revidert forprosjekt.

Det kan hende man skulle ha snakket med tidligere forsvarsminister, eventuelt før regjeringsskiftet også, om i hvor stor grad det hadde begynt å modne seg en vurdering allerede da av at det ikke var hensiktsmessig med den løsningen, for Forsvarsdepartementets platt-

form har et høyt sikkerhetsnivå. Det å skulle ha alle departementenes bruk inn i den plattformen – det var tatt en prinsippavgjørelse om det, men det var neppe godt nok fundert, hvis jeg kan bruke det ordet. Markedet kunne levere dette bedre. Det hadde vært veldig uhensiktsmessig for departementsfellesskapet å måtte bruke Forsvarsdepartementets løsning. Da hadde vi risikert at en rekke applikasjoner ikke kunne blitt koblet på det nye systemet. Målet er jo å komme fram til et system som er sikkert, men også fleksibelt og hensiktsmessig for departementene.

Det må sies at det da ikke ble besluttet at man skulle gå over på en gjenbrukt Depnet/U-løsning. Det er ikke korrekt. Det ble besluttet – med forankring i regjering – at vi skulle finne en løsning i markedet, en privat skyløsning, for det som ikke er gradert informasjon. Den graderte informasjonen skulle fortsatt tilhøre Forsvarsdepartementets systemer.

Møtelederen: Det er interessant. Spørsmålet mitt er fortsatt hvem som tok den beslutningen om det endrede målbildet. Altså: Hvor er den beslutningen tatt, og hvor er den forankret?

Bjørn Arild Gram: Det er departementene som er konstitusjonelt ansvarlige, og statsrådene som tar beslutningene, men alle viktige beslutninger, milepæler og veivalg i programmet er forankret i regjering.

Møtelederen: Så regjeringen hadde dette oppe til vurdering og sa at det var greit å gå vekk fra planen om FD II-nivå og over på et annet system som baserer seg på kommersielle løsninger?

Bjørn Arild Gram: Det var ingen i systemet som mente at det var hensiktsmessig å gå videre med FDs tonivåmodell fullt ut, som opprinnelig skissert i en prinsippbeslutning.

Møtelederen: Da må dere ha bygget på noen faglige råd. Er det riktig?

Bjørn Arild Gram: Absolutt. Hvis det tillates, kan jeg gjerne be departementsråden utdype hvorfor FDs tonivåmodell ikke var hensiktsmessig for departementsfellesskapet.

Frede Hermansen: Forsvarsdepartementets plattform har vært utviklet tidlig på 2000-tallet, og gradvis egentlig forvaltet på en god måte, men den har vært knyttet mot at FD primært samhandler med Forsvaret og har behov for at den samhandlingen skal skje effektivt. Det gjør at den ugraderte delen av denne er veldig knyttet mot den graderte, og sånn sett har den veldig sterke skiller med hva annet som kommer inn på den. Det er også den eneste ugraderte plattformen som per nå er sikkerhetsgodkjent for skjermingsverdig, på grunn av den tilknytningen.

Det vi så da vi begynte å jobbe med å realisere den prinsippbeslutningen som var tatt tidligere, var at med en gang man skal ha med andre departementer som har helt andre grensesnitt – utenrikstjenesten med hundre utenriksstasjoner, Finansdepartementet med tunge makromodeller, osv. – ville det være ekstremt vanskelig og kostnadskrevende og innebære enormt mye «one-off», altså særløsninger, for å kunne få det til å fungere. Det var nok også det som preget litt den første runden med ekstern kvalitetssikring, hvor ekstern kvalitetssikrer sa at grunnlaget ikke var godt nok for å gå videre. Dette var i 2020–2021.

Da så vi at skal vi lage en plattform som møter de målsettingene – altså både sikker, effektiv og kostnadsforsvarlig drift – kunne ikke det bygges på FDs opprinnelige tonivåplattform. Derfor gikk man til Stortinget med endringsproposisjonen i 2022 og anbefalte at man brukte FDs plattform mot det graderte, men lagde en ny, ugradert plattform som skulle sikkerhetsgodkjennes, basert på en kommersiell leveranse fra leverandører. Så det er årsaken til at man gikk vekk fra det opprinnelige.

Møtelederen: I brevet som vi har fått fra Tung, sier hun klart og tydelig at den nye løsningen skulle være basert på DSS. I et brev fra 18. februar står det at målbildet var å videreutvikle IKT-plattformen som ble driftet av DSS. Det er mulig at jeg bare har misforstått.

Bjørn Arild Gram: Jeg kan oppklare det, for det er flere faser i dette, og det har vært utvikling i saken. Det som var klart etter at FD-modellen ble skrinlagt i den opprinnelige planen, var at man skulle gå ut i markedet når det gjaldt det ugraderte. Den løsningen ble kvalitetssikret av en ekstern kvalitetssikrer. Det var den eksterne kvalitetssikreren som foreslo – dette var våren 2022 – at man av praktiske, økonomiske og sikkerhetsmessige årsaker burde se på om det var elementer i Depnet/U som kunne gjenbrukes. Det ble det da jobbet videre med fram mot årsskiftet 2022–2023 og inn i 2023, som da ble det første kontrollpunktet, hvor man ettergikk en modell for hvordan man kunne gjenbruke enkelte deler av Depnet/U-løsningen. Så det kom senere i den prosessen.

Møtelederen: Kan jeg spørre om dere synes kostnadene for dette prosjektet har vært rimelige så langt? Det er et spørsmål til begge.

Bjørn Arild Gram: Kostnadene er jo i stort holdt innenfor de rammene som er godkjent av Stortinget. Man gikk til Stortinget med en ramme på 1,4 mrd. kr,

men så kom dataangrepet sommeren 2023, som har gjort at man har måttet replanlegge programmet, gå bort fra gjenbruk av enkeltelementer fra Depnet/U og tilbake til en markedsbasert løsning. Det er hovedforklaringen på at kostnadsrammen er økt. Da man justerte kostnadsrammen i 2024, var det hovedforklaringen. Det er nesten hele beløpet. I tillegg var det prisstigning, og endringstrinn tre er også tatt inn i sluttkostnaden, noe som ikke var en del av det opprinnelige kostnadsanslaget, fordi det var for stor usikkerhet knyttet til hva det kunne innebære. Det ble også med en frontløsning i tillegg som ikke hadde vært inkludert. Hovedforklaringen på at rammen ble utvidet og godkjent av Stortinget, var dataangrepet sommeren 2023.

Sigbjørn Gjelsvik: Eg kan slutte meg til det som Gram seier her, for den perioden eg kan svare for som tidlegare statsråd. Det er nettopp dataangrepet, handteringa av dataangrepet og dei endringane i prosjektet som vart gjorde i etterkant, som rører ved veldig mange av dei auka kostnadene som det var, og som ein òg gjekk til Stortinget med, i etterkant av at dataangrepet hadde skjedd.

Møtelederen: Tusen takk. Vi går videre til Arbeiderpartiet, og det er Frode Jacobsen, som har 5 minutter.

Frode Jacobsen (A): Takk skal du ha, og takk til dere begge. Jeg synes Gram bidro med mye klarhet her rundt hvorfor FDs tonivåplattform ikke kunne brukes. Kunne dere – i hvert fall Gram, i første omgang – si noe om hvordan dette egentlig fungerer? Du var litt inne på det i din redegjørelse – dette programstyret og hvordan beslutninger tas i et sånt program. Hvor ofte fikk du som statsråd forelagt deg ting som du måtte ta beslutninger om? Eller fikk du opp notater der det på en måte var slik at hvis dette ikke er greit, må du si ifra nå? Kan du si noe mer om hvordan dette styres av dere som politisk ledelse i et departement?

Bjørn Arild Gram: Det er klart at det er både en uformell og en formell dialog mellom statsråd og departementsråd og embetsverk i et departement. Man snakker sammen hele tiden og blir holdt orientert hvis det er spesielle ting. Samtidig har det vært noen større korsveier, når man har gjort hovedvalg av målbilde og veien videre, skal legge fram saker for Stortinget, osv. Da får du jo opp saker om det, og så vurderer du om du da bør gå til regjering og få forankring for de største beslutningene. Og det har skjedd i denne saken. Vi har hatt en løpende dialog, vært involvert ved de sentrale korsveiene og vært med og tatt beslutninger.

Frode Jacobsen (A): Kunne dere – hvem av dere vet jeg ikke – si noe om hvilke initiativ dere tok, eller hvordan dere stilte spørsmål for å prøve å redusere omfanget av eksterne konsulenter inn i et prosjekt som dette?

Bjørn Arild Gram: Det har vært viktig for regjeringen generelt å gå kritisk gjennom konsulentbruken, prøve å få ned den så mye som mulig og bygge kompetanse i egen organisasjon. Man var i noen grad inne på dette i den forrige sekvensen, fra etatene. Det har vært et omfattende arbeid hele veien for å søke etter ressurser i egen virksomhet. Ambisjonene har nok vært større enn man har fått til. Det er etterspurt kompetanse. IKT-kompetanse er krevende å skaffe seg for mange slags virksomheter, så det har vært krevende, men man har vært veldig opptatt av at etatene også skal ha folk sentralt i dette – selvsagt – slik at man også kan bygge kompetanse i egen regi og ta dette videre. Det har også ført til at man har måttet frigjøre ressurser fra sin ordinære drift og puttet dem inn i programmet, som da kanskje i noen grad har blitt erstattet av konsulenter. Så det er knapphet på ressurser her. Men dette er noe vi har vært opptatt av, både i det programmet spesielt og i departementsfellesskapet generelt.

Frode Jacobsen (A): Nå er jo dere begge på utsiden av dette. Jeg regner med at dere til dagens høring har gått grundig igjennom det som skjedde på deres vakt, det virker i hvert fall sånn. Er det noe dere ser nå i ettertid at man burde gjort annerledes?

Sigbjørn Gjelsvik: Eg meiner at kvar vurdering ein gjer, gjer ein basert på den kunnskapen som ein løpande har.

Eg har vore inne på det når det gjeld dataangrep. Eg har registrert at det har vore spørsmål rundt sikkerheita i plattforma, osv., men det som skjedde knytt til dataangrepet sommaren 2023, var at det var ein avansert og ressurssterk aktør som utnytta det ein kallar ei nulldagssårbarheit, i ei programvare som er levert av ein leverandør som òg leverer den same programvara til ei rekkje aktørar internasjonalt, som vart ramma av det same. Det var DSS som oppdaga sikkerheitshòlet, som gjorde at leverandøren tetta det sikkerheitshòlet. Men som eg sa i innleiinga mi, er det ein type sårbarheit som det nesten er umogleg å gardere seg mot, og som kvar og ein plattform kan risikere å verte utsett for. Difor er det viktig når ein etablerer plattformer, at ein har redundans, og at ein har gode løysingar for å gjenopprette funksjonen når hendingar skjer.

Møtelederen: Da går vi videre. Neste på listen er Senterpartiet. Drivenes, vær så god.

Eivind Drivenes (Sp): Takk for det, leder. Dere har utdypet svarene og deres syn på saken veldig godt. Jeg har et spørsmål til Gram. Du var inne på det forarbeidet

som var gjort før din tid. Du sa noe om det. Du antydet vel at det kanskje ikke var det beste grunnlaget som var der, med tanke på framtidens sikkerhet og framtidsvisjonene, for det var et gammelt opplegg som kom fra departementet. Er det riktig forstått?

Bjørn Arild Gram: Jeg vil ikke karakterisere noe arbeid. Jeg vil bare konstatere at det var satt i gang en ekstern kvalitetssikring av styringsunderlag og kostnadsoverslag for felles IKT-løsning for departementsfelleskapet. Det var våren 2021. Det ble da stoppet samme høst på bakgrunn av at ekstern kvalitetssikrer mente styringsdokumentene som forelå, ikke tilfredsstilte kravene til KS2. Derfor besluttet vi å gå videre med å ferdigstille et forprosjekt som så ble kvalitetssikret eksternt.

Sigbjørn Gjelsvik: Viss eg berre kan få lov til å leggje til noko: Det er alltid ein balanse når det gjeld IKT og avveginga mellom sikkerheit og brukarvenlegheit, og at det skal fungere til føremålet. Det sikraste hadde kanskje vore berre å brukt penn og papir, men vi er opptekne av å kunne kommunisere både mellom departement og mellom departement og underliggjande etatar og andre aktørar ein har å gjere med.

Det var nettopp det departementsråden i Forsvarsdepartementet òg var inne på, at det er ei anna vurdering som må gjerast i eit system som primært gjeld berre Forsvarsdepartementet isolert, enn når det skal fungere for heile departementsfellesskapet – når Arbeids- og inkluderingsdepartementet skal handtere kommunikasjonen med Nav, når Finansdepartementet skal handtere sine aktørar, og når ein i Helse- og omsorgsdepartementet skal kommunisere med sine og på tvers.

Det å finne det rette grensesnittet der er nettopp viktig når ein skal lage ei felles IKT-plattform som skal ha ein felles grunnmur og ei felles ytre ramme, men at ein innanfor det samtidig kan finne nokre ulike løysingar tilpassa behova til dei ulike brukarane.

Eivind Drivenes (Sp): Gram var også inne på det og sa vel noe om at hadde du kjørt videre med den første påtenkte løsningen, ville det blitt en dyr overløsning. Var det fordi det var så mange usikkerhetsfaktorer i forhold til Hermansens plattform, kan du si, fordi det var Forsvarsdepartementet?

Bjørn Arild Gram Det var vel det at du da måtte … For det første er det ikke gitt at du hadde fått de løsningene du ville ha, rett og slett fordi sikkerhetsnivået var som det var. Det andre var at du måtte ha bygd særløsninger. Det var de vurderingene som konkluderte med at det ble dyrt og uhensiktsmessig i sum. Dette er jo ikke en partipolitisk tilnærming.

Jeg må si det, og det blir selvsagt bare en påstand og spekulasjon, at jeg tviler sterkt på at man, uansett hvilken regjering som hadde sittet, hadde kommet til den konklusjonen at man skulle gå videre med det som var. De faglige rådene var at det ikke var hensiktsmessig. Hva markedet kunne levere, hadde også utviklet seg. Det må vi være klar over. Her var det mulig å få sikre skyløsninger på norsk jord, med norske krav og norsk sikkerhet, sikkerhetskrav som vi selv stilte, sikkerhetsklareringer og så videre, som gjorde at du fikk de rette. Du fikk sikre løsninger og samtidig fleksible og hensiktsmessige løsninger som gjorde at departementene fikk dekket behovene sine. Det graderte skulle fortsatt leveres av Forsvarets plattformer.

Eivind Drivenes (Sp): Så et siste spørsmål: Det har vært litt diskusjon om hvor mye makt eksterne konsulenter har hatt. Føler dere at dere har hatt en virkelig avgjørende myndighet og rolle i dette, og at det ikke bare er konsulentene som har styrt prosjektet?

Sigbjørn Gjelsvik: Det er veldig tydeleg at alle viktige avgjerder er forankra i regjeringa. Det er òg slik at embetsverket jobbar på fullmakter frå regjeringa. I oppfølginga av prosjektet har ein òg på høgt nivå i dei to departementa handtert prosjektet, representert ved dei som sit på kvar vår side her. Den som har vore programleiar, som det òg vart sagt i førre bolk, er ein tilsett i Forsvarsdepartementet. Så her har alle viktige avgjerder når det gjeld både økonomi og viktige vegval i prosjektet, vorte forankra. Det har vore løpande dialog om det.

Møtelederen: Da går vi videre på listen, og det er Fremskrittspartiet og Carl Ivar Hagen.

Carl I. Hagen (FrP): Takk skal du ha, leder.

Første spørsmål går til Gram. Du nevnte at den viktige beslutningen som komitélederen spurte om, ble tatt av regjeringen. Hvilken statsråd var det som la frem saken for regjeringens beslutning? Var det deg, eller var det en annen statsråd?

Bjørn Arild Gram Det uttrykket jeg brukte, var at det var «forankret» i regjeringen. Det er jo den enkelte statsråd som på sine områder er konstitusjonelt ansvarlig, men du forankrer ting i regjering. I denne saken er det to statsråder som har vært ansvarlige for saksfeltet. Det er forsvarsministeren hele veien, og det er kommunal- og distriktsministeren, senere digitaliserings- og forvaltningsministeren, etter at departementet ble delt.

Carl I. Hagen (FrP): Ok, takk skal du ha. Så bruker dere begreper der jeg liker navn. Det ble nevnt en ekstern kvalitetssikrer som var negativ og anbefalte at man ikke gikk videre. Hvilket firma var det som var den eksterne kvalitetssikreren?

Bjørn Arild Gram: Det klarer ikke jeg å svare på, og akkurat den konklusjonen ble jo trukket før regjeringsskiftet. Det kan jeg ikke. Er det noen som kan det?

Carl I. Hagen (FrP): Det er litt interessant av og til å vite hvem som har gjort ting. Å bare bruke et uttrykk som «ekstern kvalitetssikrer» – jeg skulle gjerne hatt at man heller brukte navn.

Jan Olav Pettersen: Takk for det. Når vi bruker eksterne kvalitetssikrere, er det også en rammeavtale som Finansdepartementet har inngått. Vi bruker da rammeavtalen til Finansdepartementet, og hvis jeg husker rett, jeg må ta et lite forbehold, er de som har vært med i kvalitetssikringen, A-2 og Holte Consulting. Det er et samarbeid med konsulentfirmaer som er tatt under rammeavtalen til Finansdepartementet. Jeg er litt usikker på den første kvalitetssikringen i 2021, men jeg tror det var A-2 og Holte Consulting da også.

Carl I. Hagen (FrP): Var det også det i 2023?

Jan Olav Pettersen: Da var det A-2 og Holte Consulting, ja.

Carl I. Hagen (FrP): Det ble også nevnt en ekstern leverandør som tettet det hullet som ble utnyttet i angrepet. Hvem var den eksterne leverandøren, som visstnok var over hele verden og leverte samme program?

Jan Olav Pettersen: Det er jeg ikke hundre prosent sikker på, så det må vi komme tilbake til.

Carl I. Hagen (FrP): Som dere skjønner, synes jeg det hadde vært naturlig at man ikke bare brukte begrepet ekstern leverandør ditten og datten i stedet for navn, særlig når dette hullet ble tettet relativt raskt av den eksterne leverandøren av dataprogrammet.

Sigbjørn Gjelsvik: Eg lurer på om det er Ivanti han er på jakt etter i det spørsmålet han stiller.

Jan Olav Pettersen: Ivanti var leverandøren som leverte den tjenesten som det var nulldagssårbarhet på. Det var leverandøren, som er en amerikansk leverandør, som leverte tjenester til bl.a. DSS og Depnet/U. Det stemmer. Hvorvidt det var dem eller noen andre som tettet hullet, er det jeg ikke er helt sikker på.

Carl I. Hagen (FrP): Det var de som også tettet hullet etter at angrepet var slått tilbake.

Jeg har et spørsmål jeg tok opp før i dag også. Programstyret er et rådgivende organ som gir råd til eierdepartementene. Var det noen av rådene fra programstyret som de to eierdepartementene ikke fulgte opp? Jeg prøver å få vite litt om kompetanse og programstyrets reelle funksjon. Hvis alle rådene og anbefalingene fra programstyret er fulgt opp, har jo det programstyret i realiteten betydelig makt og også ansvar.

Frede Hermansen: Jeg kan kort forklare litt om hvordan dette er. Programstyret er et rådgivende organ for oss som er programeiere. Det betyr at alle saker som behandles der, enten er informasjonssaker, drøftingssaker eller beslutningssaker. Ofte er det en progresjon i det, altså at det først informeres, deretter drøfter vi, og til slutt trekker vi kanskje en konklusjon. Det betyr at vi jobber nokså tungt igjennom alle aspekter som ender opp som beslutningssaker. Vi får synspunkter underveis fra de forskjellige deltakerne i programstyret. De går ofte tilbake til sin organisasjon, undersøker mer, gjør nye vurderinger, osv.

I veldig stor grad har vi da gjennom programstyreprosessen klart å komme fram til det man oppfatter egentlig er en konsensusløsning, eller vi har jobbet oss igjennom materialet og saksfeltet slik at vi er trygge når vi trekker en konklusjon. Formelt sett er det vi som programeiere som trekker en konklusjon, så lenge det er innenfor rammene av de fullmaktene vi har fra våre statsråder. Slik sett er det litt vanskelig å si. Ja, vi har fått masse på vårt bord som har vært drøftet i programstyret, som vi har vært uenig i, og så har vi jobbet oss igjennom sakene. Det er viktig, særlig for å ha både forankring og ikke minst få fram alle aspektene ved så store og viktige beslutninger.

Møtelederen: Da går vi videre til SV og Audun Lysbakken.

Audun Lysbakken (SV): Det er et spørsmål jeg har behov for å få full oversikt over. I den forrige bolken ble det pekt på angrepet og sikkerhetsvurderinger som avgjørende for at man ikke kunne velge en eller annen variant av gjenbruksløsning, men slik jeg forsto Gram nå, handler det kanskje vel så mye om applikasjoner som ikke kunne kjøres, altså brukervennligheten. Kan du oppklare det for meg?

Sigbjørn Gjelsvik: Eg kan prøve å svare litt rundt det. Det som det var snakk om, var som sagt ikkje ein full gjenbruk av den plattforma ein hadde, men å kunne gjenbruke komponentar av ho. Det kan framleis vere aktuelt – ikkje i det omfanget, men når ein snakkar om komponentar, kan det totalt sett vere ganske mange komponentar i eit IKT-system, så eg vil ikkje avvise at det framleis kan vere aktuelt å gjenbruke komponentar frå plattforma til DSS og òg frå den tidlegare plattforma til Utanriksdepartementet.

Grunnen til at vurderingane endra seg, var som sagt at ein hadde vorte utsett for eit angrep. Det var dokumen-

tert at e-postserveren var kompromittert, altså at det hadde vore nokon på innsida, og at den aktøren ein stod overfor, var ein ressurssterk og avansert aktør som hadde vore villig til å bruke betydelege ressursar på dette.

Audun Lysbakken (SV): Så det er sikkerhet som er det avgjørende for beslutningen?

Sigbjørn Gjelsvik: Det var grunnen til at ein gjorde dei vurderingane då eg var statsråd. Som eg viste til i innleiinga mi, vart det òg bedt om vurderingar frå Nasjonal sikkerheitsmyndigheit i etterkant av angrepet. Dei vurderingane var ikkje klare før etter at eg gjekk av som statsråd. Dei er graderte òg, så det må eventuelt statsråd Tung, som kjem seinare i dag, utdjupe.

Audun Lysbakken (SV): Det kan vi komme tilbake til. Jeg skjønner at vi ikke kan gå inn i innholdet i disse sikkerhetsvurderingene her, men det er fint for komiteen å få svar på hvordan beslutningen ble fattet. Noe jeg spurte om i forrige bolk, og som jeg ikke fikk svar på da, var om det lå noen form for skriftlig utredning til grunn. Altså: Hva slags beslutningsgrunnlag fantes da dere tok denne beslutningen?

Sigbjørn Gjelsvik: Kan du presisere kva slags avgjerd du snakkar om no?

Audun Lysbakken (SV): Dere har fått et faglig råd, så jeg lurer egentlig på hva som var formen på det faglige rådet. Var det gjort en utredning, f.eks.?

Sigbjørn Gjelsvik: Viss vi spolar tilbake til tida før dataangrepet, var det, som Gram viste til, kome eit råd frå ekstern kvalitetssikrar om å gjenbruke delar av plattforma. Det låg i utgangspunktet ikkje inne i den avgjerda som først vart teken, men det var eit råd frå ekstern kvalitetssikrar som vart gjennomgått i dei ansvarlege departementa, og som ein òg jobba ut frå og hadde til hensikt å informere Stortinget om. Det var forankra i regjeringa. Alle viktige avgjerder knytte til framdrift i programmet, var forankra i regjeringa.

Til det spørsmålet vil eg òg seie at det generelt sett alltid er slik at det går prosessar og er dialog undervegs. Òg frå oss som utgjorde den politiske leiinga, vart det stilt spørsmål tilbake til programmet. Det vart òg gjeve føringar og rammer for det vidare arbeidet. Eg kan berre svare for den tida eg satt som statsråd, men både avgjerder om endringar i målbildet knytt til å gjenbruke delar av plattforma, og at ein seinare valde andre løysingar, var forankra i regjeringa.

Audun Lysbakken (SV): Det har vi hørt flere ganger, at det er forankret i regjering, men jeg lurer på beslutningsgrunnlaget under det. Du har fått et faglig råd, men hvilken form er det på det? Jeg tenker da på tiden etter dataangrepet og beslutningen om at en måtte gå for et nytt system: Hvilken form var det på det faglige rådet? Er det en vurdering som kommer fra konsulentene, eller er det en bredere utredning? Kan du beskrive det for oss?

Sigbjørn Gjelsvik: Før dataangrepet kom det ein rapport frå ekstern kvalitetssikrar, som skulle vere grunnlag for dei vurderingane som skulle gjerast vidare i programmet, med forankring i regjeringa.

Når det gjeld vurderingane som vart gjorde etter dataangrepet, har eg vist til nokre av dei prosessane som vart sette i gang mens eg var statsråd. Angrepet vart oppdaga i juli 2023, og det vart sett i gang prosessar som Stortinget vart informert om, i forlenging av det. Dei vurderingane som kom i etterkant, var ikkje ferdige på det tidspunktet eg gjekk av som statsråd, i oktober 2023. Så forma på det, og kor langt ein eventuelt kan gå i innhaldet i dei vurderingane som då vart gjorde, f.eks. av Nasjonal sikkerheitsmyndigheit, må statsråd Tung kome tilbake til.

Møtelederen: Da har vi kommet til Venstre og Naomi Ichihara Røkkum.

Naomi Ichihara Røkkum (V): Jeg vil også bygge litt videre på det som ble sagt i forrige runde. Hvordan har man, fortløpende og på ulike tidspunkt, vurdert balansen mellom intern ressursbruk, ved reallokering, midlertidig prosjektansettelse – som man tross alt har anledning til, med tanke på at DSS meldte at de ikke nødvendigvis hadde en del av den kapasiteten tilgjengelig – og konsulentbruk, i og med at regjeringen tross alt har vært kritisk til konsulentbruk i regjeringsapparatet?

Sigbjørn Gjelsvik: Eg kan igjen svare på noko av det som gjeld min periode, og så kan Jan Olav Pettersen eventuelt utdjupe noko. Når det gjeld både dei auka kostnadene som var i den perioden eg sat, og at det var ein betydeleg grad av konsulentbruk då, skriv veldig mykje av det seg frå konsekvensar av dataangrepet og etterarbeid i etterkant av det. Nye kostnadsrammer vart òg følgde opp i etterkant av det. I ein slik situasjon var det behov for raskt å hente ressursar for å handtere ein krevjande situasjon. Jan Olav Pettersen kan kanskje seie noko meir generelt om konsulentbruk.

Jan Olav Pettersen: Ambisjonen vår var å ha en 50/50-deling mellom innleide ressurser og interne. Vi brukte mye tid på å se etter ressurser som kunne bistå oss, både i departementene – hele departementsfellesskapet – og i de eksisterende IKT-organisasjonene. Vi har ikke klart den ambisjonen. Vi har ligget et sted mellom 25 pst. og 30 pst. i intern bistand. Det har rett og

slett å gjøre med at folkene i departementsfellesskapet og IKT-organisasjonene har andre oppgaver, og vi klarte ikke å ...

Naomi Ichihara Røkkum (V): Har da midlertidig ansettelse vært vurdert?

Jan Olav Pettersen: Vi har ikke vurdert midlertidige ansettelser som sådan, for det andre vi trenger, er spisskompetanse. Det jeg ikke kom til, var at det har vært behov for teknisk spisskompetanse og spisskompetanse på prosjektstyring, som ikke departementene, eller IKT-organisasjonene, hadde.

Naomi Ichihara Røkkum (V): Det er også egentlig grunnen til at jeg spør om hvorfor man ikke har vurdert midlertidig prosjektansettelse, som man kan gjøre for en sånn type stort prosjekt, som varer over en viss periode. Det var jo også det som kom fram av DSS tidligere, at hvis man mangler den kompetansen – og regjeringen hadde denne ambisjonen om lavere konsulentbruk.

Kunne dere sagt litt om hva som er misjonen framover – hvis jeg først kan spørre deg, Jan Olav Pettersen: Kommer dere til å gjøre noen videre justeringer på denne 50/50- og 25/75-fordelingen?

Jan Olav Pettersen: Framover nå er det veldig viktig å få en god overgang mellom IKT-programmet og overgangen til drift, så det er viktig at DIO og DIOs ansatte nå får en innsikt og forståelse av det systemet som de etter hvert skal overta og drifte. Vi bruker mye tid på å sørge for den overgangen, og da er det også naturlig å bruke DIOs ansatte. Så må vi ha respekt for at de er nyetablert – etablert for fire måneder siden – og sånn sett har kapasitetsutfordringer. Men fram mot ferdigstillelse er det viktig at DIOs ansatte er delaktige og etter hvert overtar programmet.

Naomi Ichihara Røkkum (V): Jeg kan stille et siste spørsmål – så kan du, Gjelsvik, svare ut det samtidig, kanskje?

Sigbjørn Gjelsvik: Men no beveger vi oss litt meir inn i det som eg trur det er naturlig at statsråd Tung kan svare ut.

Naomi Ichihara Røkkum (V): Ja, men det kan vi ta da.

Sigbjørn Gjelsvik: Men viss det gjeld konkret den perioden som eg kan...?

Naomi Ichihara Røkkum (V): Ja, det gjør det. Både du, Gjelsvik, og Gram var inne på dette med kostnadsbildet, men jeg fikk en smørbrødliste, og det er litt vanskelig å forholde seg til økonomisk. Altså: Dere sa at hackerangrepet var en viktig del av det, men hva slags type forholdstall snakker vi om nå? Hvor stor andel kan man egentlig tilskrive at det var et hackerangrep? Det ble også nevnt prisøkning? Det var særlig Gram som hadde en sånn liste, innledningsvis.

Bjørn Arild Gram: Grunnkalkylen for å gjennomføre programmet har økt med 513 mill. kr, eks moms. Av det skyldes 360 mill. kr dataangrepet. 87 mill. kr skyldes inkludering av endringstrinn 3, som ikke var kostnadsberegnet før nå, og som skulle komme i tillegg. Det siste tallet, 65 mill. kr, skyldes et nytt system for bruker- og driftsadministrasjon som ikke lå inne. Det kan man si at det kanskje skulle ha gjort. Samtidig var jo den opprinnelige tanken nettopp å bruke FDs løsning, som for så vidt hadde et sånt system. Det handler om hvordan en kan drifte og forvalte dette på en kostnadseffektiv måte, nemlig hvordan brukergrensesnittet er, men også hvordan selve driftsorganisasjonen kan håndtere systemet. Men det går egentlig ikke an å si at det sånn sett er noen annen kostnadssprekk enn at det er... Nå har vi inkludert totalen av det som skulle inkluderes, samt at vi har tatt konsekvensene av dataangrepet.

Møtelederen: Da har vi kommet til den åpne spørsmålsrunden, som er på totalt 15 minutter, og Kirsti Leirtrø har tegnet seg.

Kirsti Leirtrø (A): Takk for det. Jeg har litt behov for å få tidsaspektet på dette, så da har jeg to spørsmål, og jeg tror begge går til Gram. Det er fordi da du tiltrådte, lå det på ditt bord, hvis jeg forsto deg riktig, en bestilling, altså en ekstern kvalitetssikring og et mer detaljert forprosjekt som skulle igangsettes, som det ikke var du som bestilte. Det er det ene spørsmålet. Det andre går på dette med politiske beslutninger om programvare kontra utvikling. Vi snakker ikke her om en hyllevare som skal bestilles, men er det riktig at det var fire ulike IKT-organisasjoner som skulle slås sammen til én da du tiltrådte?

Bjørn Arild Gram: Til det siste: Ja, det har hele tiden vært intensjonen å få samlet fire ulike IKT-miljøer – i tre departementer pluss DSS – til ett felles, og det gjør vi nå, så det gjennomføres jo.

Til det første: Av forrige regjering ble det satt i gang et eksternt kvalitetssikringsarbeid, som man selv kom til at måtte stoppes, etter at ekstern kvalitetssikrer, slik jeg oppfattet det – og nå lener jeg meg litt på svaret fra Karianne Tung til komiteen, for det står egentlig beskrevet der – mente at at styringsdokumentene ikke tilfredsstilte kravene for å gjennomføre KS2. I departementet var vi da enige om at vi skulle ferdigstille forprosjektet, og det var da, gjennom det, man så på andre løsninger,

som så ble kvalitetssikret våren 2022. Og i den tilrådingen sa kvalitetssikrer at i tillegg til å se på en markedsbasert skyløsning, se også på om dere kan gjenbruke komponenter fra Depnet/U, og det jobbet vi videre med. Alt dette er framlagt for Stortinget.

Møtelederen: Da går vi videre på listen, til Carl I. Hagen.

Carl I. Hagen (FrP): Det var litt spørsmål i sted om konsulentbruk, og da fikk vi opplyst at målet hadde vært 50/50 med innleide konsulenter og fast ansatte, men at man på grunn av problemer og utfordringer nå lå på 25–30 pst. egne ansatte. Det betyr altså at innleide konsulenter må være på 75 pst., som er et veldig, veldig høyt tall i normale virksomheter. Da har jeg lyst til å spørre – av ren nysgjerrighet: Hva er kostnadsforskjellen? Altså: En fast ansatt har en årslønn på et eller annet, som dere vet, og som jeg spør om, mens en innleid konsulent på årsbasis koster hvor mye? Hva er forskjellene her? Jeg vet jo selvsagt at konsulenter varierer, at hvis det er spisskompetanse og annet, så går lønningene opp, men betyr det at konsulenter i private firmaer har høyere lønn enn det som er mulig å tilby i departementene, og i statsansattes systemer?

Frede Hermansen: Det er veldig vanskelig å si noe generelt om det, annet enn at kostnadene per hode per time vil jo bli høyere når du leier inn en konsulent, og det ligger også en overhead i selskapet osv. Samtidig er det slik at når du leier inn en konsulent – litt avhengig av hvordan det er – får du også mer, du får mer tilgang til hele selskapets kompetanse enn bare det ene hodet. Det er sånne elementer i det. Så ja, isolert sett vil det bidra til at du øker kostnadene, sammenlignet med et annet alternativ. Men samtidig har vi jo, som vi har vist, fortsatt styrt dette innenfor rammen og på de leveransene, så sånn sett styrer vi prosjektet på rammen, som forutsatt.

Jeg har bare lyst til å legge til et siste element til det med konsulentbruken, og det er den andre bidragsytende årsaken til at vi har fått en høyere andel enn det vi la til grunn innledningsvis. Det har å gjøre med at mens vi nå bygger ny plattform, driftes fortsatt de opprinnelige plattformene med sine opprinnelige brukere. Dette er da organisasjoner som er på slutten av sin levetid – de vet at de skal inn i en omstilling, og de vet at de skal bli en ny organisasjon, og at plattformen og kompetansen som de sitter med, i varierende grad skal gjenbrukes. Det gjør også at det er veldig vanskelig å holde på den kompetansen inn i en omstilling, og vi har nok overvurdert vår evne til å holde på den kompetansen i omstillingen. Det har også å gjøre med hvordan etterspørselen i markedet er, som har gjort at det har vært vanskeligere for de eksisterende organisasjonene å holde på den, og dermed har vi fått høyere konsulentbruk enn vi la til grunn. Så har vi fortsatt styrt det på ramme, mot mål, og vi har klart å gjennomføre det totalt sett. Derfor er det vanskelig for meg å si hva som egentlig er effekten av den vridningen. Det klarer jeg ikke å si entydig. Jeg bare prøver å beskrive litt hvilke mekanismer som har eksistert i den styringen.

Bjørn Arild Gram: Jeg vil bare presisere litt i mitt siste svar til Leirtrø. Det var rett det jeg sa om at vi nå samler for ugradert og skjermingsverdig ugradert i den nye etaten DIO. Samtidig har vi etablert Statens graderte plattformtjenester som en etat under Forsvarsdepartementet, som da håndterer gradert informasjon, altså Nasjonalt begrenset nett og Nasjonalt hemmelig nett, som da skal levere den type løsninger til totalforsvaret.

Møtelederen: Fint. Da har jeg tegnet meg selv, og først til en kort oppklaring: I brevet fra Tung og i svaret fra Gram sies det at denne KS2-rapporten anbefaler å se på det å bygge på DSS-elementer som et alternativ. Men det kan vel ikke leses som en anbefaling, som vel var det Gjelsvik sa, at KS2-rapporten direkte anbefalte det. Nå ligger den KS2-rapporten åpent, så det går sikkert an å sjekke, men jeg bare lurer på om det kan presiseres over bordet. Var det en anbefaling om å se på alternativer, eller var det en anbefaling om faktisk å gå for DSS-komponenter?

Bjørn Arlid Gram: Jeg tar ikke ordlyden helt igjen, men det var, skal vi si, en anbefaling om å vurdere. Dette var alternativer til bare å kjøpe det i markedet, men når vi hadde dem selv, og høsten 2022 delvis hadde kjøpt inn og oppgradert de løsningene vi hadde i Depnet/U, ba ekstern kvalitetssikrer programmet om å vurdere det. Det ble gjort, og en konkluderte med at det kunne være en farbar vei å gå videre. Så kom dataangrepet, og da var det ikke lenger aktuelt.

Møtelederen: Da forstår jeg at de ba dere vurdere det, men at det ikke var en direkte anbefaling. Dette bare for å forstå.

Bjørn Arild Gram: Jeg klarer ikke å ta igjen ordlyden noe mer.

Sigbjørn Gjelsvik: Eg støttar det som Gram seier her, at det var tilråding om å vurdere det. Det kom frå ekstern kvalitetssikrar. I utgangspunktet låg ikkje det inne i arbeidet med prosjektet på det tidspunktet, men det var eit element som kom frå ekstern kvalitetssikrar, og som i etterkant av det vart vurdert vidare av prosjektet.

Møtelederen: Det skjønner jeg, takk. Det var egentlig til oppklaring.

Jeg kommer tilbake til avgjørelsen, altså før hackerangrepet, om å skifte målbilde, som det heter, fra FD-system til et nytt system basert på DSS-komponenter. Idet den avgjørelsen tas og forankres på politisk nivå i regjeringen, sitter dere med et rimelig godt kostnadsoverslag over de to ulike alternativene? Vil du, Gram, si med sikkerhet at dere mente at FD-systemet ville være både dyrere i tillegg til å være litt mindre fleksibelt, som det er blitt pekt på?

Bjørn Arild Gram: Ja, det var den klare faglige vurderingen og anbefalingen. Om vi satt med konkrete tall? Det ble jo lagt fram senere, for man måtte ferdigstille et forprosjekt. Man måtte ha det kvalitetssikret, og det måtte gjennomføres ekstern kvalitetssikring, noe det ikke var grunnlag for da vi gjorde det valget. Det kom våren, altså første halvår, 2022, og det var i november/desember vi la det fram for Stortinget. Det var først da, etter mange års arbeid, kostnadsrammen ble fastsatt.

Møtelederen: Det står i svaret fra Tung også at en av uhensiktsmessighetene med FD-systemet nettopp var den veldig høye og for så vidt veldig gode sikkerheten, som gjør at man får en del tilpasningsproblemer med apper og slikt. For meg virker det som at man egentlig tar en kalkulert vurdering av at vi har et kjempegodt system sikkerhetsmessig, som i dag brukes operativt av SMK, og det brukes av FD i det daglige arbeidet i regjering, men man ønsker ikke – eller vil ikke – at dette skal brukes i det bredere departementslivet, rett og slett fordi man ønsker mer fleksibilitet. Ergo: Man ønsker å gå ned på sikkerheten i bytte mot mer brukervennlighet.

Et sikkerhetsbrudd kan være dyrt, og nå ser vi kostnaden. Var det 350-ish mill. kroner man estimerte bare kostnadene av hackerangrepet, isolert sett, til? Det får meg til å spørre om sikkerhetsvurderingene på dette tidspunktet. Jeg skal være veldig tydelig. I brevet fra Tung står det om denne vurderingen: «Det ble heller ikke gjort noen særskilte sikkerhetsvurderinger og risikoanalyser utover de vurderingene og analysene som DSS har gjort selv.»

Det stemmer? Man gjorde ikke vurderinger av Norges regjerings saksbehandlingssystem i den tiden vi er inne i nå – at det burde gjøres en særskilt vurdering av hackerisikoen og de potensielle omkostningene økonomisk og sikkerhetsmessig ved et hackerangrep? Slike vurderinger ble ikke gjort i den avgjørelsen om å gå vekk fra FD og over på DSS-systemet?

Bjørn Arild Gram: Jeg vet ikke om det er helt presis måte å si det på, i det svaret som er gitt, men det kan man jo spørre statsråd Tung om. Det er klart det er gjort sikkerhetsvurderinger. Informasjonen man skal sikre, har veldig forskjellig verdi. Poenget er å få rett sikkerhetsnivå på rett type informasjon. Det er det dette arbeidet har handlet om – og så skal det faktisk være mulig å bruke det på en hensiktsmessig måte. Det er klart at det var de vurderingene vi satt i. Mens disse vurderingene pågikk videre, hvor vi skulle vurdere å ta inn elementer fra Depnet/U, ble det i den perioden gjort inntrengningstesting av Nasjonal sikkerhetsmyndighet, med gode tilbakemeldinger. Vi oppgraderte i den perioden de systemene det kunne være aktuelt å gjenbruke noe fra. Systemene skulle, når vi var ferdige med løsningen, godkjennes av Nasjonal sikkerhetsmyndighet, og som sagt: Den graderte informasjonen skulle beholdes på Forsvarsdepartementets plattformer.

Møtelederen: Da går vi videre til Audun Lysbakken.

Audun Lysbakken (SV): Jeg har et siste spørsmål knyttet til konsulentbruken, for DSS tok i forrige bolk ansvar for at det ikke hadde vært god nok kontroll når det gjaldt avtalen for 2022–2024, med et tak på 600 mill. kr for IT-konsulenter. Men det politiske ansvaret ligger hos regjeringen, og da er det naturlig å spørre – gitt at dette med konsulentbruk var et så sentralt mål for regjeringen og en sentral sak for Senterpartiet, prisverdig nok: Har ikke regjeringen hatt for dårlig kontroll med rutinene når DSS kan havne i den situasjonen at det brukes langt mer penger enn forutsatt, og at man fortsetter å hente inn konsulenter til tross for at anskaffelsesregelverket er brutt?

Sigbjørn Gjelsvik: Lat meg svare på det. Eg kan svare for den perioden som eg var statsråd, og det som skjedde i den perioden. Eg har forsøkt å gjere greie for både dei totale kostnadene i prosjektet og knytt til konsulentbruk i den perioden. Så har det kome ting i etterkant av det, der eg nesten må vise til statsråd Tung og late henne svare på konsulentbruken som har vore, og det som har kome frå DSS si side.

Audun Lysbakken (SV): Jeg vil bare utfordre deg, for dette var perioden 2022–2024. Hva gjorde regjeringen for å sikre at en hadde kontroll på konsulentbruken i dette og lignende prosjekter? En skulle tro at det var noe regjeringen hadde tett kontroll med, gitt viktigheten av det politiske målet.

Sigbjørn Gjelsvik: Generelt kan eg seie at når det gjeld konsulentbruk, er det gjevne føringar – ikkje berre til DSS, men til alle etatar. Dei er følgde opp gjennom tildelingsbrev, med ei klar forventing om at ein skal bidra til å redusere konsulentbruk der det er mogleg, og ikkje minst knytt til informasjons- og kommunikasjonstenes-

tene. Mykje av det vi no snakkar om, knytt til konsulenttenester, er av ein litt annan art. Det gjeld meir spesialkompetanse som kanskje er knytt til utvikling òg av IKT-tenester. Det eg kjenner best til frå min periode, er det som var knytt til handtering av dataangrepet, som eg som statsråd var tett og løpande involvert i nær sagt dagleg. Det er ulik karakter av konsulentbruk i ulike periodar òg, så eg har forsøkt etter beste evne å svare for den perioden som eg sit med ansvaret for.

Møtelederen: Vi går videre til Naomi Ichihara Røkkum.

Naomi Ichihara Røkkum (V): Det er åpenbart en vanskelig balansegang mellom brukervennlighet, hackerangrep og sikkerhet. I forbindelse med hackerangrepet og endret målbilde er ikke dette systemer som nødvendigvis er hyllevare, sa noen i dag. Det er også ganske dyrt å bygge noe opp fra bunnen. Det jeg lurer på, er: I hvilken grad har man sett til land som man har sikkerhetssamarbeid med, eller sammenlignbare land, f.eks. nordiske land, og hvilke systemer de har? Det kan jo tenkes at det kan være billigere å anvende noe som allerede eksisterer, og som også kanskje er anvendelig?

Sigbjørn Gjelsvik: Jeg gir ordet til Jan Olav Pettersen.

Jan Olav Pettersen: Takk for det. Som Hermansen var innom, er dette et marked som har vært i utvikling. Og det vi har sett, er at de store selskapene på skyteknologi og datasenter tilpasser løsninger mer og mer til nasjonale sikkerhetskrav. Det vi gjør i Norge, i vårt program, er likt tilsvarende vurderinger som gjøres i andre land. Vi har ulike kjøremiljøer basert på en verdivurdering av informasjonen. Det sikreste kjøremiljøet som gjelder ugradert, er en skjermingsverdig ugradert plattform, slik vi legger opp til. Den skal sikkerhetsgodkjennes, sammen med hele plattformen, av Nasjonal sikkerhetsmyndighet, men hvor vi bruker markedet som har oppdatert informasjon, stordriftsfordeler og erfaring med drift i en helt annen størrelsesorden enn det vi kunne klare å levere.

Møtelederen: Da rekker vi et siste spørsmål fra Frode Jacobsen. Vi er litt på overtid, men jeg tror vi holder tidsrammen.

Frode Jacobsen (A): Takk. Jeg vil litt tilbake til skiftet og vurderingene som ble gjort når en gikk bort fra FD tonivåløsningen. I forbindelse med hva komitélederen spurte om, ble det sagt at det var lite hensiktsmessig å gå videre med den. Kan du si noe om hvilke sikkerhetsvurderinger som ble gjort i den forbindelse? Og når en da valgte en ny løsning, kan du si noe mer om NSMs rolle her? Sikkerhet er jo viktig, og jeg antar at sikkerhet var i høysetet også for dere som statsråder når det gjaldt å finne ny løsning. Ved å gå bort fra FD II la man ikke sikkerheten bort, men ut fra hva Hermansen sa tidligere, var det ikke like hensiktsmessig å legge seg på samme sikkerhetsnivå på hele linja her som man ville gjort på FD II. Var det en vurdering man også fikk faglig støtte til fra NSM?

Bjørn Arild Gram: Det var definitivt faglig anbefalt. I hvor stor grad NSM var inne i vurderingene da, klarer ikke jeg å svare på, men det var forutsatt at NSM skulle godkjenne løsningen til slutt. NSM skulle ha en rolle med tanke på løsningen vi skulle ende med. Det var en prosess – husk at vi gikk inn i et forprosjekt som så skulle kvalitetssikres. Det er mange steg her, og vi var fortsatt ikke der at beslutningen skulle tas. Det ble fremmet for Stortinget et år etterpå, etter at prosessen var tatt videre. Det har skjedd ting etter det igjen, som har gjort at vi har måttet planlegge på nytt.

Sikkerhet har vært et kjernepunkt hele veien. Hovedårsaken til at vi gjør dette, er for å få bedre sikkerhet for informasjonsflyten vår og informasjonen vi har, i tillegg til å kunne greie å drifte departementene på en effektiv måte.

Møtelederen: Da går vi over til siste del av høringen, som er den åpne runden, hvor det er mulighet for de inviterte til 5 minutter hver hvis man ønsker å si noen bevingede ord.

Sigbjørn Gjelsvik: Eg trur vi har fått svart ut ganske godt dei spørsmåla som komiteen har kome med. Hagen hadde nokre spørsmål knytte til konkrete namn, som eg trur Jan Olav Pettersen har noko utfyllande informasjon om, så eg gjev ordet vidare til ham.

Jan Olav Pettersen: Takk for det. Hagen spurte om hvem som har gjennomført de eksterne kvalitetssikringene. Våren 2021 var det konsulentselskapet Metier som gjorde de første vurderingene, basert på rammeavtalen fra Finansdepartementet, som jeg nevnte. Etter det har vi hatt tre kvalitetssikringer: én i april 2022, og to kontrollpunkter i 2023 og 2024. Alle disse kvalitetssikringene har vært gjort av A-2 Norge, Holte Consulting og Menon Economics, som sammen har en rammeavtale med Finansdepartementet.

Jeg har lyst til å si en siste ting. Jeg nevnte at vi hadde en andel på mellom 25 pst. og 30 pst. av interne i programmet, og da snakker jeg om i programmet og i programkontoret. I tillegg har departementene styrt dette programmet tett, og vår tidsbruk er ikke inkludert i den vurderingen. Vi har brukt mye tid på styringen i tillegg til programgjennomføringen.

Sigbjørn Gjelsvik: Eg vil avslutningsvis seie for min eigen del: Det med sikkerheit har gjentekne gonger kome opp. Eg vil understreke at vurderingar av sikkerheit er viktig, og det har òg vore eit viktig grunnlag for at ein ville ha ei ny, felles IKT-plattform – ei moderne plattform som både kan vareta sikkerheit og vere brukarvenleg. Eg vil seie at under den regjeringa som tidlegare statsråd Gram og eg har vore del av, har ein nettopp fått framdrift i det arbeidet. Det er viktig.

Som Gram var inne på, skulle ei ny plattform verte godkjend av NSM. Det er viktig sikkerheit i det, men det er òg viktig at ein sikrar at ho er god og effektiv. Her snakkar ein om ei plattform som det er tusenvis av tilsette i departementa som skal bruke dagleg, og det er snakk om at ein skal kommunisere godt med underliggjande etatar og andre som departementa har å gjere med. Difor er det viktig å finne gode løysingar som varetek ulike behov, og det var nettopp i vurderinga av det at ein gjorde nokre viktige vegval undervegs, som er status på prosjektet slik det er vorte beskrive.

Bjørn Arild Gram: Jeg har bare noen få ord helt til slutt, da jeg føler vi har fått belyst ting på en grei måte. Det har vært litt forvirring i debatten, det hørte jeg også i den første sekvensen. Men vi har vært inne i ulike faser, og vi har tilpasset oss med ny kunnskap og når hendelser har skjedd. Det har for øvrig ligget en fleksibel tilnærming til programmet til grunn, som har gjort det mulig for oss å justere oss inn.

Jeg ser at det nå har blitt gitt karakteristikker av hvordan en skal oppfatte denne saken. Stort sett har vi gjennomført arbeidet som vi har tenkt, med den nødvendige fleksibiliteten, men vi ble rammet av en veldig alvorlig hendelse: dataangrepet. Det er det som har gjort at vi får forsinkelser, og som gjør at det blir dyrere. Ellers har det stort sett blitt styrt i tråd med de effektmålene vi har ønsket å oppnå, og budsjettene som har vært lagt. Det har vært forankret i både regjering og storting. Alt vi har sagt nå, har det blitt informert om. I hvert fall har de ulike fasene og målbildene i programmet blitt framlagt for Stortinget, med kostnadsrammer og uten merknader.

Møtelederen: På vegne av komiteen vil jeg takke de inviterte for at dere tok dere tid til å møte opp og svare på våre spørsmål.

Komiteen tar en pause nå, til kl. 12.30, men jeg ber komiteen sitte igjen litt for å drøfte behovet for lukket høring.

Høringen ble avbrutt kl. 11.58.

Høringen ble gjenopptatt kl. 12.31.

Høring med digitaliserings- og forvaltningsminister Karianne O. Tung og forsvarsminister Tore Onshuus Sandvik

Møtelederen: Da er komiteen klar til å starte opp igjen. Jeg vil få ønske velkommen digitaliserings- og forvaltningsminister Karianne Oldernes Tung. Du har med deg to bisittere. Det er ekspedisjonssjef Jan Olav Pettersen og departementsråd Christine Hamnen. Jeg vil også få ønske velkommen forsvarsminister Tore Onshuus Sandvik, som har med seg som bisitter departementsråd Frede Hermansen. Velkommen til dere alle.

Vi er blitt informert om at dere ønsker å fordele den samlede taletiden litt annerledes enn vanlig, så det blir 12 minutter til digitaliserings- og forvaltningsministeren og 8 minutter til forsvarsministeren. Det er i den skjønneste orden for komiteen.

Dere kjenner opplegget, men for ordens skyld: Etter innledningene starter en utspørring fra komiteen hvor saksordføreren får 10 minutter, deretter får hver partigruppe 5 minutter til sine spørsmål, og så blir det en åpen runde på slutten med oppklarende spørsmål. Helt til slutt blir det mulighet for de inviterte til en oppsummering.

Jeg minner for ordens skyld om at dette er en åpen høring. Hvis det skulle være behov for å si ting som er gradert eller underlagt taushetsplikt, må det gjøres i lukket rom, så da må dere gi beskjed om det.

Da tror jeg vi går rett på sak og gir ordet til digitaliserings- og forvaltningsminister Karianne Tung, som har 12 minutter til sin innledning. Vær så god!

Statsråd Karianne O. Tung: Tusen takk for det, leder.

Jeg tiltrådte som digitaliserings- og forvaltningsminister i oktober 2023. Tidligere statsråder Bjørn Arild Gram og Sigbjørn Gjelsvik har redegjort for sine statsrådsperioder.

Jeg vil i mitt innlegg fokusere på tre problemstillinger:

1. Hva er målet for programmet, og hva er det vi ønsker å oppnå?
2. Hvordan har programmet vært styrt?
3. Hvorfor er kostnadsrammen endret?

Først til programmets målbilde: La meg starte med å si hvorfor vi har satt i gang program for felles IKT-tjenester i departementsfellesskapet. Programmet skal sørge for å oppnå to overordnede ting, for det første en ny, sikker og moderne IKT-plattform for Statsministerens kontor, alle departementene, Norges utenriksstasjoner, Departementenes digitaliseringsorganisjon, DIO, og Departementenes sikkerhets- og serviceorganisasjon, DSS.

For det andre skal man etablere en ny, felles organisasjon som samler IKT-kompetansen i departementene.

Gjennom dette arbeidet vil vi kunne balansere hensynene til sikkerhet og kraften som ligger i moderne digitale verktøy på en ny måte. Fram til nå har departementene hatt fire ulike IKT-organisasjoner med fire helt separate IKT-plattformer. Det er verken effektivt eller økonomisk, men det er først og fremst ikke sikkert nok. Ved å samle disse plattformene sikrer man en trygg og moderne digital plattform mellom departementene.

Programmet har eksistert over flere år, men fram til 2021 var arbeidet preget av interne uenigheter og lite framgang. Etter 2021 har vi hatt stram styring, og det har blitt oppnådd to viktige milepæler i prosjektet. Det første er at vi har etablert en ny virksomhet som samler de tidligere IKT-miljøene. Det skjedde 1. januar 2025, da Departementenes digitaliseringsorganisasjon, DIO, ble etablert. DIO, sammen med Statens graderte plattformtjenester, som er underlagt Forsvarsdepartementet, er departementsfellesskapets leverandører av henholdsvis ugraderte, ugraderte skjermingsverdige og graderte IKT-tjenester.

Vi jobber nå med å ferdigstille den andre delen, nemlig å etablere en ny, felles IKT-plattform. Her ligger vi godt an i henhold til den framdriften Stortinget er informert om, og som ble lagt etter dataangrepet sommeren 2023. Komiteens skriftlige spørsmål, som jeg har besvart i fire brev, dreier seg i all hovedsak om dette.

Så til styringen av programmet. Som jeg har skrevet i svarbrevene til komiteen, har jeg vært opptatt av å styre programmet stramt. Jeg har sørget for forankring i regjering ved viktige stoppunkt. Programmets målbilde for å etablere en felles IKT-plattform for departementsfellesskapet har blitt justert underveis. Dette er nettopp en konsekvens av at vi har styrt og fulgt programmet tett. Endringene skyldes særlig et alvorlig dataangrep, anbefalinger fra ekstern kvalitetssikrer og endrede teknologiske forutsetninger. Regjeringen har vært opptatt av å holde Stortinget godt informert underveis om endringene som har skjedd i programmet.

En viktig forutsetning for å lykkes i dette arbeidet har vært arbeidet i programstyret. Styret består av den administrative toppledelsen i de sentrale departementene og etatene som er involvert. Embetsverket i Forsvarsdepartementet og Digitaliserings- og forvaltningsdepartementet har ukentlig kontakt med ledelsen i programmet. Det er ikke vanlig at departementene er så tett på et prosjekt som de er i dette programmet. Dels skyldes det den store betydningen av å bedre sikkerheten og effektiviteten i digital samhandling, som skal understøtte regjeringens og departementenes arbeid, og dels tilsier erfaringene fra enkelte tidligere digitaliseringsprosjekter at sånne prosjekter nettopp trenger tett og god ledelse for å lykkes. Jeg vil derfor avvise påstandene om at programmet ikke er godt styrt. At det er styrt av konsulenter, som noen hevder, er ikke riktig.

I departementenes styring av programmet har vi hatt stor nytte av at ekstern kvalitetssikrer har fulgt programmet tett, først gjennom en KS2 av programmets forprosjekt og styringsdokumentasjon. Dette var grunnlaget for at regjeringen i 2022 kunne gå til Stortinget med et forslag om å starte programmet med en tilhørende kostnadsramme. Etter dette har det vært gjennomført to kontrollpunkter for å kvalitetssikre sentrale beslutninger og endringer som er gjort underveis. Vi planlegger nå et tredje kontrollpunkt i løpet av neste år.

Til sist til endringer i kostnadsrammen: I Digitaliserings- og forvaltningsdepartementets og Forsvarsdepartementets Prop. 1 S for 2024–2025 redegjorde vi for situasjonen etter dataangrepet, hvilke nye vurderinger som var gjort, og forslag til økt kostnadsramme for programmet. I forbindelse med behandlingen av Innst. 7 S for 2024–2025 vedtok Stortinget den nye kostnadsrammen på om lag 2,2 mrd. kr. Komiteen hadde ingen merknader.

Dette er en vesentlig økning fra den opprinnelige kostnadsrammen, men kvalitetssikreren vurderer fortsatt at gjennomføring av programmet er samfunnsøkonomisk lønnsomt. Kvalitetssikreren støtter videreføring av programmet uten vesentlige endringer. Denne prosessen er for øvrig i tråd med statens prosjektmodell, og endelig beslutning var forankret i Stortinget.

La meg nå redegjøre for de endringene som fulgte etter dataangrepet sommeren 2023. Før dataangrepet var planen å bygge en ny, felles IKT-plattform med gjenbruk av enkelte komponenter fra plattformen Depnet/U. Basert på sikkerhetsvurderinger av Depnet/U fra først og fremst Nasjonal sikkerhetsmyndighet konkluderte Digitaliserings- og forvaltningsdepartementet og Forsvarsdepartementet til slutt med at tilliten til aktuelle komponenter var svekket og ikke lenger egnet til gjenbruk. Prosessen fram til da har tidligere statsråder Gram og Gjelsvik redegjort for.

Et nytt målbilde ble derfor utredet basert på de endrede forutsetningene etter angrepet. Beslutningen om nytt målbilde var forankret i regjeringen, på samme måte som andre viktige veivalg i prosjektet. Det nye målbildet etter dataangrepet er å etablere en ny, felles IKT-plattform gjennom anskaffelse i markedet. Den nye plattformen vil være en hybrid løsning, hvor det etableres tre kjøremiljøer. En hybrid løsning vil si at det etableres ulike kjøremiljøer for behandling av informasjon med ulike verdier: ett kjøremiljø for behandling av ugradert skjermingsverdig informasjon, ett kjøremiljø for behandling av ugradert informasjon og ett kjøremiljø for behandling av ugradert informasjon i offentlige

skytjenester. Det er viktig å understreke at alle kjøremiljøene skal samles i den nye virksomheten, DIO.

Det er viktig at departementenes verdier sikres på riktig nivå, og at vi ikke skaper begrensninger for oss selv gjennom et unødvendig høyt sikkerhetsnivå. Det er nettopp dette ny, felles IKT-plattform vil gi oss. De ulike sikkerhetsnivåene gjør at vi kan sikre verdiene på en hensiktsmessig måte, samtidig som vi får tilgang til effektive og moderne digitale verktøy.

Regjeringen har lagt til grunn at Nasjonal sikkerhetsmyndighet skal sikkerhetsgodkjenne kjøremiljøet for behandling av ugradert skjermingsverdig informasjon. For at kjøremiljøet skal kunne sikkerhetsgodkjennes, er det mange sikkerhetskrav som må oppfylles. Blant annet må løsningene leveres fra et datasenter med høy grad av nasjonal kontroll av personell og infrastruktur.

Vi har sørget for at programmet og Nasjonal sikkerhetsmyndighet jobber tett sammen i denne prosessen. Når kjøremiljøet for behandling av ugradert skjermingsverdig informasjon blir sikkerhetsgodkjent, vil det være et stort framskritt. Det vil være første gang et kjøremiljø for behandling av ugradert skjermingsverdig informasjon blir formelt godkjent av Nasjonal sikkerhetsmyndighet. Erfaringene fra dette arbeidet vil være en pilot for arbeidet med nasjonal sky.

Kjøremiljøene for behandling av ugradert informasjon vil beskyttes i tråd med beste praksis. Det er ikke behov for å beskytte ugradert informasjon på like høyt nivå som for ugradert skjermingsverdig informasjon.

Etableringen av ny, felles IKT-plattform, med tre kjøremiljøer for behandling av informasjon med ulik verdi, vil bidra til sikker og effektiv informasjonsforvaltning i departementsfelleskapet. Dette vil gi oss bedre forutsetninger for å kunne håndtere stadig mer komplekse problemstillinger, som krever effektiv samhandling på tvers av sektorer.

Når ny, felles IKT-plattform er ferdig etablert, vil vi starte å teste og overføre data og applikasjoner fra dagens IKT-plattformer til én ny plattform. Dette vil skje gradvis og planlegges gjennomført i løpet av 2026. Deretter starter arbeidet med å fase ut gamle plattformer og avslutte programmet. Etter planen skal det hele være ferdig i løpet av 2027.

Forsvarsminister Sandvik vil i sitt innlegg redegjøre nærmere for status og veien videre for programmet. Jeg avslutter med dette min innledning.

Møtelederen: Tusen takk for det. Du trengte ikke engang tidsjustering, det var godt levert på tid!

Forsvarsminister Sandvik, du kan fortsette med dine tildelte minutter.

Statsråd Tore Onshuus Sandvik: Takk for det, leder.

Jeg tiltrådte som forsvarsminister i februar i år, så mitt ansvar for program for felles IKT-tjenester i departementsfellesskapet, heretter kalt programmet, er ganske avgrenset i tid. Det har derfor vært naturlig at statsråd Karianne Tung står for den mest omfattende redegjørelsen.

Tung har nettopp redegjort for endringer i målbildet, styringen av programmet og endringer i kostnadsrammen. Jeg kan supplere med status for programmets arbeid per mai 2025 og veien videre for programmet.

Programmet har avsluttet sitt arbeid med etableringen av Departementenes digitaliseringsorganisasjon, DIO. Vi er i disse dager i dialog med markedet for kjøp og implementering av den nye plattformen. Basert på denne dialogen vil vi gjennom direktøren i DIO inngå økonomisk og juridisk bindende kontrakter for kjøp og implementering av en ny, felles, sikker, kostnadseffektiv og moderne IKT-plattform.

Etter planen skal det inngås tre kontrakter før sommeren: en kontrakt for støtte til overgang og utfasing av gamle løsninger, en kontrakt for etablering av den nye, felles IKT-plattformen og en kontrakt for en fellesavtale for bruk av allmenne skytjenester. Etter kontraktsinngåelse vil programmet starte selve etableringen av den nye plattformen. Etter at plattformen er etablert, vil vi starte arbeidet med å teste plattformen og overføre data og applikasjoner fra de eksisterende plattformene til den nye. Dette blir en trinnvis prosess før de gamle plattformene kan fases ut.

I januar i år ble Statens graderte plattformtjenester opprettet som etat under Forsvarsdepartementet. Formålet til virksomheten er å tilby og videreutvikle nasjonale fellestjenester for best mulig gradert digital samhandling for virksomheter underlagt sikkerhetsloven, for å ivareta nasjonale sikkerhetsinteresser. Virksomheten har ansvar for å levere både nasjonal begrenset plattform og nasjonal hemmelig plattform. Statens graderte plattformtjenester vil sammen med DIO levere digitale plattformer og tjenester til departementsfellesskapet på ugradert og gradert nivå.

Det er uvanlig at to statsråder deler ansvar for et stort prosjekt, her organisert som et program. Jeg vil understreke at det i min periode som forsvarsminister har vært et godt og tett samarbeid mellom Digitaliserings- og forvaltningsdepartementet og Forsvarsdepartementet i den felles styringen av programmet. Nå er programmet i en ny fase, en gjennomføringsfase, hvor vi skal anskaffe og etablere den nye, felles IKT-plattformen som skal overtas og forvaltes av DIO. På bakgrunn av dette er digitaliserings- og forvaltningsministeren og jeg enige om å foreslå overfor Stortinget å overføre hele ansvaret for eierstyringen og oppfølgingen av programmet, inkludert budsjettmidlene til programmet, fra Forsvarsde-

partementet til Digitaliserings- og forvaltningsdepartementet.

Basert på anbefalinger fra ekstern kvalitetssikrer vil Digitaliserings- og forvaltningsdepartementet plassere ansvaret organisatorisk inn i DIO. Dette er for å sørge for at programmets leveranser er tett integrert i DIO, som skal overta og drifte den nye plattformen.

Med dette avslutter jeg min korte innledning.

Møtelederen: Tusen takk for det.

Da går vi videre til komiteens utspørring, og vi starter med 10 minutters spørsmål fra saksordføreren, som i denne anledning er meg selv.

Jeg starter med et spørsmål til statsråd Tung. Det gjelder den saken som sto i Aftenposten om at navnene på dem som har jobbet med dette prosjektet, har kommet på avveier. Stemmer det for det første at disse navnene er gradert?

Statsråd Karianne O. Tung: Ved en feil i saksbehandlingsrutinene i Statsbygg ble dokumentene dessverre ført feil. Så raskt den feilen ble oppdaget, fjernet man disse dokumentene fra postlisten. Man har nå gått gjennom retningslinjene i Statsbygg for å sørge for at det ikke skal skje.

Møtelederen: Er det statsrådens vurdering at dette kan være et lovbrudd?

Statsråd Karianne O. Tung: Her vil jeg be ekspedisjonssjef Jan Olav Pettersen svare.

Jan Olav Pettersen: Vår vurdering så langt er at dette ikke er noe lovbrudd. Det er jo sånn at vi har mange lag med sikkerhet. Her var det informasjon om ansatte som kom på avveier, men vi har mange lag. Det betyr at det ikke innebærer at det har hatt vesentlig skade når ett av disse lagene brytes.

Møtelederen: Takk.

Da fortsetter jeg å spørre statsråd Tung: Kan dette si oss noe om en sikkerhetskultur i prosjektet?

Statsråd Karianne O. Tung: Nei, dette vil jeg ikke si er et eksempel som generelt beskriver sikkerheten i prosjektet. Programmet for felles IKT har vært gjennom mange sikkerhetsvurderinger i flere ledd, både som følge av dataangrepet, selvfølgelig, og ikke minst endret målbilde, og også den endrede teknologiske utviklingen. Den går veldig fort nå, og det gjør f.eks. at man vurderer skytjenester annerledes i dag enn man gjorde for 5–10 år siden.

Møtelederen: Vi skal litt over til nettopp sikkerhetsvurderingene som ble gjort rundt skifte av målbilde, som det heter, og da før hackerangrepet – altså når man går vekk fra den tidligere planen om FD II-nivå og over til et system med elementer fra DSS, det jeg tidligere har beskrevet at ser ut som en reversering eller iallfall delvis en snuoperasjon.

Jeg vet at du ikke var utnevnt som statsråd på det tidspunktet, statsråd Tung, men du har skrevet til komiteen i et av brevene – vi har jo skrevet en del brev fram og tilbake – om denne avgjørelsen at «[d]et ble heller ikke gjort noen særskilte sikkerhetsvurderinger og risikoanalyser» på dette tidspunktet. Her sitter man altså og vurderer regjeringens saksbehandlingssystem i en tilspisset situasjon, med risiko for bl.a. hacking fra fremmede makter. Burde ikke sikkerhet være topp prioritet når man skal avgjøre retningsvalg for saksbehandlingssystemet til regjeringen?

Statsråd Karianne O. Tung: Jeg er helt enig med lederen i at sikkerhet bør settes i høysetet, og det har vært hovedmålet til programmet hele veien, nettopp fordi man har hatt fire ulike miljøer og i det vurdert sikkerhetsrisikoen som for høy. Det er krevende å drifte disse fire ulike miljøene som skal levere hver sine IKT-plattformer, og det er noe av hovedbegrunnelsen for at man ønsker å opprette den felles IKT-plattformen, og også samle de IKT-ansatte i en felles organisasjon – nettopp for å styrke sikkerheten og kompetansen.

Som det har blitt sagt tidligere i høringen også, har man først hatt et målbilde hvor man som prinsippbeslutning hadde FDs tonivåplattform som utgangspunkt. Underveis så man – som Hermansen redegjorde for i den forrige bolken – at det ble ineffektivt og for krevende. Når en nesten skal løfte nærmere 500 ulike applikasjoner, og alt fra utenrikstjenestens og Finansdepartementets til alle andres ulike applikasjoner skulle over på FDs plattform, ble det for krevende og krevde for mye spesialsøm, som potensielt også kunne ha ført til mye høyere kostnader enn det som etter hvert ble rammen.

Så endret man jo det målbildet. Man gikk fra FDs tonivåplattform mot høsten 2021 og tok en beslutning om å gå til privat lukket sky. Man arbeidet så med forprosjektet og gjorde det klart for ekstern kvalitetssikring våren 2022. I den kvalitetssikringen anbefalte ekstern kvalitetssikrer også å vurdere gjenbruk av komponenter fra Depnet/U. På den tiden, i 2022, foretok NSM en penetrasjonstest, eller inntrengingstest, av Depnet/Us komponenter for å sjekke om det var godt nok. NSMs vurdering var at disse komponentene var mulige å gjenbruke, hvilket førte til at DSS da gjorde ytterligere investeringer i sin plattform for nettopp å gjøre gjenbruken av de komponentene så sikker som mulig. Det gjorde at man igjen endret målbildet: først fra FDs tonivåplattform til privat lukket sky, og deretter til å ha privat lukket sky, men også med gjenbruk av komponenter fra Depnet/U. Det skulle

man jo informere Stortinget om i Prop. 1 S for 2022–2023, etter et eksternt kontrollpunkt, som også hadde gått gjennom ekstern kvalitetssikrer, men da kom dataangrepet, som gjorde at Depnet/Us plattform ble kompromittert.

Møtelederen: Jeg skal bare spørre om en presisering. Vi må litt tilbake til det første spørsmålet, som gikk på dette med de som jobber i prosjektet. Det første spørsmålet mitt var om navnene var gradert. Veldig enkelt: Var det gradert informasjon? Jeg tenker da på navnene på dem som jobber i prosjektet, som ble publisert av staten selv.

Jan Olav Pettersen: Vi ønsket ikke å gå ut med den informasjonen. Hvorvidt det var gradert, er jeg ikke sikker på, men vi ønsket ikke å gå ut med den informasjonen.

Møtelederen: Det var derfor jeg spurte nå – rett og slett med tanke på om det var et lovbrudd eller ikke. Det ville fort vært et lovbrudd hvis det var gradert. Det var egentlig bare for presisering eller oppklaring.

Jan Olav Pettersen: Min forståelse er at det i seg selv ikke var gradert, reelt sett, men det må vi eventuelt dobbeltsjekke.

Møtelederen: Ok, takk. Det var bare til oppklaring.

Jeg har lyst til å snakke om etatene og det arbeidet som er gjort i opprettelsen av dem. Det er jo blitt store organisasjoner, med mye penger som har gått med, og vi har sett i brevene vi har fått, at det er mye som er etablert. Jeg bare lister opp: egen administrasjon, regnskap, IKT-løsninger, profil, kultur, nye lokaler med tidsriktig arbeidsplassdesign, mye som går til utredninger og tilrettelegging, prosjekthåndbok med rutiner og retningslinjer, utvikling av styrende dokumentasjon og fasilitering for KS2 og kontrollpunkt, utarbeidelse av samfunnsøkonomiske analyser, kost-nytte-analyser, usikkerhetsanalyser, dokumentasjon for programstyret, økonomioppfølging og -analyser, kommunikasjonsplaner og rekruttering av ressurser – det antar jeg betyr ansatte eller mennesker, hvis jeg forstår det riktig. Det er store organisasjoner vi snakker om her, og mye midler, men vi har fortsatt ikke noe IKT-prosjekt. Det virker egentlig som vi ble satt kraftig tilbake på grunn av denne skjebnesvangre situasjonen med at systemet ikke tålte hackerangrep.

For å gjøre en lang historie kort: Kan dere garantere at vi er «on time», og at vi kommer til å få et saksbehandlingssystem i tråd med rammene og tidsplanen?

Statsråd Karianne O. Tung: Jeg er ikke enig i premisset om at det ikke har skjedd noe som helst. For det første har vi fra 1. januar 2025 fått på plass DIO, som lederen redegjør godt for hva krever av kapasitet. Den ene hovedleveransen i prosjektet er nå på plass med etablering av DIO. Vi jobber nå med kontraktinngåelse for levering av selve IKT-plattformen, som skjer omtrent i disse tider, fra mai og juni og utover. Vi har informert Stortinget, og Stortinget har fattet beslutning om en kostnadsramme på 2,2 mrd. kr, hvor vi nå skal gjennomføre programmet med mål om å være ferdig i 2027. Det er ingen grunn til å tro at vi ikke skal klare det.

Møtelederen: Da skal jeg bare presisere at jeg absolutt ikke antydet at det ikke var gjort ting. Tvert imot, det er en lang liste over ting som er etablert, men det er altså fraværet av et IKT-system og saksbehandlingssystem som er bekymringen. Da oppfatter jeg at ting er «on time», og at det er innenfor rammene. Jeg skal ikke spørre om en garanti – jeg vet at rutinerte politikere ikke gir det – men jeg leser det som at det er en forsikring, i alle fall, om at ting er i rute.

Statsråd Karianne O. Tung: Prosjektet, eller programmet, styres stramt med flere kontrollpunkt. Vi har nå gjennomført to av de tre kontrollpunktene for endringstrinnene som er i gang, og vi er i gjennomføringsfasen. Som sagt skal det straks signeres tre nye kontrakter for å starte arbeidet med programmet, og det er ingenting som tyder på at vi ikke skal rekke det.

Når det er sagt, er det et komplekst program som krever mye ressurser og mye innsats, men med DIO på plass og etablert, med det som leveranse, er vi i rute i henhold til det som Stortinget er informert om. Så er det som forsvarsminister Sandvik er inne på: Vi legger nå opp til gjennom RNB å overføre programmet til DFD i sin helhet som en del av gjennomføringsfasen.

Møtelederen: Tusen takk. Da er det Arbeiderpartiet og Frode Jacobsen, som har 5 minutter.

Frode Jacobsen (A): Takk skal du ha. Du var inne på det i din innledning også, Tung, men kunne du utdypet litt mer om organisering? Det har også vært et tema gjennom de tidligere rundene vi har hatt i dag. Hvor er det beslutninger tas? Noe har vi hørt at tas på regjeringsnivå, og noe tas antakeligvis på administrativt nivå i departementene. Vi hører om et programstyre. Kunne du sagt litt mer om hvem disse i programstyret er, og også hvordan dere som statsråder er tett på de beslutningene? Og hva slags beslutningsgrunnlag er det dere får til de beslutningene som skal tas?

Statsråd Karianne O. Tung: Det kan jeg redegjøre for.

Det er etablert som et program med en styringsmodell, og programmet har også fullmakter etter statens

prosjektmodell. Viktige prinsippbeslutninger blir løftet opp til regjeringen, hvor regjeringen også informerer Stortinget, sånn som vi har gjort i fasene fra 2021. Programmet har jo eiere, og det er i dag DFD og Forsvarsdepartementet som er eiere av programmet. Derfor – jeg må bare presisere det også – er svarbrevet som har gått til komiteen, fra både DFD og Forsvarsdepartementet. DFD og FD er programeiere. Så har man et programstyre som består av miljøene fra de andre departementene som skal slås sammen. Det består altså av toppledelsen fra UD, og Justisdepartementet er med. Vi har også DSS, som nevnt, og DIO er med. I tillegg ble SMK med i programstyret fra 2023.

Som Hermansen redegjorde for tidligere: Det er ulike faser i beslutningsprosessen. Det er både drøftingsfase og beslutningsfase. Når beslutningene blir fattet, kommer de opp i linjen til eierdepartementene for videre beslutning, hvor vi som konstitusjonelt ansvarlige statsråder fatter de beslutningene og løfter de prinsipielle beslutningene opp til regjeringen ved behov. Vi informerer også Stortinget om viktige beslutninger, som kostnadsramme, styringsramme og endret målbilde, sånn som vi har gjort.

Kanskje kan Frede Hermansen utdype.

Frede Hermansen: Det er kanskje ikke så mye å legge til, men jeg vil understreke det som jeg var innom i forrige del, når det gjelder hvem som sitter i programstyret. Det er representanter fra ledelsen på det tilsvarende nivået fra Utenriksdepartementet, Justisdepartementet og Statsministerens kontor. Litt av poenget er nettopp at det bredder ut det totale behovet, og det treffer også betydelige deler av de sentrale prosessene. Poenget er, som jeg fortalte i stad, med tanke på stegene fra informasjon og drøfting til beslutning, at alle beslutninger blir gjennomdrøftet for å sørge for at vi ivaretar alle aspekter og hensyn, slik at vi skal få en gjennomgående, god løsning. Det vil alltid være uenigheter internt i de enkelte departementene, men nettopp derfor har vi sørget for at det er virksomhetsledelsen i det enkelte departement som til syvende og sist støtter eller eventuelt er uenig i de beslutningene når de løftes videre.

Frode Jacobsen (A): Da vil jeg gå inn på valget om å gå bort fra FDs tonivåløsning, som i og for seg skjedde før begge dere ble statsråder, men som likevel har vært et viktig tema her. Er det da slik å forstå at den eksterne kvalitetssikreren har gitt råd om at man ikke burde gå videre med den løsningen, men heller gå videre med noe annet? Er det slik at det drøftes i programstyret, hvor SMK, UD, FD, DSS – alle – er til stede, så blir man enig om dette, og så jobber man videre ut fra det? Tas det en beslutning noe sted om det?

Statsråd Karianne O. Tung: For å starte må jeg bare presisere at beslutningen om å gå bort fra FDs tonivåplattform ble tatt i løpet av 2021 i arbeidet etter at den første eksterne kvalitetssikringen ble avvist på grunn av for dårlig grunnlag. Da gikk man i utgangspunktet til den eksterne kvalitetssikringen med FDs tonivåplattform, men i arbeidet etterpå endret man målbildet og ønsket å benytte en privat lukket sky. Det arbeidet skjer i programstyret og av programeierne – litt det som Hermansen redegjorde for i forrige bolk, om begrunnelsen for hvorfor man ønsket å gå over til privat lukket sky i stedet.

Statsråd Tore Onshuus Sandvik: Jeg vet ikke om departementsråden kan utdype dette. Dette har også noe å gjøre med at sikkerhetsnivået i Forsvarsdepartement er høyere enn det som kreves for å drive normal forvaltningsdrift, og det ville medført store begrensninger.

Frede Hermansen: Jeg kan gå litt tilbake til det elementet hvor den eksterne kvalitetssikreren mente at beslutningsdokumentasjonen ikke var grundig og god nok. Det var et signal om at vi ikke hadde jobbet tungt nok med løsningen, og redegjort og vurdert tungt nok. Den eksterne kvalitetssikringen og starten på den, som egentlig ble anbefalt stoppet av en ekstern leverandør, var egentlig startskuddet for å begynne å vurdere om dette var en riktig vei videre. Så det var der vridningen mot en privat sky istedenfor FDs tonivåplattform egentlig startet.

For saken kan det også nevnes at vi egentlig av samme årsaker nå vil avvikle FDs tonivåplattform i den formen – nettopp av de samme årsakene. De andre brukerne som er på plattformen i dag, eksempelvis SMK og NSM, vil også gå vekk fra den av samme årsaker som vi vurderte tilbake i 2021.

Møtelederen: Da går vi videre til neste spørrer, Eivind Drivenes fra Senterpartiet.

Eivind Drivenes (Sp): Nå er vi kommet langt ut i debatten og langt ut i spørsmålsrekken, så mye er allerede spurt om. Jeg har lyst til å stille et spørsmål til statsråd Tung: Er det noe du ville gjort annerledes i prosessen etter at du overtok? Du har vært med i en avgjørende fase i prosjektet.

Statsråd Karianne O. Tung: Takk for spørsmålet.

Nei, slik jeg ser det, er det ingenting vi kunne gjort annerledes i min tid fra da jeg tiltrådte i oktober 2023. Da jeg tiltrådte som digitaliserings- og forvaltningsminister i oktober 2023, var dataangrepet som hadde blitt utført av en veldig avansert aktør, nettopp skjedd. Man var midt i et arbeid med å vurdere handlingsalternativ-

ene, man hadde akkurat iverksatt en rekke tiltak for å prøve å minske sårbarhetene som følge av angrepet, man hadde stengt ned e-postserverne, man hadde gjort om saksbehandlingsrutinene, slik at mer av saksbehandlingen foregikk på begrenset nett, og man vurderte hvilke alternativer man hadde i det videre arbeidet med felles IKT-plattform. Det ble også redegjort for i proposisjonen til Stortinget høsten 2023 at man ønsket å vurdere de ulike alternativene for å se hva som var mulig.

Det ble gjort en sikkerhetsvurdering av Depnet/U-plattformen etter angrepet for å se på om det var mulig å gjenbruke noen av komponentene. Da konkluderte man med at man ikke hadde tillit til Depnet/U-plattformen, som gjorde at man gikk bort fra det. Man måtte igjen replanlegge programmet og målbildet, og kom fram til at man ønsket å gå for en løsning i markedet, som også gikk gjennom en ekstern kvalitetssikring for å sørge for at man gjorde riktige vurderinger, før man på nytt fremmet forslag for Stortinget om endret målbilde og endret kostnadsramme høsten 2024 i Prop. 1 S for 2024–2025 – som også var årsaken til den økte kostnadsrammen.

Jeg mener programmet har gått gjennom flere sikkerhetsvurderinger i etterkant av dataangrepet, gått gjennom flere kontrollpunkter for å sørge for at man har styring og kontroll, og at man også skal klare å levere på det som er målet, nemlig å gi en moderne IKT-plattform for departementene, slik at man klarer å jobbe effektivt og godt sammen på riktig sikkerhetsnivå gitt data av ulik verdi.

Eivind Drivenes (Sp): Så et spørsmål til statsråd Sandvik. Du sa nå at dere ville trekke dere litt ut på sidelinjen i prosjektet og overlate hovedansvaret til digitaliseringsministeren. Er det gjort en strategisk vurdering, eller er det mer praktiske årsaker til at det endres?

Statsråd Tore Onshuus Sandvik: Jeg vil be departementsråden svare på det, men jeg kan svare selv først. Det er en praktisk inngang, men Forsvarsdepartementet vil fortsatt være representert i programstyret og følge det hele tett. Det er riktig nå når DIO overtar ansvaret, å ha rene eierlinjer på det. Så kan departementsråden, som sitter tett på, utdype om det er noen strategiske vurderinger i tillegg.

Frede Hermansen: Nei, det er egentlig ikke det. Det er ganske enkelt at nå er DIO etablert, og programmet tas inn i DIO fordi det er der den nye virksomheten skal bygges. Det er naturlig at man da skaper en entydig styringslinje. Vi vil fortsatt følge programmet, inngå i programstyret og være like tett involvert i fortsettelsen. Dessuten har vi også ansvaret for å levere den graderte delen inn i dette, som vil være en viktig aktivitet og et område for oss også i fortsettelsen. Men vi er nå i en fase hvor det er naturlig at vi rendyrker styringslinjene gjennom DIO.

Eivind Drivenes (Sp): Da er jeg ferdig.

Møtelederen: Da går vi videre til Fremskrittspartiet og Carl I. Hagen, som har 5 minutter til sine spørsmål.

Carl I. Hagen (FrP): La meg følge opp det siste ved å spørre: Når blir det formelle ansvaret overført til Digitaliserings- og forvaltningsdepartementet, slik at det blir en ensidig ledelse og et ansvarsforhold av konstitusjonell art? Når forventes den gjennomføringen?

Statsråd Karianne O. Tung: Det foregår gjennom behandlingen av revidert nasjonalbudsjett. Det blir foreslått når det legges fram – aldeles straks. Så skal Stortinget behandle revidert nasjonalbudsjett. Gitt at det blir flertall i Stortinget for at vi foretar den overføringen, blir det iverksatt fra 1. juli i år.

Carl I. Hagen (FrP): Dere har nå snakket om at inngåelse av tre kontrakter som skal skje før sommeren. Hva slags type kontrakter, og hvilken prosess er det i forbindelse med å inngå kontraktene? Er det et åpent anbud? Er det først og fremst programarbeid som skal skje? Er det også maskiner og utstyr, eller er det først og fremst leveranse av programmet? Hvor mange firmaer har vært med i prosessen før dere velger ut den som skal ha kontrakten til slutt?

Statsråd Karianne O. Tung: Her overlater jeg til ekspedisjonssjef Jan Olav Pettersen å svare.

Jan Olav Pettersen: Takk for det. Det har vært en åpen anbudsprosess, slik som er vanlig, gjennom flere steg og prekvalifisering av kandidater. Dette er jo en del av ansvaret for selve programmet. Inngåelse av kontrakter gjøres på bakgrunn av og innenfor kostnadsrammen fastsatt av Stortinget. Vi kan ikke si noe nå om hvilke kontrakter det er snakk om, for kontraktene er jo ikke ferdig inngått, men vi er i sluttfasen. Vi snakker om mai/juni i år.

Carl I. Hagen (FrP): Hva forventes kontraktsrammen å være?

Jan Olav Pettersen: Det kan jeg ikke si noe om på nåværende tidspunkt, men jeg kan si at det er innenfor den fastsatte kostnadsrammen.

Carl I. Hagen (FrP): Ok.

Dere har tydeligvis fulgt med på de andre høringene vi allerede har hatt, og bruk av konsulenter har vært et tilbakevendende tema. I den fasen man nå er i, er det helt naturlig at man bruker en del innleide konsulenter.

Når programmet er ferdig gjennomført i 2027, kan man da regne med at det vil være statsansatte som styrer, eller vil det fortsatt være en betydelig andel innleide konsulenter i 2027, 2028, 2029 og så videre fremover? Eller baserer man seg på at man nå skal greie seg selv?

Statsråd Karianne O. Tung: For denne regjeringen har det vært et mål å få ned konsulentbruken i staten. Derfor har vi nå for fjerde år på rad en felles føring til alle statlige virksomheter om å få ned konsulentbruken. Det har vi lyktes veldig godt med. Fra 2021 til 2024 har det vært en reduksjon i bruken av konsulenter på 9,1 pst., og i penger utgjør det 1,28 mrd. kr – bare for å ha sagt det på overordnet nivå først.

Så er det sånn at DIO i dag er bemannet for å drifte og videreutvikle dagens IKT-plattform og IKT-løsninger, altså Depnet/U. Det har vært grunnen til at man i programmet har måttet benytte seg av konsulenter – fordi man har en topp i utviklingsarbeidet. Vi har lyktes med å få brukt noen egne ansatte i programmet, og for så vidt også i DIO, til å være med i utviklingsarbeidet. Det er viktig for å klare å få til en så smidig overgang som mulig til den nye IKT-plattformen.

Målet er at antall konsulenter skal betydelig ned når vi er ferdige med utviklingen, implementeringen, migrasjonen og avslutningen av de gamle IKT-miljøene. Da er målet at man i størst mulig grad skal ha egne ansatte som skal drive den nye IKT-plattformen med de tre ulike kjøremiljøene som er nevnt tidligere.

Carl I. Hagen (FrP): Jeg spurte tidligere i dag om forskjeller i lønnsnivå, kostnadsnivå osv., og om dere kunne si noe mer om det. Er det noen eksempler på at de som er ansatt i staten, slutter og går over til de private konsulentfirmaene? Er det noe uro i forbindelse med det? Det er jo enkelte områder der det faktisk skjer.

Statsråd Karianne O. Tung: Jeg skal ikke uttale meg spesifikt her, det har vi ikke noe faktagrunnlag som underbygger, men vi vet det er en utfordring for staten å rekruttere og beholde kompetanse, og kanskje særlig på dette feltet, IKT-kompetanse, som er sterkt konkurranseutsatt, og hvor det er vanskelig å få tak i dyktige folk. Det har vært noe av grunnen til at man også har måttet benytte seg av konsulenter i dette prosjektet.

Møtelederen: Da går ordet videre til Audun Lysbakken, SV, som har 5 minutter.

Audun Lysbakken (SV): Takk. Jeg begynner der forrige mann slapp, på konsulentbruken. Dere er jo veldig tydelige på at prosjektet ikke er styrt av konsulenter. Samtidig viser det seg at bruken av konsulenter i prosjektet var høyt over taket, og det uten at staten oppdaget det. Hvis konsulentene ikke er i styringen, hvordan kunne det da skje? Fra utsiden ser det litt ut som konsulentene har vært alene hjemme, når regningen bare går av seg selv på den måten.

Statsråd Karianne O. Tung: Jeg tror det er viktig at vi her skiller mellom arbeidet med IKT-plattformen og det som er kjent som emagine-avtalen, som Lysbakken er inne på.

Emagine-avtalen er en felles rammeavtale for bruk av konsulenttjenester innenfor IKT-området, altså en rammeavtale for IKT-tjenester som alle departementene kan benytte seg av. Utenriksdepartementet, Justisdepartementet – mange departementer har benyttet seg av denne avtalen. Den hadde en maksimal ramme på 600 mill. kr., og i høst ble det oppdaget at grensen for denne rammeavtalen var nådd. Man hadde også samlet sett gått over 600 mill. kr.

Med en gang vi fikk kjennskap til den overskridelsen, reduserte vi bruken til et absolutt minimum, så langt vi fikk det til uten at det skulle gå ut over sikkerheten til de IKT-tjenestene vi skulle utføre. Man startet umiddelbart arbeidet med å lage en ny rammeavtale for å ha den ut på anbud. Konkurransen ble kunngjort i starten av november 2024, og vi fikk en ny kontrakt i slutten av januar 2025.

Det er uheldig at det skjedde, og vi har gjort en rekke tiltak etter at vi oppdaget at denne rammeavtalen ble overgått, for å unngå at det skjer igjen. For det første har vi overført ansvaret for rammeavtalen på IKT-konsulentformidling fra DSS til DIO, siden DIO ble opprettet fra 1. januar. Vi har stilt krav til bedre internkontroll for å oppdage, for at dette ikke skal skje, og for å følge opp. Tidligere i denne rammeavtalen hadde man rapportering fra leverandør hver sjette måned. Vi har stilt krav om at man skal ha månedlige rapporteringer, nettopp for å unngå at dette skjer igjen.

Audun Lysbakken (SV): Det har vi hørt, og det er bra. Selv om den avtalen er bredere, som vi selvfølgelig er klar over, har det vært en betydelig pengebruk knyttet til det prosjektet vi snakker om i dag, også etter at taket var nådd, og egentlig pengebruk utover det, i strid med anskaffelsesreglementet. Hvem har det politiske ansvaret for det bruddet?

Statsråd Karianne O. Tung: Så snart det bruddet ble oppdaget, iverksatte vi tiltak umiddelbart. Den rammeavtalen lå høsten 2024 under DSS. Den har blitt overført til DIO fra 1. januar, og både DSS og DIO er underliggende virksomheter i DFD, og det er gjennom eierstyringen vi har …

Audun Lysbakken (SV): Så det korte svaret er at du har det?

Statsråd Karianne O. Tung: Det er riktig.

Audun Lysbakken (SV): Riktig. Vi har flere ganger vært innom dette med grunnlaget for de ulike beslutningene underveis, altså først beslutningen om å gå til privat sky, så beslutningen om å gå til en eller annen form for mellomløsning. Digitaliseringsministeren beskrev det som noe man liksom så underveis – det har vært mange av den typen formuleringer.

Vi skjønner jo at programstyret og eierne er ansvarlige for beslutningene, og beslutningene er forankret i regjering, men det vi ikke har fått helt grep om i dag, er hvordan de faglige rådene ved disse ulike beslutningene ble gitt. Det må jo ha vært et faglig grunnlag som kom et sted fra. Jeg vil anta at det kanskje har sitt utspring i konsulentmiljøet som har jobbet med det. Kan vi nå få et mer konkret svar på det? Har det kommet faglige råd i form av noen form for bred utredning, eller er det vurderinger som kommer fra konsulentmiljøet? Kan dere beskrive det litt grundigere for oss?

Statsråd Karianne O. Tung: Jeg kan starte først, før jeg gir ordet til ekspedisjonssjefen. Dette er jo et program som har vart over lang tid. Programmet er en blanding av fagmiljøer fra departementene, fra IKT-miljøene, men også innspill fra de faglige eksterne kvalitetssikrerne, som i sum har gitt grunnlaget for beslutningsdokumentasjon, altså papirer. Dette har vært et program som har hatt mange beslutninger, med godt saksgrunnlag – saksgrunnlag både for drøftinger, for beslutninger, for forankring i regjering og ikke minst for informasjon til Stortinget.

Så det har vært saksdokumenter med mange vedlegg basert på tunge faglige råd fra egne miljøer, men også med innspill og vurderinger fra de ulike eksterne kvalitetssikrerne, både i første runde, fra Metier, som anbefalte å stoppe hele arbeidet under den forrige regjeringen våren 2021, til den eksterne kvalitetssikringen som kom våren 2022 fra Holte Consulting. Så dette er en blanding, men her kan jo ekspedisjonssjefen utdype.

Jan Olav Pettersen: Takk for det. Faglige vurderinger er gjort på mange nivåer. Vi har jo, som statsråden redegjorde for, hatt en rekke kvalitetssikringer. I forkant av de kvalitetssikringene leveres det inn informasjon, bakgrunnsmateriale, som da er gjenstand for kvalitetssikring.

Så er det kvalitetssikringsrapporter som er offentlig kjent. Den første kvalitetssikringsrapporten tror jeg hadde 71 oppfølgingspunkter. Den type vurderinger, av hvordan man følger opp de punktene, behandler vi i første rekke i programstyret.

Da kommer jeg tilbake til viktigheten av programstyret. Der sitter også representanter fra de fire IKT-miljøene som var inne, som har med seg vurderinger fra sine virksomheter, med ulike perspektiver og gjerne forberedt på bakgrunn av materialet, inn i programstyremøtene. De har med seg vurderinger fra DSS, fra Justisdepartementets IT-avdeling, fra Utenriksdepartementet og fra Forsvarsdepartementet, og på bakgrunn av det gjør vi våre vurderinger. Vi får råd fra eksisterende miljøer. Dernest opererer vi på de fullmaktene vi har fra statsråder, og vi orienterer våre statsråder på gitte punkter, både skriftlig og muntlig.

Dette legges fram for regjeringen, og da er det jo regjeringsnotater, hvor vi tradisjonelt redegjør for hva ekstern kvalitetssikrer mener, og hva de enkelte statsrådene har ment. Så tas det beslutninger på bakgrunn av de vurderingene. I den runden pleier også Finansdepartementet å være tydelige, for ekstern kvalitetssikring gjøres sammen med Finansdepartementet, som også er med og følger dette arbeidet tett. I neste steg, etter forankringer av viktige kontrollpunkter i regjeringen, legges relevante saker fram for Stortinget.

Møtelederen: Da skal vi videre til Naomi Ichihara Røkkum fra Venstre.

Naomi Ichihara Røkkum (V): Beklager, men jeg var ute en tur. Det foregår en annen høring jeg også måtte på.

Jeg tenkte bare å høre litt mer om dette med konsulentbruk, og den emagine-avtalen. Det som ble nevnt av statsråden, var at man i realiteten egentlig må bremse opp noe av virksomheten fordi man begynner å nærme seg den kostnadsgrensen. Det jeg lurer på, er: Når man har gjort justeringer rundt denne avtalen, har man da fortløpende prognoser? Er det slik at det settes av penger, så man på en måte vet at man har penger framover? Altså: Hvordan er det man i realiteten fører kontroll i dag slik at man ikke havner i den samme situasjonen igjen? For det høres jo ikke ut som man på kort sikt kommer til å ha flere statlige ansatte rundt dette prosjektet, men det høres ut som man fortsatt kommer til å ha en del konsulenter. Så jeg er litt nysgjerrig på hvordan den kontrollen i realiteten utøves, som nå er annerledes.

Statsråd Karianne O. Tung: Som følge av overskridelsen av rammeavtalen i høst er det, som jeg nevnte i sted, innført nye rutiner. For det første har ansvaret blitt overført fra DSS til DIO, og for det andre har vi styrket samhandlingen mellom fagavdelingene og miljøene for anskaffelse og internkontroll for å sørge for at det skal bli bedre. Vi har også stilt nye krav til rapportering, som vil bidra til å forhindre at dette skjer igjen, ved at man går for rapportering fra hver sjette måned til hver måned for å følge bedre med.

Naomi Ichihara Røkkum (V): Dere var inne på utfordringen med å tiltrekke seg IKT-kompetanse i staten. Det er jo et kjent problem. Hva har dere gjort konkret for å endre på det? For det er ikke bare kortsiktig, men også langsiktig, når vi går over til driftsfasen, som også enkelte av de andre representantene løftet.

Statsråd Karianne O. Tung: Det er helt riktig. Som konstitusjonelt ansvarlig statsråd for statens arbeidsgiverpolitikk er det klart at det er et stort arbeid for staten å sørge for at man har god og riktig kompetanse tilgjengelig. Det er noe vi arbeider med hele tiden gjennom de årlige lønnsoppgjørene, som skal være i tråd med frontfagsrammen, men ikke minst med tanke på hvordan vi utvikler statens lederplakat – nå må jeg bare komme på riktig tittel her – altså forventningen til lederne når man skal rekruttere eller beholde. Så er det klart at når man driver store, komplekse utviklingsprogram, som en felles IKT-plattform er, ville det vært uhensiktsmessig å skulle ansette absolutt alle internt, for når man er over utviklingstoppen, vil man ikke ha bruk for den samme type spisskompetanse.

Naomi Ichihara Røkkum (V): Selv ikke midlertidig ansettelse – for det har man jo anledning til?

Statsråd Karianne O. Tung: Denne regjeringen er opptatt av å sørge for at man skal ha faste ansettelser. I toppene på utviklingsprosjekter kommer vi likevel ikke bort fra at vi er nødt til å hente noe kompetanse eksternt, også gjennom konsulenter.

Når det er sagt, gjentar jeg selvfølgelig gladelig at det har vært et mål for denne regjeringen å få ned konsulentbruken, og den har nå, i løpet av fire år, gått ned med 9,1 pst., tilsvarende 1,98 mrd. kr. Vi har hatt sterke fellesføringer til over 200 statlige virksomheter hvert eneste år nå i fire år om å få ned konsulentbruken. Det er tema i alle samtalene i oppfølgingen av virksomhetene fra departementenes og eierstyringens side. Vi er på god vei, og vi ønsker å komme oss ytterlige ned i den bruken.

Naomi Ichihara Røkkum (V): Er det noen realistisk plan for å få den ned i dette prosjektet?

Statsråd Karianne O. Tung: Det er realistisk. Her er det redegjort godt for gjennomføringsfasen, med de tre ulike kontraktsinngåelsene som nå skal gjøres, både ved å etablere de nye løsningene for IKT-plattformen, og ikke minst sørge for at man får en vellykket migrasjon, når det kommer, hvor man skal gå over fra de fire ulike miljøene til den ene felles i de ulike kjøremiljøene. Når det er gjort, mot 2027, og man satser på å være ferdig med programmet, er målet at programmet skal driftes og styres av egne ansatte i DIO.

Naomi Ichihara Røkkum (V): Jeg har ikke flere spørsmål.

Møtelederen: Da går komiteen over til oppklaringsspørsmål, hvor det er satt av 15 minutter til at de ulike medlemmene i komiteen kan tegne seg for nye runder. Jeg starter med meg selv.

Jeg lurer rett og slett bare på: Denne komiteen har jo det privilegiet å kunne se bakover og se historisk på ting. Vi sitter nå med en fasit som viser at det å skifte målbilde i begynnelsen av 2023 og tro på et system bygget på DSS-elementer, viste seg ikke å holde. Det ble hacket og ble en veldig dyrekjøpt erfaring for Norge. Det er en beslutning, slik jeg forstår av denne høringen, som er tatt med sikre faglige vurderinger i bunnen osv. Det viste seg å være feil. Er det noe å se tilbake på og erkjenne at man rett og slett gjorde feil, at man valgte feil, og at man burde velge annerledes?

Statsråd Karianne O. Tung: Jeg synes Forsvarsdepartementet tidligere har redegjort godt for hvorfor man valgte å gå bort fra FDs tonivåplattform, for å si det først.

Møtelederen: Men det ville jo ikke blitt hacket, bare for å si det.

Statsråd Karianne O. Tung: Nei, det er helt riktig. Og bare for å kommentere vurderingene rundt komponenter i plattformen til Depnet/U, som komitélederen her er inne på, hvor man mener det var feil beslutning, så vidt jeg oppfattet komitélederen, at man skulle gjenbruke komponenter fra Depnet/U: Det var ingenting som tydet på det da dataangrepet skjedde. Heller tvert imot: I løpet av 2022 hadde NSM gjennomført en inntrengingstest med målrettede angrep på komponentene i plattformen til Depnet/U, hvor NSM sa at det var mulig med gjenbruk av komponenter fra Depnet/U. Man gjorde deretter også investeringer i Depnet/U-plattformen for å gjøre den sikrere.

Så kom dataangrepet sommeren 2023, som ble utført av en avansert trusselaktør. Det var en nulldagssårbarhet som ble utnyttet, altså en sårbarhet ingen visste at fantes, eller som hadde blitt angrepet før, og det var DSS som oppdaget at det hadde blitt utført et angrep hos en underleverandør, som også leverte flere andre steder i verden. Jeg er ganske stolt over at det var det norske fagmiljøet som oppdaget dette og fikk varslet videre.

Møtelederen: Når det gjelder NSMs testing i 2022, er det mulig å si noe i en åpen høring om det lå på et realismenivå som tilsvarer en avansert statlig aktør? Vi snakker tross alt om regjeringens saksbehandlingssystem, så man må på en måte rigge testene dithen at man utsettes for et sånt angrep, som da skjedde et par måne-

der senere, og som ville, med FDs system, i alle fall gitt en større trygghet.

Jan Olav Pettersen: Det er mange aktører som gjennomfører inntrengingstester, og vår beslutning som ansvarlig etatsstyrer av DSS var å gå til Nasjonal sikkerhetsmyndighet, som har særlig kompetanse på slike tester. De bruker all den kunnskap de har, som de har fått gjennom sine erfaringer, for å vurdere og prøve å trenge seg inn i systemene. Det var bakgrunnen for de vurderingene som de da gjorde. Jeg har ikke nok kunnskap til å sammenligne NSMs miljø med et annet, men det er det beste sikkerhetsmiljøet vi har, og det var viktig for oss å bruke dem og ikke noen eksterne i den vurderingen.

Møtelederen: Da er det et spørsmål fra Carl I. Hagen.

Carl I. Hagen (FrP): En oppfølging av dette: Da man gikk bort fra gjenbruk av noen av komponentene i Depnet/U, var det basert på at det var den eksterne kvalitetssikrer som sa fra om det, så vidt jeg har oppfattet det. Eller er det misforstått? Det har vært nevnt flere ganger at det var den eksterne kvalitetssikreren som anbefalte å gå bort fra modellen om gjenbruk av Depnet/U-komponenter, altså ikke det interne systemet i regjeringsapparatet.

Statsråd Karianne O. Tung: Det var NSM som hadde en vurdering av DSS, altså Depnet/Us plattform, etter dataangrepet, som var utført av en avansert trusselaktør. NSMs vurdering var at komponentene var kompromittert, og vi kunne ikke lenger ha tillit til å gjenbruke de delene. Det er det jeg kan si i denne åpne delen.

Møtelederen: Kirsti Leirtrø, Arbeiderpartiet.

Kirsti Leirtrø (A): Takk for det. Saksordføreren sier at dette handler om regjeringens saksbehandlingssystem, men jeg forsto på Tung at dette handler om så utrolig mye mer enn det – en organisering og kanskje 500 framtidige systemer.

Sikkerheten i samfunnet vårt og beredskapen er under hardt press. Da vi behandlet langtidsplanen for Forsvaret, hadde vi en samstemthet og økt prioritering på det. Kan du si noe om sammenhengen mellom langtidsplanen og digitaliseringsstrategien? Egentlig er spørsmålet om det handler om mer enn regjeringens saksbehandlingssystem.

Statsråd Tore Onshuus Sandvik: Jeg kan starte med å si litt om det, før statsråd Tung utdyper videre.

Jeg kan bare minne om at da det ble vurderinger, som jeg opplyste om før, knyttet til å bruke FDs nett, var også sikkerhetsnivået der så høyt at det ville lagt store begrensninger på hele departementsfellesskapet om man skulle kjøre på samme sikkerhetsnivå. Det ville gjøre det vanskelig å hente ut effekter og gevinster og digitalisere hele virksomheten det er snakk om. Det ligger store muligheter i det, og det er et kappløp mellom sikkerhet og utvikling hele veien. Det er jo de store dilemmaene som ligger i sånne anskaffelser. Derfor er det også viktig at man gjør det grundig og går nøye til verks, sånn som man har gjort i denne sammenhengen.

Det er klart at vi skal hente ut store gevinster av å digitalisere og bruke nye systemer godt, ikke minst innenfor AI, også i forvaltningen, og da må vi ha et system som gjør at en har et sikkerhetsnivå som er riktig ut fra de ulike tjenestene som skal brukes og leveres. Noe skal være veldig hemmelig, noe skal være begrenset, noe skal være ugradert skjermingsverdig, og så videre nedover. Det å finne riktig teknologi på de ulike miljøene er viktig å vektlegge, sånn som det er vurdert i disse situasjonene.

Så kan kanskje Tung ta over og fortelle mer om hvilke ambisjoner som er, men det er viktig med riktig sikkerhetsnivå. Hvis sikkerhetsnivået er for høyt på alt man skal gjøre, vil det bli veldig vanskelig å drive effektiv forvaltning.

Statsråd Karianne O. Tung: Vi har satt som ambisjon at Norge skal bli det mest digitaliserte landet innen 2030, og den ambisjonen skal også gjelde offentlig forvaltning. Jeg synes forhistorien her – med fire IKT-miljøer hvor UD og utenriksstasjonene har sitt eget, Justisdepartementet har sitt eget, DSS har hatt sitt eget og FD og SMK har hatt sitt eget – egentlig eksemplifiserer hvor viktig det er å arbeide med å sørge for moderne digitale verktøy, sånn at man også får en moderne og digital forvaltning. Det er nettopp denne organiseringen som egentlig har hindret at man kan jobbe effektivt nok i årene som har vært, og som beskriver hvor viktig det er å få på plass denne plattformen, for at vi skal kunne nyttiggjøre oss nye teknologier, som KI, automatisering og maskinlæring, også i årene framover. Det er det ene punktet om hvorfor det er viktig med den felles IKT-plattformen, og så handler det – som forsvarsministeren er inne på – om sikkerhet.

Vi lever i en verden der de digitale truslene øker for hver dag. Digital svindel er nå større på verdensmarkedet enn narkotikahandel. Det viser hvor viktig det er hele tiden å jobbe med sikkerhet i systemene. Å gå fra fire IKT-miljøer, hvor vi er sårbare og ineffektive, til ett felles IKT-miljø vil bidra til å øke sikkerheten i departementsfellesskapet og er en viktig milepæl for oss. Sikkerhet og modernisering av forvaltningen er viktige stikkord i arbeidet med felles IKT-plattform.

Møtelederen: Da har jeg tegnet meg selv til et oppfølgingsspørsmål nettopp om det.

Alle er enige om at å samle fire miljøer er en riktig ting å gjøre, men som flere kritikere har påpekt, vil en jo – med den løsningen som er valgt – ende opp med fire såkalte kjøremiljøer, altså hvor ulik informasjon lagres ulike steder. Skjermingsverdig ugradert skal i privat sky i norske datasentre, ugradert skal driftes delvis i offentlig sky og delvis i eget datasenter, og så skal vi ha graderte løsninger som skal levere statens graderte plattformtjenester. Er dere da i realiteten over i samme situasjon, iallfall når det gjelder sårbarhet for angrep? Det er fortsatt spredt over mange forskjellige punkter.

Statsråd Karianne O. Tung: Jeg forstår spørsmålet. Det kan være komplisert når man snakker om både kjøremiljø og ulike løsninger, men det en felles IKT-plattform handler om, er at vi bygger oss en felles grunnmur. Huset vårt, hvor grunnmuren skal stå, er trygt. Før har vi egentlig hatt fire ulike hus med mange dører, mange vinduer og mange verandadører. Nå bygger vi ett hus med én felles grunnmur, som vil sikre oss, og så er det ulike løsninger i ulike etasjer, avhengig av hvor godt man må skjerme de dataene som ligger der. Det har vært viktig for oss å klare å få samlet både de miljøene og den plattformen. Forsvarsdepartementet kan eventuelt utdype de ulike kjøremiljøene, hvis det er behov for det.

Møtelederen: Vi går videre til Frode Jacobsen.

Frode Jacobsen (A): Som forsvarsministeren var inne på, er det en avveining her mellom sikkerhet, økonomi og effektiv forvaltning. Å finne den rette balansen der kan ikke alltid være så enkelt.

Jeg har to spørsmål. Det ene er: Har dere fått noen advarsler underveis som dere ikke har tatt hensyn til, eller hvor dere har tenkt at det overser vi, eller det gjør vi ikke noe med, til tross for at noen har vært bekymret? Det andre er: Statsråd Tung har jo ansvar for digitalisering i offentlig forvaltning, og denne komiteen har vel før vår tid av og til hatt noen runder om ulike IKT-prosjekter i offentlig forvaltning. Har dere vært inne på tanken om at det enkleste hadde vært å la det skure og gå og ikke sette i gang noe så stort, hvor det jo er en potensiell risiko for at vi sitter her igjen om noen år?

Statsråd Karianne O. Tung: Jeg kan starte, og jeg tror jeg kan svare uavhengig av både politisk farge og bakgrunn: Jeg tror ingen er tjent med å la det fortsette å skure og gå. Når det er sagt, lar vi det heller ikke skure og gå. Vi har iverksatt en rekke tiltak etter dataangrepet som er gjort på eksisterende plattformer, bare for å si det. Det er både av sikkerhetshensyn og av hensyn til utviklingen av forvaltningen at vi er avhengig av å få på plass en ny IKT-plattform. Det er kritisk viktig for at vi skal kunne levere gode tjenester.

Jeg har bare lyst til å kommentere det første spørsmålet ditt, om det noensinne har kommet advarsler underveis. Da har jeg lyst til å nevne én ting. Vi har fått en bekymringsmelding underveis fra de tillitsvalgte i Utenriksdepartementet, som har vært bekymret for IKT-plattformen. Den bekymringsmeldingen er håndtert i Utenriksdepartementet. Det er klart at når en har fire opprinnelige miljøer som er skreddersydd for hver sin sektor, vil det alltid være en bekymring for hva som skjer med ens eget område når vi skal over i noe nytt som skal favne en mye større helhet. Det er derfor det er så viktig med god styring av plattformen, og at det er noen som har et helhetsblikk, som kan vurdere hva vi trenger, både for utenriksstasjonene og for så vidt for Finansdepartementets, Justisdepartementets eller Forsvarsdepartementets del. Bekymringsmeldingen fra UDs tillitsvalgte er behandlet i UD, og man velger også i den nye IKT-plattformen å ta med noe fra UDs del, nettopp basert på erfaringer fra utenrikstjenesten, f.eks., på hva man trenger.

Statsråd Tore Onshuus Sandvik: Jeg tenkte jeg ville legge til noe. Det kan jo godt tenkes man kommer tilbake hit, men nettopp disse kontrollfunksjonene er viktige. Det er derfor man har laget statens prosjektmodell, og det er derfor man har hatt denne grundige gjennomgangen – at man har både KS2, man har flere kontrollpunkter, og man har en fleksibel måte å gjøre det på for å kunne tilpasse seg virkeligheten, så man ikke ender opp med et utdatert system den dagen man innfører det. For her er det et teknologikappløp, der det også er kommersielle selskaper som er i lead på teknologiutviklingen, samtidig som vi må sikre at vi har nasjonal kunnskap og kunnskap internt i forvaltningen for å kunne skjerme ting som ikke vil passe seg å ha ut i rene kommersielle løsninger. Jeg synes nettopp denne kontrollfunksjonen understrekes av at det er viktig å ha denne utviklingen framover, og jeg synes statsråd Tung også har redegjort veldig godt for at dette følges veldig godt opp.

Møtelederen: Da er foreløpig sist inntegnede Audun Lysbakken.

Audun Lysbakken (SV): Mye av kjernen i denne saken er egentlig spørsmålet om hvor solid det faglige grunnlaget har vært for de veivalgene som har vært tatt underveis, og hvorvidt det har vært motforestillinger eller andre mulige veier å gå. Til det som flere av oss har prøvd å bore i i dag, synes jeg Jan Olav Pettersen brakte oss i hvert fall nærmere en forståelse av det i sted, knyttet til disse ulike veivalgene som er tatt, beslutninger i

programstyret – at det har vært lagt fram ulike faglige råd for programstyret.

Mitt siste spørsmål går på disse faglige rådene. Jeg antar at de finnes i en skriftlig, konsentrert form. Betyr det at det foreligger tydelige faglige grunnlag for disse beslutningene som det også kan være mulig for komiteen å få innsyn i, hvis vi ber om det?

Jan Olav Pettersen: De eksterne kvalitetssikringsrapportene er offentlige. De ligger der. R-notater er det jo ikke vanlig å utgi til komité, til Stortinget, der er de samlede vurderingene, hvor det gjengis både hva kvalitetssikrer måtte mene, og hva statsrådene mener, fram til regjeringen, ei heller konklusjoner derfra. Vi har også interne beslutningsdokumenter som normalt er unntatt offentlighet, så jeg tror vi må komme tilbake til hva vi eventuelt kan bistå med for å få en synliggjøring av det.

Statsråd Karianne O. Tung: Bare for å utdype: Vi er innstilt på å gi innsyn i de interne beslutningsnotatene fra programstyret.

Møtelederen: Takk. Da kan komiteen ta det til vurdering i det videre arbeidet med saken.

Vi er kommet til siste del av høringen, og det er den avsluttende runden, hvor det gis anledning til å si det man måtte ønske å legge til. Dere har 5 minutter hver.

Statsråd Karianne O. Tung: Takk, leder. Jeg har bare aller først lyst til å si takk til komiteen for å reise høringen om det som jeg mener er en veldig, veldig viktig sak. Igjen: Vi må minne oss om hvorfor vi nå står i dette arbeidet, som har tatt lang tid, fra oppstarten i 2011 og til her vi befinner oss i dag. Det handler altså om å samle fire IKT-miljøer for både å øke sikkerheten og ikke minst kompetansen, moderniteten og effektiviteten i departementsfellesskapet, og det handler om å samle de ulike miljøene, slik at man også får felles retningslinjer og felles rammer å jobbe innenfor.

Fra den spede starten i 2011 og fram til 2021 var programmet – eller prosjektet, kan vi kalle det da – preget av ganske mye interne uenigheter og lite framgang, nettopp fordi det besto av fire miljøer som hver ville sine ting, men etter forprosjektets start og etter KS2 i 2021 er prosjektet nå på stø kurs. Det er stram styring.

Det har vært forskjellige målbilder. Det skyldes i all hovedsak særlig dataangrepet sommeren 2023. Jeg mener at programmet gjennom den styringen som har vært, altså det å følge statens prosjektmodell, etablerte standarder, både gjennom PRINCE2 og annen metodikk, har vært styrt godt, men ikke minst smidig. Det blir kanskje satt et spørsmålstegn ved at man bruker ordet «smidig» organisering og «smidig» prosjektstyring, men det er altså en metodikk som er veldig egnet for å kunne håndtere endringer som skjer underveis. Er det én ting vi alle sammen vet nå, er det at her har det skjedd endringer underveis, men nettopp fordi man har styrt som man har gjort, og organisert som man har gjort, har man klart å fatte gode beslutninger i tide, både forankret i regjering og ikke minst forankret i Stortinget, ved alle viktige milepæler. Det er fordi prosjektet og programmet er organisert slik som det er.

Vi har god tro på at gjennom kontraktsinngåelsene og arbeidet som skal skje med migrering over til den nye IKT-plattformen, skal dette nå gå bra. Det er komplekst, det er vanskelig, men målet er at dette skal være ferdig innen 2027, slik at departementsfellesskapene får én IKT-plattform å forholde seg til. Det er viktig for å kunne være en moderne forvaltning overfor innbyggerne, men ikke minst for at man skal kunne drive saksbehandling, utredningsarbeid og arbeid internt i departementene og i regjering på en effektiv måte, og det tror jeg i hvert fall undertegnede kan si at det gleder jeg meg til å få på plass.

En kort oppklaring: Jeg bruker enhver anledning til å skryte av å kutte i konsulentvirksomhet, men jeg tok kanskje litt hardt i. Jeg sa at vi hadde spart oss for 1,9 mrd. kr. Det riktige er 1,28 mrd. kr, slik at det ikke blir feil.

Møtelederen: Der unngikk du en ny kontrollsak!

Ønsker Sandvik også ordet?

Statsråd Tore Onshuus Sandvik: Jeg tror ikke det er nødvendig. Min periode er så kort, og jeg synes statsråd Tung og de forhenværende har redegjort godt nok for det. Det er ikke så mye for meg å si, annet enn å oppsummere med at det er viktig at vi lykkes med dette. Det gjøres et veldig godt arbeid nå, men det kommer til å bli utfordringer framover. For det kan vi si fra forsvarssektoren: Det er stor aktivitet fra ulike trusselaktører innenfor cyberdomenet, og desto viktigere er det at vi er godt forberedt.

Møtelederen: Det er fint. Da gjenstår det bare for meg som leder av komiteen å takke dere så mye for at dere stilte opp og svarte på våre spørsmål.

Med det er kontrollhøringen over. Takk for i dag!

Høringen slutt kl. 13.48.

STORTINGET

VEDLEGG 2

Statsråd Karianne Oldernes Tung
Digitaliserings- og forvaltningsdepartementet
Postboks 8004 Dep,
0030 Oslo

Vår ref.:	Deres ref.:	Dato:
		11.02.2025

Vedr. rammeavtaler i staten

Kontroll- og konstitusjonskomiteen viser til artiklene «Toppbyråkrater vraket gjenbruk. Ny pris: 2,2 milliarder» og «Sprengte konsulentavtale med 130 millioner» i Aftenposten hhv. 3. og 5. februar 2025.

1. Kan statsråden redegjøre for hvordan rammeavtaler inngått av departementene og underliggende etater følges opp, for å sikre korrekt etterlevelse av anskaffelsesregelverket?

2. Kan statsråden redegjøre for hvorfor eksisterende IT-plattform for Utenriksdepartementet ikke kan videreføres, og om det er nødvendig å be eksterne konsulenter lage ny plattform for en svært høy pris?

Komiteen ber om svar innen 18. februar 2025.

Med vennlig hilsen
Kontroll- og konstitusjonskomiteen

Peter Frølich
komitéleder

Stortinget
Postboks 1700 Sentrum
NO-0026 OSLO

Tlf. 23 31 30 50
NO 971 524 960

ww.stortinget.no

VEDLEGG 3

DET KONGELIGE DIGITALISERINGS- OG FORVALTNINGSDEPARTEMENT

Statsråden

Stortingets kontroll- og konstitusjonskomite

0026 Oslo

Deres ref	Vår ref	Dato
	25/504-3	18. februar 2025

Spørsmål fra kontroll- og konstitusjonskomiteen vedrørende rammeavtaler i staten

Jeg viser til brev fra Stortingets kontroll- og konstitusjonskomité datert 11. februar 2025. I brevet stilles følgende spørsmål:

1. Kan statsråden redegjøre for hvordan rammeavtaler inngått av departementene og underliggende etater følges opp, for å sikre korrekt etterlevelse av anskaffelsesregelverket?
2. Kan statsråden redegjøre for hvorfor eksisterende IT-plattform for Utenriksdepartementet ikke kan videreføres, og om det er nødvendig å be eksterne konsulenter lage en ny plattform for en svært høy pris?

Svaret på spørsmål 2 er skrevet i samarbeid med forsvarsministeren som følge av at Forsvarsdepartementet (FD) og Digitaliserings- og forvaltningsdepartementet (DFD) er programeiere for og styrer Program for felles IKT-løsninger i departementsfellesskapet i fellesskap.

Svar på spørsmål én:
Innledningsvis ønsker jeg å redegjøre for ansvarsfordelingen på anskaffelsesområdet. Nærings- og fiskeridepartementet er fagdepartement for offentlige anskaffelser og har overordnet ansvar for lovverket for offentlige anskaffelser i offentlig sektor. Dette inkluderer Direktoratet for forvaltning og økonomistyring (DFØ) sitt arbeid på området. Den enkelte offentlige oppdragsgiver er ansvarlig for å gjennomføre anskaffelser i henhold til lovverket.

DFD har gjennom Statens innkjøpssenter ansvar for innkjøpsavtaler på vegne av statlige virksomheter innenfor utvalgte innkjøpsområder. Det er i dag fellesavtaler i kategoriene

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

kontor, reise og IKT. Kontraktsoppfølgingen gjennomføres på overordnet nivå av Statens innkjøpssenter, mens den enkelte virksomhet som benytter avtalene har ansvaret for egne bestillinger og leveranser. Statens innkjøpssenter har ikke fellesavtaler for konsulenttjenester.

DFD har også ansvaret for Departementenes sikkerhets- og serviceorganisasjon (DSS) som inngår og forvalter felles rammeavtaler for departementsfellesskapet (ikke underliggende etater[1]), inkludert koordinering av avtaler i regi av Statens innkjøpssenter. Anskaffelsesmiljøet i DSS bistår også departementsfellesskapet med juridisk og merkantil rådgivning i forbindelse med anskaffelser og kontraktsoppfølging.

Jeg tolker spørsmål 1 dithen at det handler om rammeavtaler for departementsfellesskapet og ikke staten som helhet (jf. artikkelen i Aftenposten om rammeavtale for konsulentformidling). Det videre svaret er derfor rettet mot felles rammeavtaler som er inngått og forvaltes av DSS og Departementenes digitaliseringsorganisasjon (DIO) på vegne av departementsfellesskapet.

DSS har policy, rutiner og retningslinjer for hvordan anskaffelsene skal gjennomføres for å sikre at anskaffelsesregelverket følges. I tillegg har DSS rutiner for kontraktsforvaltning for å sikre at kontraktene etterleves, og internkontroll av både anskaffelser og kontraktsforvaltning. Departementene forvalter selv rammeavtaler som er inngått av det enkelte departement.

Rammeavtaler som omfatter hele departementsfellesskapet, er kostnadseffektivt og bidrar til bedre avtalevilkår enn om departementene inngår avtaler enkeltvis. De økonomiske rammene for de enkelte rammeavtalene er erfaringsbasert og fastsettes i dialog med de departementene som ønsker å bruke avtalene. Denne avtalestrukturen gir imidlertid enkelte utfordringer med løpende kontroll av uttak på avtalene, ettersom det er flere departementer som gjør uttakene. Dette håndteres i dag gjennom rapporteringskrav som stilles til leverandørene. Basert på praksis og erfaring med ulike avtalestrukturer vurderer DSS fortløpende behov for endring i leverandøroppfølging og eventuelle andre tiltak som kan styrke kontrollen med uttak på avtalene.

Departementene ble 21. oktober 2024 varslet av DSS, om at samlet forbruk av rammeavtale for konsulentbruk på IKT-området hadde oversteget maksimal økonomisk ramme på 600 mill. kroner. For denne rammeavtalen mottok DSS statusrapporter fra leverandøren hver 6. måned. Som følge av høyt uttak på avtalen mellom rapporteringstidspunktene ble det ikke tidsnok oppdaget at avtalen ville bli oversteget i løpet av høsten 2024. DSS hadde på dette tidspunktet allerede satt i gang et arbeid for å få på plass en ny rammeavtale med forventet signering innen mars 2025. Arbeidet med inngåelse av ny rammeavtale ble intensivert så langt det var praktisk mulig. Ny avtale ble signert av DIO 25. januar 2025. Ansvaret for avtalen ble flyttet fra DSS til DIO da IKT-miljøet til DSS ble en del av DIO ved DIOs opprettelse 1. januar 2025.

[1] Utenom 22. julisenteret, Departementenes digitaliseringsorganisasjon og DSS selv.

Umiddelbart etter at DSS og departementene som brukte avtalen fikk kjennskap til overforbruk av avtalen, ble det iverksatt tiltak for å redusere bruken av avtalen til et absolutt minimum. Departementene og DSS så seg imidlertid nødt til å videreføre konsulentoppgaver som var helt nødvendig for å opprettholde driften og sikkerheten på IKT-plattformene til departementene. Det ble også vurdert som nødvendig å opprettholde et minimumsnivå av aktivitet i utviklingsprosjektene slik at disse ikke skulle stoppe opp. En stans i utviklingsprosjektene, ville forårsaket vesentlige forsinkelser som igjen ville ført til høye merkostnader og en utfordrende sikkerhetssituasjon for departementene.

Det er satt i gang flere kompenserende tiltak for at overforbruk på felles rammeavtaler ikke skal skje igjen:

- I den nye rammeavtalen for konsulentmegling plikter leverandøren hver måned å sende DIO en rapport over hvor mye som er fakturert totalt under rammeavtalen.
- I tillegg stilles det krav til leverandøren om en digital kundeportal som skal gi tilgang til informasjon og tjenester, og ha rapporteringsmuligheter som skal gi oversikt over aktive avrop på avtalen m.m.
- DSS skal gå gjennom og vurdere kontraktsoppfølgingen av fellesavtaler, og skal foreslå eventuelle forbedringstiltak til DFD. Dette er et oppdrag gitt i tildelingsbrev for 2025.

Svar på spørsmål to:
Program for felles IKT-løsninger i departementsfellesskapet er styrt av Forsvarsdepartementet og Digitaliserings- og forvaltningsdepartementet i fellesskap, jf. Prop. 18. S (2022-2023).

I dag er det fire ulike IKT-plattformer i bruk i departementsfellesskapet: plattformene til FD/SMK, JD, UD og plattformen som benyttes av resten av departementene (som ble driftet av DSS). Fra 1. januar 2025 driftes de tre siste av DIO. Dette er lite hensiktsmessig både fra et teknisk og økonomisk perspektiv. Det er svært dyrt og krevende å opprettholde og sikre tre ulike plattformer til samme høye standard. I tillegg øker angrepsflatene mot departementene når man har flere ulike plattformer. Plattformen som ble driftet av DSS ble utsatt for et svært alvorlig dataangrep sommeren 2023. Dette medfører en usikkerhet og et ytterligere behov for å snarest mulig få etablert en ny felles IKT-plattform.

Programmets mål er å bistå i å etablere en ny IKT-virksomhet og legge til rette for en felles digital plattform for applikasjoner og løsninger og for lagring og behandling av ugradert og skjermingsverdig ugradert informasjon. Plattformen vil tas i bruk av alle departementene, Statsministerens kontor og utenrikstjenesten og være særlig innrettet mot å ivareta digital sikkerhet tilpasset fremtidens trusselbilde. Programmet er organisert med en programleder og underliggende prosjekter. Det er etablert et programstyre som i dag består av DFD, FD, Utenriksdepartementet (UD), Justis- og beredskapsdepartementet og Statsministerens kontor. DIO og DSS er observatører i programstyret.

Arbeidet med å samle departementenes IKT-miljøer og IKT-løsninger har pågått i flere år. Det ble utarbeidet en konseptvalgutredning i 2017. I 2021 ble det startet et forprosjekt. Dette ledet fram til program for felles IKT-tjenester i departementsfellesskapet (programmet), som ble kvalitetssikret (KS2) i 2022. Mot slutten av 2022 fastsatte Stortinget en kostnadsramme på 1,4 mrd. kroner inkl. mva., jf. behandlingen av Prop. 18 S (2022-2023). Programmets tekniske målbilde var å videreutvikle IKT-plattformen som ble driftet av DSS. Etter dataangrepet mot IKT-plattformen til DSS sommeren 2023, var ikke dette målbildet lenger mulig å gjennomføre. Programmet ble derfor nødt til å utrede en ny løsning som var gjenstand for ekstern kvalitetssikring sommeren 2024. Stortinget fastsatte høsten 2024 ny kostnadsramme på 2,24 mrd. kroner inkl. mva., jf. behandlingen av FDs Prop. 1. S (2024-2025). Endringen i kostnadsrammen skyldtes i hovedsak dataangrepet 2023.

For å sikre at programmet følges opp tilstrekkelig på kostnad og tid, er det lagt opp til jevnlige kvalitetssikringer med ekstern kvalitetssikrer gjennom programperioden. Det har fram til nå være gjennomført tre kvalitetssikringer, og det planlegges for en fjerde. DFD og FD har stram styring av programmet både på tid og kostnad, iht. den nye planen etter dataangrepet. Den første leveransen var etableringen av DIO 1. januar 2025. DIO består av de tidligere IKT-miljøene til DSS, JD og UD.

Ett av hovedmålene til programmet er å etablere det man kaller en skjermingsverdig ugradert plattform for å sørge for at departementene alltid vil ha tilgang til sikre digitale tjenester. Det må presiseres at det ikke tidligere er utarbeidet ugradert skjermingsverdige plattformer i Norge. En skjermingsverdig ugradert løsning vil sammen med graderte løsninger levert av Statens graderte plattformtjenester (SGP), som er en etat underlagt FD, gi departementene sikre digitale tjenester i alle deler av krisespekteret.

Etter dataangrepet sommeren 2023 ble flere alternative løsninger vurdert, siden IKT-plattformen som ble driftet av DSS ikke lenger egnet seg som utgangspunkt for ny løsning. Ett av disse alternativene var gjenbruk av løsningen til UD som en mulig ny felles løsning. Dette alternativet ble vurdert å være dyrere, mer risikabelt og ta lengre tid å utvikle enn å bygge en ny felles løsning. Av denne grunnen ble ikke dette alternativet med i det endelige beslutningsgrunnlaget. Løsningen til UD er tilpasset UD, og den egner seg ikke som en løsning for flere individuelle kunder, som departementene er. Den nye løsningen som skal utvikles er en grunnleggende sikker og moderne plattform som vil være designet for å kunne håndtere alle departementene, og deres felles og individuelle behov.

Flere komponenter fra løsningen til UD vil likevel kunne gjenbrukes i ny løsning, og viktige erfaringer og kompetanse knyttet til arbeidet med utenrikstjenestene og utenriksstasjonene er tatt med inn i arbeidet med ny løsning. Nettverksinfrastrukturen fra plattformen som betjener utenriksstasjonene vil også videreføres. Likeledes vil erfaringer og enkeltkomponenter fra plattformene til JD og DSS kunne gjenbrukes i ny felles IKT-plattform.

De tidligere IKT-organisasjonene (og nå DIO) er ikke bemannet for å gjennomføre komplekse utviklingsprosjekter av denne størrelsen. Slike utviklingsprosjekter krever

kapasitet og spisskompetanse som ikke var tilgjengelig i de tidligere IKT-organisasjonene. Uansett hvilken løsning som ble valgt ville det derfor være behov for å innhente ekstern kompetanse.

Etableringen av en ny sikker IKT-plattform for departementsfellesskapet er et midlertidig og komplekst utviklingsprosjekt. Det ville vært vanskelig og lite lønnsomt for staten å ansette ressursene som kreves for et slikt arbeid i faste stillinger. DIO vil bidra med ressurser inn i programmet der det er hensiktsmessig og forsvarlig for å kunne opprettholde driften av dagens plattformer.

Med hilsen

Karianne Oldernes Tung

STORTINGET

VEDLEGG 4

Statsråd Karianne Oldernes Tung
Digitaliserings- og forvaltningsdepartementet
Postboks 8004 Dep,
0030 Oslo

Vår ref.:	Deres ref.:	Dato:
2025/498		04.03.2025

Vedr. rammeavtaler i staten

Kontroll- og konstitusjonskomiteen viser til svarbrev av 18. februar 2025.

Under svaret på spørsmål 2 (første avsnitt på side 4) skriver statsråden:

> «Programmets tekniske målbilde var å videreutvikle IKT-plattformen som ble driftet av DSS. Etter dataangrepet mot IKT-plattformen til DSS sommeren 2023, var ikke dette målbildet lenger mulig å gjennomføre.»

Komiteen har følgende oppfølgingsspørsmål:

1. I Prop. 1 S (2022–2023) for Forsvarsdepartementet opplyses det at den nye IKT-plattformen skal leveres på Forsvarsdepartementets plattform. I brevet fra statsråden fremgår det at prosjektets mål frem til hackingen var å benytte DSS' plattform. Når ble det besluttet å levere på DSS' plattform i stedet for Forsvarsdepartementets plattform, og hvem tok denne beslutningen?
2. Hvilken informasjon er gitt til Stortinget om at ny plattform skulle bygges på DSS' plattform, ikke Forsvarsdepartementets plattform?
3. Hvilke sikkerhetsvurderinger og risikoanalyser ble gjort før byttet til DSS' plattform?
4. Det bes om en redegjørelse for bevilgninger til prosjektet fra og med 2022, formålet med bevilgningene og hvordan den enkelte bevilgning har blitt brukt.

Stortinget
Postboks 1700 Sentrum
NO-0026 OSLO

Tlf. 23 31 30 50
NO 971 524 960

ww.stortinget.no

Komiteen ber om svar innen 14. mars 2025.

Med vennlig hilsen
Kontroll- og konstitusjonskomiteen

Peter Frølich
komitéleder

VEDLEGG 5

DET KONGELIGE DIGITALISERINGS- OG FORVALTNINGSDEPARTEMENT

Statsråden

Stortingets kontroll- og konstitusjonskomite
0026 OSLO

Deres ref	Vår ref	Dato
	25/504-7	14. mars 2025

Vedr. rammeavtaler i staten - oppfølgingsspørsmål

Jeg viser til brev fra Stortingets kontroll- og konstitusjonskomité med oppfølgingsspørsmål, datert 4. mars. Jeg viser videre til brev fra komiteen av 11. februar, og det påfølgende svaret datert 18. februar.

Brevet er skrevet i samarbeid med forsvarsministeren. Forsvarsdepartementet (FD) og Digitaliserings- og forvaltningsdepartementet (DFD) er programeiere for og styrer Program for felles IKT-løsninger i departementsfellesskapet i fellesskap, jf. Stortingets behandling av Prop. 18 S (2022–2023) Endringar i statsbudsjettet 2022 under Forsvarsdepartementet, jf. Innst. 110 S (2022-2023), 6. desember 2022:

> «II
> Stortinget samtykker i at Forsvarsdepartementet og Kommunal- og distriktsdepartementet kan iverksette Program felles IKT-tenester i departementsfellesskapet med ei kostnadsramme på 1 392 mill. 2023-kroner for endringstrinn 1 og 2.»

I dette brevet besvares følgende oppfølgingsspørsmål fra kontroll- og konstitusjonskomiteen:

1. I Prop. 1 S (2022-2023) for Forsvarsdepartementet opplyses det at den nye IKT-plattformen skal leveres på Forsvarsdepartementets plattform. I brevet fra statsråden fremgår det at prosjektets mål frem til hackingen var å benytte DSS' plattform. Når ble det besluttet å levere på DSS' plattform i stedet for Forsvarsdepartementets plattform, og hvem tok denne beslutningen?
2. Hvilken informasjon er gitt til Stortinget om at ny plattform skulle bygges på DSS' plattform, ikke Forsvarsdepartementets plattform?

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

3. Hvilke sikkerhetsvurderinger og risikoanalyser ble gjort før byttet til DSS' plattform?
4. Det bes om en redegjørelse for bevilgninger til prosjektet fra og med 2022, formålet med bevilgningene og hvordan den enkelte bevilgning har blitt brukt.

Innledningsvis vil jeg understreke at Stortinget har blitt jevnlig informert om utviklingen i programmet. Metodikken programmet benytter er en smidig tilnærming som gjør det mulig å håndtere hendelser eller endrede forutsetninger. IKT og digitalisering er et fagfelt som er under rask endring, og den smidige tilnærmingen muliggjør nødvendige endringer underveis i programperioden.

Svar på spørsmål 1-3

Som beskrevet i brev datert 18. februar, har arbeidet med å samle departementenes IKT-miljøer og IKT-løsninger pågått i flere år. Det ble utarbeidet en konseptvalgutredning i 2017. I 2021 ble det startet et forprosjekt. Dette ledet fram til program for felles IKT-tjenester i departementsfellesskapet (programmet), som ble kvalitetssikret (KS2) våren 2022.

Før programmet ble etablert og KS2 gjennomført, var planen for ny felles IKT-løsning for departementsfelleskapet, at departementene skulle migreres til FDs to-nivå plattform. I arbeidet fram mot KS2 ble en full migrering til FDs to-nivå plattform vurdert som uhensiktsmessig.

FDs plattform ville måtte endres og utvides betydelig for å kunne tas i bruk av hele departementsfelleskapet. Sikkerhetsnivået på plattformen ville også gitt vesentlige begrensninger for hvilken type applikasjoner departementene ville kunne benytte seg av. I tillegg ville det vært sikkerhetsmessig utfordrende å plassere Statsministerens kontor (SMK), departementene, Departementenes sikkerhets- og serviceorganisasjon (DSS), Departementenes digitaliseringsorganisasjon (DIO) og utenriksstasjonene på en plattform hvor de ugraderte og graderte (BEGRENSET) delene er så tett integrert. Det må understrekes at dette fungerer godt for FD og SMK i dag, men jo større mangfold i behov det blir på plattformen, jo mindre egnet vil denne plattformen være til å dekke behovene.

Forprosjektet til Programmet gikk derfor bort fra dette i arbeidet frem mot KS2.

I Prop 18 S (2022–2023) ble det redegjort for organiseringen av programmet, og blant annet forprosjektet som var gjennomført. Planleggingsfasen for programmet foregikk vinteren 2021–2022. Målbildet som ble utredet i forprosjektet, og som ble levert til ekstern kvalitetsikrer i KS2, var en løsning hvor man tok i bruk markedet (privat lukket skytjeneste) for å utvikle og drifte en ugradert plattform. Dette for å kunne dra nytte av den erfaringen, kompetansen, skaleringsmulighetene og stordriftsfordelene som eksisterer i markedet. Lavgraderte løsninger var fortsatt planlagt levert på FD sin to-nivåplattform. Dette var det målbildet som ble presentert når etableringen av programmet ble vedtatt iverksatt av Stortinget gjennom behandling av Innst. 110 S (2022-2023) til Prop. 18 S (2022-2023) for

Forsvarsdepartementet med en kostnadsramme på 1392 mill. 2023-kroner inkl. mva. Følgende beskrivelse av målbildet ble gitt til Stortinget i Prop. 18 S (2022-2023), side 18:

> «Programmet legg til rette for ei felles løysing som handterer ugradert, ugradert skjermingsverdig og begrensa informasjon. Begrensa informasjon vil bli levert frå Forsvarsdepartementet si plattform. Ugradert og skjermingsverdig ugradert vil bli levert frå den nye verksemda sin plattform. Den nye plattforma vil bli basert på sky-teknologi, i hovudsak som ei privat, lukka løysning. Ein såkalla to-nivåklient for sikker og effektiv behandling av gradert og ugradert informasjon er under utvikling»

I KS2-rapporten vurderte ekstern kvalitetssikrer at gevinstene ved en privat lukket skytjeneste slik som programmet hadde utredet ikke alene sto i forhold til kostnadene ved å anskaffe og etablere en ny plattform. Det ble derfor anbefalt å undersøke om gjenbruk av komponenter fra DSS sin løsning kunne være et godt alternativ til å anskaffe en ny løsning basert på skyteknologi.

Programmet gikk videre med opprinnelig målbilde som hovedalternativ, men gjennomførte samtidig en utredning basert på vurderingene fra ekstern kvalitetssikrer om gjenbruk av komponenter fra eksisterende plattform hos DSS. Det ble vurdert at det var mulig å bygge en ny plattform og å gjenbruke komponenter fra DSS sin løsning i kombinasjon med skyteknologi. Det var ikke tatt stilling til omfanget av gjenbruk av DSS sin løsning på dette tidspunktet. Det ble heller ikke gjort noen særskilte sikkerhetsvurderinger og risikoanalyser utover de vurderingene og analysene som DSS har gjort selv. DSS hadde blant annet gjennomført en penetrasjonstest i regi av NSM hvor de fikk gode tilbakemeldinger på arkitekturen i løsningen.

Basert på utredningen endret programmet målbildet vinteren/våren 2023. Det nye målbildet forutsatte delvis gjenbruk av enkeltkomponenter fra plattformen til DSS. Endret målbilde var gjenstand for ekstern kvalitetssikring (Kontrollpunkt 1) i april 2023. Ekstern kvalitetssikrer støttet det nye målbildet til programmet, men de understreket utfordringene knyttet til å oppgradere infrastruktur til å håndtere et høyere sikkerhetsnivå (fra ugradert til skjermingsverdig ugradert). Det var planlagt å informere Stortinget om endringene i målbildet til programmet høsten 2023 i budsjettprosessen for 2024, etter å ha fått kvalitetssikret det nye målbildet.

Som et resultat av dataangrepet mot DSS sin plattform sommeren 2023, ble tilliten til plattformen svekket. I Prop 1. S (2023-2024) for Forsvarsdepartementet ble det derfor informert om følgende (side 69):

> «I programmet er det blant annet lagt til grunn at DSS' plattform delvis skal kunne gjenbrukes. Som følge av dataangrepet mot DSS` plattform sommeren 2023 vil programmet også vurdere alternative handlingsalternativer som

innebærer etablering av helt ny plattform (…). På grunn av dette kan det være aktuelt å re-planlegge deler av programmet.»

I Prop.104 S (2023-2024) ble Stortinget informert om at dataangrepet mot DSS hadde ført til en ny utredning av flere alternativer for programmets fremtidige plattformløsning, inkludert mindre grad av gjenbruk.

Basert på replanleggingen etter dataangrepet ble et nytt løsningsforslag og målbilde lagt frem for ekstern kvalitetssikrer (Kontrollpunkt 2) våren 2024. Nytt løsningsforslag som ble kvalitetssikret våren 2024 var en hybrid løsning hvor det etableres flere kjøremiljøer for behandling av skjermingsverdig ugradert og ugradert. Den skjermingsverdige ugraderte delen vil leveres som en privat sky av tredjepart i norske datasentre, mens den ugraderte delen vil være delt mellom en del i offentlig sky, og en del i eget datasenter. Sikkerhetsgraderte løsninger vil leveres av Statens graderte plattformtjenester (SGP) som er underlagt Forsvarsdepartementet. En slik hybrid løsning vil sørge for at departementene har fungerende IKT-løsninger i alle deler av krisespekteret. I rapporten fra Kontrollpunkt 2 støttet ekstern kvalitetssikrer programmets oppdaterte kostnadsestimater og de mener at programmet er lønnsomt og bør videreføres. De viser videre til at kostnadsøkningene står i forhold til konsekvensene av dataangrepet sommeren 2023 og de nødvendige endringene. Ekstern kvalitetssikrer vurderte videre at løsningsforslaget vurderes som fornuftig, men at det foreligger en del usikkerheter som det må tas hensyn til i den videre utviklingen.

Anbefalingene og usikkerheten som ble pekt på av ekstern kvalitetssikrer er lagt til grunn i den oppdaterte kostnads- og styringsrammen til programmet. Oppdatert forslag til kostnads- og styringsramme for endringstrinn 1, 2 og 3 ble vedtatt endret gjennom Stortingets behandling av Innst. 7 S (2024-2025) til Prop. 1 S (2024-2025) for Forsvarsdepartementet med en kostnadsramme på 2242 mill. 2025-kroner inkl. mva.

Svar på spørsmål 4

Millioner kroner per år	**2021**	**2022**	**2023**	**2024**
Bevilget budsjett til Felles IKT	80	135	311	396
Overføring, RNB, omgruppering, andre justeringer		18	-139	-211
Til disposisjon	**80**	**153**	**172**	**185**
Regnskap, kontant	**62**	**102**	**158**	**132**

Det er som tidligere omtalt lagt til grunn en smidig metodikk for gjennomføring av programmet. Det innebærer at aktiviteter løpende tilpasses etter hendelser eller strategiske beslutninger som tas underveis. Det gjenspeiles også i de planer og den styrende dokumentasjonen som utarbeides og som har vært gjenstand for ekstern kvalitetssikring.

Programmet opererer med en såkalt produktnedbrytning på det som skal utredes, anskaffes eller produseres. Denne strukturen ligger til grunn for aktivitetsoversikten presentert nedenfor.

Regnskap per aktivitet (mill. kroner)	2021	2022	2023	2024	Totalt
1. Teknisk målbilde for ny felles løsning/IKT-plattform	14	31	43	55	143
2. Opprettelse og operasjonalisering av Departementenes digitaliseringsorganisasjon (DIO)	1	13	33	51	98
3. Utvikling av en tonivåklient for sikker og effektiv behandling av gradert og ugradert informasjon	33	39	58	9	139
4. Programstyring, samfunnsøkonomiske analyser og gevinstplanlegging, finansiering, felleskostnader og ekstern kvalitetssikring	14	19	24	17	74
Totalt per år	**62**	**102**	**158**	**132**	**454**

Nærmere om aktivitetene som er oppført i tabellen:

1. Teknisk målbilde for ny felles løsning / IKT-plattform:

Gjennom programmets utvikling har det vært lagt til grunn forskjellige tilnærminger til målbilder for ny løsning. Det innebærer at løsninger og planer må revideres og justeres. Ressursinnsatsen for dette er i hovedsak innhentet fra departementsfellesskapet og eksterne konsulentselskap. I 2023 arbeidet programmet i hovedsak mot målbildet om gjenbruk av plattform til DSS og utredninger av alternative løsninger etter dataangrepet sommeren 2023. Økningen i kostnaden for 2024 skyldes arbeid for etablering av nytt målbilde, utarbeidelse av konkurranse- og kontraktsgrunnlag for anbudsinnbydelser, utlysninger og dialog med markedet.

2. Opprettelse og operasjonalisering av Departementenes digitaliseringsorganisasjon (DIO)

Etableringen av DIO har krevd at det etableres en egen administrasjon, regnskap, IKT-løsninger, profil, kultur og nye lokaliteter med et tidsriktig arbeidsplassdesign. Ressursinnsatsen er i hovedsak knyttet til utredningsarbeid og tilrettelegging, men også andre nødvendige investeringer for å sikre etableringen.

3. Utvikling av en tonivåklient for sikker og effektiv behandling av gradert og ugradert informasjon

Den nye løsningen som skal tas fram innebærer skyløsninger i allmenn sky, skjermingsverdig ugraderte og ugraderte løsninger i eget datasenter. I tillegg skal departementene gjennom DIO tilbys en lavgradert løsning (NBN). Denne løsningen leveres av Statens Graderte Plattformtjenester (SGP). I den sammenheng er det utviklet en plattform

og en to-nivåklient (PC) som både kan aksessere NBN og ugradert plattform på en enhet sikker måte. Løsningen gjøres klar for å kunne sameksistere med den nye ugraderte løsningen når den settes i drift.

4. Programstyring, samfunnsøkonomiske analyser og gevinstplanlegging, finansiering, felleskostnader og ekstern kvalitetssikring

Denne posten omfatter i hovedsak programmets fellesaktiviteter knyttet til planlegging, etablering av prosjekthåndbok med rutiner og retningslinjer, utvikling av styrende dokumentasjon og fasilitering for KS2 og kontrollpunkt. Videre omfatter det oppfølging av ekstern kvalitetssikrer sine anbefalinger, utarbeidelse av samfunnsøkonomiske analyser, herunder kost- og nytteanalyser og usikkerhetsanalyser. I aktivitetene inngår videre å utarbeide og fremme dokumentasjon for programstyret, økonomioppfølging og analyser; kommunikasjonsplaner; rekruttere ressurser. En viktig del er også sikkerhetsstyring i Programmet, inkludert personellsikkerhet, samt å sørge for egnede lokaler og kommunikasjonsløsninger.

Med hilsen

Karianne Oldernes Tung

STORTINGET

VEDLEGG 6

Statsråd Karianne Oldernes Tung
Digitaliserings- og forvaltningsdepartementet
Postboks 8004 Dep,
0030 Oslo

Vår ref.:	Deres ref.:	Dato:
2025/498		25.03.2025

Vedr. rammeavtaler i staten

Det vises til statsrådens svarbrev datert 14. mars 2025.

I sitt svar skriver statsråden at det var «forprosjektet i programmet» som tok beslutning om å bytte fra Forsvarsdepartementets til DDS sin plattform. I den forbindelse ber komiteen om svar på følgende spørsmål:

1. Konkret på hvilket tidspunkt ble statsråden orientert om det planlagt byttet, og hva foretok hun seg konkret da hun ble kjent med opplysningene?

2. Hvorfor ble det ikke, på tross av en skjerpet sikkerhetspolitisk situasjon, foretatt en sikkerhetsvurdering av byttet?

3. Kan statsråden redegjøre for hvilke konkrete fullmakter som er gitt når målbildet for et så stort og viktig prosjekt kan endres av prosjektet selv? Dersom fullmaktene er skriftliggjort, bes disse oversendt.

4. Hvilke konkrete og/eller skriftlige fullmakter har prosjektet i dag?

5. Til media uttaler statsråden at hun styrer prosjektet «stramt». Kan statsråden gi en konkret redegjørelse for hvordan den stramme styringen arter seg, når valg av målbilde er overlatt til prosjektet selv?

6. Det bes om en konkret fremdriftsplan for prosjektet hvor de viktigste milepælene er tidfestet.

Kontroll- og konstitusjonskomiteen
Stortinget
Postboks 1700 Sentrum
NO-0026 OSLO

Tlf. 23 31 30 50
NO 971 524 960

www.stortinget.no

7. Selv om DSS sin plattform etter hackingen ikke vurderes sikker nok for ny felles IKT-løsning, er den likevel i full bruk i dag. Hvilke sikkerhetsvurderinger har regjeringen gjort rundt dette?

8. En viktig begrunnelse for å etablere en felles IKT-løsning, var å redusere antallet kjøremiljøer til ett. NSM har tydelig uttalt at sikkerheten svekkes ved mange ulike IKT-løsninger. Nå planlegges en hybrid løsning, med fire ulike kjøremiljøer fordelt på privat sky, offentlig sky, eget datasenter og SGP. Hvilke konkrete sikkerhetsvurderinger er gjort knyttet til at det nå tas sikte på fire ulike kjøremiljøer?

9. Hvilke konsekvenser har etableringen av fire ulike kjøremiljøer for kostnadene for ny felles IKT-løsning?

Komiteen ber om svar innen 1. april 2025.

Med vennlig hilsen
Kontroll- og konstitusjonskomiteen

Peter Frølich
komiteleder

VEDLEGG 7

DET KONGELIGE DIGITALISERINGS- OG FORVALTNINGSDEPARTEMENT

Statsråden

Stortingets kontroll- og konstitusjonskomite

0026 Oslo

Deres ref	Vår ref	Dato
	25/504-14	1. april 2025

Spørsmål fra kontroll- og konstitusjonskomiteen vedrørende program for felles IKT-tjenester i departementsfelleskapet

Jeg viser til brev fra Stortingets kontroll- og konstitusjonskomite datert 25. mars 2025 med oppfølgingsspørsmål knyttet til program for felles IKT-tjenester i departementsfellesskapet (programmet). Komiteen viser til at jeg i brev av 14. mars 2025, skriver at det var «forprosjektet i programmet» som tok beslutningen om å bytte fra Forsvarsdepartementets IKT-plattform til IKT-plattformen Depnet/U driftet av daværende Departementenes sikkerhets- og serviceorganisasjons (DSS) (driftes i dag av Departementenes digitaliseringsorganisasjon (DIO)). I den forbindelse ber komiteen om svar på følgende spørsmål:

1. Konkret på hvilket tidspunkt ble statsråden orientert om det planlagte byttet, og hva foretok hun seg konkret da hun ble kjent med opplysningene?
2. Hvorfor ble det ikke, på tross av en skjerpet sikkerhetspolitisk situasjon, foretatt en sikkerhetsvurdering av byttet?
3. Kan statsråden redegjøre for hvilke konkrete fullmakter som er gitt når målbildet for et så stort og viktig prosjekt kan endres av prosjektet selv? Dersom fullmaktene er skriftliggjort, bes disse oversendt.
4. Hvilke konkrete og/eller skriftlige fullmakter har prosjektet i dag?
5. Til media uttaler statsråden at hun styrer prosjektet «stramt». Kan statsråden gi en konkret redegjørelse for hvordan den stramme styringen arter seg, når valg av målbilde er overlatt til prosjektet selv?
6. Det bes om en konkret fremdriftsplan for prosjektet hvor de viktigste milepælene er tidfestet.

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

7. Selv om DSS sin plattform etter hackingen ikke vurderes sikker nok for ny felles IKT-løsning, er den likevel i full bruk i dag. Hvilke sikkerhetsvurderinger har regjeringen gjort rundt dette?
8. En viktig begrunnelse for å etablere en felles IKT-løsning, var å redusere antallet kjøremiljøer til ett. NSM har tydelig uttalt at sikkerheten svekkes ved mange ulike IKT-løsninger. Nå planlegges en hybrid løsning, med fire ulike kjøremiljøer fordelt på privat sky, offentlig sky, eget datasenter og SGP. Hvilke konkrete sikkerhetsvurderinger er gjort knyttet til at det nå tas sikte på fire ulike kjøremiljøer?
9. Hvilke konsekvenser har etableringen av fire ulike kjøremiljøer for kostnadene for ny felles IKT-løsning?

Brevet er skrevet i samarbeid med forsvarsministeren. Forsvarsdepartementet (FD) og Digitaliserings- og forvaltningsdepartementet (DFD) er programeiere for og styrer Program for felles IKT-løsninger i departementsfellesskapet i fellesskap, jf. Stortingets behandling av Prop. 18 S (2022–2023) Endringar i statsbudsjettet 2022 under Forsvarsdepartementet, jf. Innst. 110 S (2022-2023), 6. desember 2022:

> «II Stortinget samtykker i at Forsvarsdepartementet og Kommunal- og distriktsdepartementet kan iverksette Program felles IKT-tenester i departementsfellesskapet med ei kostnadsramme på 1 392 mill. 2023-kroner for endringstrinn 1 og 2.»

Budsjettmidlene for programmet bevilges over FDs budsjett, kap. 1700, post 22. FD og DFD er programeiere og styrer programmet i fellesskap. Dette inkluderer å ta sentrale beslutninger, som for eksempel beslutninger i forprosjektet om den framtidige plattformen for departementenes framtidige IKT-løsning. Jeg kommer nærmere tilbake til styringen av programmet i svaret på spørsmål 5 nedenfor.

Jeg vil også klargjøre tidsforløpet knyttet til beslutninger om valg av plattform for departementenes framtidige IKT-løsning.

Det ble under forrige regjering våren 2021 satt i gang en ekstern kvalitetssikring av styringsunderlag samt kostnadsoverslag (såkalt KS2) for en felles IKT-løsning for departementsfellesskapet. I henhold til statens prosjektmodell skal KS2 være gjennomført før forslag til kostnadsramme legges fram for Stortinget. I forprosjektet som forelå på dette tidspunktet, var det lagt til grunn at departementene skulle ta i bruk FDs IKT-plattform. Kvalitetssikringen som ble påbegynt under forrige regjering våren 2021 ble stoppet. Ekstern kvalitetssikrer mente at styringsdokumentene som forelå ikke tilfredsstilte kravene for KS2, og at det derfor ikke var grunnlag for videre kvalitetssikring. I stedet ble det planlagt et tidsløp med sikte på å ha utarbeidet et ferdig forprosjekt innen utgangen av 2021.

Det var i forbindelse med sluttføringen av dette reviderte forprosjektet – vinteren 2021–2022 – at FD og daværende Kommunal- og distriktsdepartementet (KDD) la til grunn at departementenes framtidige IKT-plattform skulle basere seg på en privat lukket skyløsning

levert fra en tredjepart. Utviklingen på IKT-området og kartlegginger av departementenes behov for digitale tjenester og applikasjoner, gjorde det nødvendig å se på alternativer til plattformer som ikke ville legge like store begrensninger på brukerne som FDs plattform ville gjøre. Vurderingene var at FDs plattform måtte ha et høyt sikkerhetsnivå og -løsninger, siden den også skulle behandle lavgradert (BEGRENSET) informasjon. Dette ville kreve at man måtte være meget restriktiv med hvilke applikasjoner og tjenester som kunne legges på FDs plattform. Mesteparten av informasjonen som departementene håndterer, og applikasjonene de bruker for å behandle den, krever ikke et like høyt sikkerhetsnivå som FDs plattform har. En eventuell migrering til FDs plattform ville derfor lagt store og unødvendige begrensninger på hvilke applikasjoner og tjenester departementsfelleskapet kunne brukt, noe som ville vært lite hensiktsmessig. Videre la FD og daværende KDD til grunn at FDs plattform skulle brukes for behandling av lavgradert (BEGRENSET) informasjon.

Ekstern kvalitetssikring (KS2) ble avsluttet våren 2022 (les rapporten her). Kvalitetssikrerne ga tilslutning til å jobbe videre med privat lukket skytjeneste som ny felles IKT-plattform. De påpekte samtidig at utfallsrommet var stort, og anbefalte å vurdere om en videreutvikling av eksisterende plattform – Depnet/U – levert fra daværende Departementenes sikkerhets- og serviceorganisasjon (DSS) (leveres i dag fra Departementenes digitaliseringsorganisasjon (DIO)) kunne gi tilsvarende gevinster.

På bakgrunn av anbefalingene fra ekstern kvalitetssikrer, la regjeringen i Prop. 18 S (2022–2023) fram forslag om oppstart av Program felles IKT-tjenester for departementsfellesskapet. I proposisjonen redegjorde regjeringen for at plattformen for ugradert og skjermingsverdig ugradert informasjon skulle baseres på skyteknologi, i hovedsak som en privat lukket løsning. Videre ble det påpekt at programmets gjennomføring skulle baseres på smidig og fleksibel metodikk. Dette er fordi usikkerheten til programmet gjør at nye utfordringer vil kunne dukke opp underveis, og dette må håndteres gjennom så vel planlegging som gjennomføring. På bakgrunn av ekstern kvalitetssikrers anbefalinger, la regjeringen opp til tre kontrollpunkter i gjennomføringen av programmet underveis. Stortinget vedtok regjeringens forslag, jf. behandlingen av Innst. S 110 (2022–2023). Ingen av komiteens medlemmer hadde merknader til valget av plattform levert som en privat lukket skyløsning.

I løpet av våren 2023 fulgte programmet, under ledelse av FD og daværende KDD, opp anbefalingene fra ekstern kvalitetssikring om å vurdere bruk av enkeltkomponenter fra Depnet/U. Det endrede målbildet var gjenstand for ekstern kvalitetssikring (Kontrollpunkt 1) i april 2023. FD og KDD skulle etter planen informere Stortinget om endringene i målbildet til programmet høsten 2023 – i budsjettprosessen for 2024 – etter at den eksterne kvalitetssikringen var ferdig.

Før FD og KDD rakk å informere Stortinget om det endrede målbildet ved å delvis gjenbruke enkeltkomponenter fra Depnet/U, istedenfor å anskaffe en helt ny plattform, ble Depnet/U utsatt for et dataangrep. Dataangrepet skjedde sommeren 2023 ved at en avansert og ressurssterk trusselaktør utnyttet en såkalt nulldagssårbarhet i den gamle løsningen for synkronisering av e-post på mobile enheter. En nulldagssårbarhet utgjør en mulighet for en

trusselaktør til å utnytte en sårbarhet som produsenten og brukerne ikke er kjent med. Dataangrepet gjorde at det igjen ble behov for å vurdere handlingsalternativer som innebærer etablering av helt ny plattform. Regjeringen informerte Stortinget om dette i flere runder, jf. Prop 1. S (2023–2024) og Prop.104 S (2023-2024) for Forsvarsdepartementet.

Basert på replanleggingen av programmet etter dataangrepet høsten 2023 og vinteren 2023/2024, ble et nytt løsningsforslag og målbilde lagt frem for ekstern kvalitetssikrer (kontrollpunkt 2) våren 2024. Det nye løsningsforslaget som ble kvalitetssikret våren 2024, var en hybrid løsning hvor det etableres flere kjøremiljøer for behandling av skjermingsverdig ugradert og ugradert. Disse kjøremiljøene danner en helhetlig og samlet løsning. Basert på anbefalingene og usikkerheten som ble pekt på av ekstern kvalitetssikrer våren 2024, fremmet regjeringen forslag om oppdaterte kostnads- og styringsrammer for programmet for endringstrinn 1, 2 og 3, for Stortinget høsten 2024. Oppdatert forslag ble vedtatt endret gjennom Stortingets behandling av Innst. 7 S (2024–2025) til Prop. 1 S (2024–2025) for Forsvarsdepartementet

Så til de konkrete spørsmålene fra komiteen:

1. Konkret på hvilket tidspunkt ble statsråden orientert om det planlagt byttet, og hva foretok hun seg konkret da hun ble kjent med opplysningene?

Som jeg har redegjort for ovenfor, ble beslutningen om ikke å bruke FDs IKT-plattform for håndtering av ugradert og skjermingsverdig ugradert informasjon tatt før jeg tiltrådte som statsråd. Beslutningen er forankret i Stortinget, jf. Innst. S 110 (2022–2023).

2. Hvorfor ble det ikke, på tross av en skjerpet sikkerhetspolitisk situasjon, foretatt en sikkerhetsvurdering av byttet?

FD og DFD vurderte at det ikke var behov for å gjennomføre en egen sikkerhetsvurdering av Depnet/U, som følge av endret målbilde til å gjenbruke enkeltkomponenter fra denne plattformen. Dette fordi vi hadde et godt nok informasjonsgrunnlag om Depnet/U. Nasjonal sikkerhetsmyndighet (NSM) gjennomførte en penetrasjonstest[1] av Depnet/U i 2022. Penetrasjonstesten ga gode tilbakemeldinger, og på bakgrunn av dette vurderte FD og DFD at det ikke var behov for en ny sikkerhetsvurdering av Depnet/U. Komponenter for gjenbruk kan være utstyr, design av løsning, sikkerhetskomponenter og andre komponenter som kan brukes som utgangspunkt for å bygge en ny felles løsning. Det er fortsatt aktuelt at enkeltkomponenter fra eksisterende løsninger gjenbrukes i ny løsning.

Gjennom hele perioden med planlegging og gjennomføring av programmet har det vært lagt til grunn at den valgte plattformløsningen skal sikkerhetsgodkjennes av NSM. Programmet, under ledelse av FD og DFD, og i samråd med Justis- og beredskapsdepartementet (JD),

[1] Penetrasjonstesting er en metodikk for sikkerhetstesting der et system, applikasjon, nettverk eller infrastruktur, med tillatelse, utsettes for simulerte angrep for å avdekke sårbarheter. Hensikten er å avdekke sårbarheter (og oppfølgingstiltak) ved å bruke de samme fremgangsmåtene og teknikkene som en ondsinnet hacker ville brukt.

jobber nå tett med NSM for å sørge for at ny felles løsning blir sikkerhetsgodkjent etter at løsningen er ferdig etablert.

3. Kan statsråden redegjøre for hvilke konkrete fullmakter som er gitt når målbildet for et så stort og viktig prosjekt kan endres av prosjektet selv? Dersom fullmaktene er skriftliggjort, bes disse oversendt.
4. Hvilke konkrete og/eller skriftlige fullmakter har prosjektet i dag?
5. Til media uttaler statsråden at hun styrer prosjektet «stramt». Kan statsråden gi en konkret redegjørelse for hvordan den stramme styringen arter seg, når valg av målbilde er overlatt til prosjektet selv?

Innledningsvis vil jeg starte med å avkrefte at endringer i målbildet til programmet, eller andre sentrale veivalg, har vært overlatt til programmet selv. Dette medfører ikke riktighet. Alle beslutninger om målbildet for programmet er tatt av FD og KDD/DFD, etter forankring og behandling i programstyret (se omtale under). Viktige beslutninger er på ordinær måte forankret i regjeringen.

Siden denne regjeringen tiltrådte, har programmet vært styrt av FD og KDD/DFD i fellesskap. Som en del av styringen er det etablert et programstyre ledet av FD og DFD (KDD før 2024), med representanter fra Utenriksdepartementet, JD, og DSS. Fra høsten 2023 har Statsministerens kontor også vært representert. Fra etableringen av DIO 1. januar 2025 har også DIO vært representert. Representantene er departementsråder, ekspedisjonssjefer og etatsledere, og representerer således den administrative toppledelsen fra sine respektive virksomheter. Det gjennomføres programstyremøter minimum en gang i måneden, i tillegg til ekstraordinære møter ved behov. Videre har FD og DFD faste ukentlige statusmøter om programmet.

Programmet gjennomføres etter anerkjent prosjektmetodikk – Prince2, MSP og statens prosjektmodell. Programkontoret utarbeider utredninger og anbefalinger, og legger dette frem for programstyret og programeierne. Eierne styrer programmet, tar beslutninger og løfter saker videre til regjeringen og Stortinget der dette er nødvendig.

Programmet arbeider etter de fullmaktene som er nedfelt i programmets styrende dokumentasjon i henhold til statens prosjektmodell, programmandatet og eventuelle beslutninger som tas i regjeringen og Stortinget. Programmet er underlagt statens prosjektmodell og gjennomgår jevnlige kvalitetssikringer av ekstern kvalitetssikrer.

Programmet og programstyret følger opp de påpekningene og vurderingene som gjøres av kvalitetssikrer. Det er gjennomført KS2, og to kontrollpunkter så langt i programmets levetid. Det planlegges også for et tredje kontrollpunkt når man kommer nærmere tidspunktet for overgang til ny plattform.

6. Det bes om en konkret fremdriftsplan for prosjektet hvor de viktigste milepælene er tidfestet.

Under følger en tabell som viser de viktigste milepælene for programmet (både historiske milepæler og milepæler fremover i tid).

Milepæler	**Tid (halvår)**
Oppstart forprosjekt for program Felles IKT (i nåværende form)	H1 2021
Besluttet privat lukket skyløsning til departementsfellesskapet	H2 2021
Oppstart gjennomføring av ekstern kvalitetssikring (KS2)	**H2 2021**
Gjennomført KS2	**H1 2022**
Oppstart Endringstrinn 1 (Q1 2022–Q1 2024) – Innledende fase	H1 2022
Videreutviklet målbilde for teknisk arkitektur, basert på KS2-rapport, legges til grunn for den videre planleggingen og arbeidet i programmet.	H2 2022
Gjennomføring av eksternt kontrollpunkt 1 (KP1) med utgangspunkt i revidert styringsdokumentasjon for programmet	**H1 2023**
Utredning av alternative løsninger grunnet dataangrepet	H2 2023
Avslutning Endringstrinn 1 og oppstart Endringstrinn 2 (Q1 2024–Q4 2026) – Gjennomføringsfase	H1 2024
Gjennomføring av eksternt kontrollpunkt 2 (KP2) med utgangspunkt i revidert styringsdokumentasjon for programmet, inkl. justering av programmets tekniske målbilde pga. dataangrep	H1 2024
Omstilling fra eksisterende IKT-organisasjon til ny virksomhet gjennomført	H1 2024
Igangsettelse av utarbeidelse av konkurransegrunnlag for ny løsning	H1 2024
Departementenes digitaliseringsorganisasjon (DIO) er etablert og i drift pr. 1.1.2025	H1 2025
Kontraktsignering av sentral infrastruktur og transisjon (Q2 2025)	H1 2025
Test av ny løsning	H2 2025
Tentativt tidspunkt for gjennomføring av eksternt kontrollpunkt 3 (KP3)	**H1 2026**
Transisjon fra eksisterende løsninger over på ny felles løsning	2026–2027
Avslutning Endringstrinn 2 og oppstart Endringstrinn 3 (Q4 2026–Q3 2027) – Avsluttende fase	H2 2026
Tentativt tidspunkt for avslutning av programmet	H2 2027

Programgjennomføringen, som startet i 2022, er inndelt i endringstrinn. Inndelingen i endringstrinn sikrer en trinnvis leveranse av programmets omfang. Hvert endringstrinn har en klar målsetning og er utformet for å være håndterbart med tanke på omfang, kompleksitet og varighet. Flere programtiltak kan inngå i et endringstrinn, og disse kan strekke seg over ett eller flere endringstrinn.

Programmets inndeling i endringstrinn:

- **Endringstrinn 1 (Q1 2022–Q1 2024): Innledende fase**

- **Endringstrinn 2 (Q1 2024–Q4 2026): Gjennomføringsfase**

    - *Endringstrinn 2A (Q1 2024–Q4 2024)*
        - *Ferdigstille av Prosjekt Organisering og ansvar (OA-prosjektet)*

        - *Ny løsning: Plan og anskaffelsesfase*

    - *Endringstrinn 2B (Q1 2025–Q4 2025)*
        - *Eventuell bistand/etterarbeid i etterkant av OA-prosjektet*
        - *Ny løsning: Kontraktsinngåelse og etableringsfase (basisplattform/pilotering, starte migrering av tjenester)*

    - *Endringstrinn 2C (Q1 2026–Q4 2026)*
        - *Ny løsning: Etableringsfase (migrering av tjenester, transisjon av brukere, sanering)*

- **Endringstrinn 3 (Q4 2026–Q3 2027): Avsluttende fase – sanering av utgående ugraderte plattformer og stabilisering av ny løsning**

7. Selv om DSS sin plattform etter hackingen ikke vurderes sikker nok for ny felles IKT-løsning, er den likevel i full bruk i dag. Hvilke sikkerhetsvurderinger har regjeringen gjort rundt dette?

Både daværende DSS (DIO i dag), i samråd med sine sikkerhetsleverandører, og NSM, gjennomførte vurderinger av tilstanden/risikoen til Depnet/U etter dataangrepet sommeren 2023. Risikovurderingene av Depnet/U etter dataangrepet er graderte, og omtales derfor ikke nærmere her.

8. En viktig begrunnelse for å etablere en felles IKT-løsning, var å redusere antallet kjøremiljøer til ett. NSM har tydelig uttalt at sikkerheten svekkes ved mange ulike IKT-løsninger. Nå planlegges en hybrid løsning, med fire ulike kjøremiljøer fordelt på privat sky, offentlig sky, eget datasenter og SGP. Hvilke konkrete sikkerhetsvurderinger er gjort knyttet til at det nå tas sikte på fire ulike kjøremiljøer?
9. Hvilke konsekvenser har etableringen av fire ulike kjøremiljøer for kostnadene for ny felles IKT-løsning?

NSMs uttalelser om ulike kjøremiljøer handler om at det er høyere risiko knyttet til utveksling av informasjon og integrasjoner mellom separerte plattformer/systemer fremfor at kjøremiljøene samles på en felles plattform.

I dag er det fire ulike IKT-plattformer med forskjellige kjøremiljøer for ugraderte tjenester i departementsfellesskapet. FD og DFD, gjennom programmet, etablerer nå én felles IKT-plattform, som vil sikre enhetlig administrasjon og sikkerhetsløsninger på ulike nivår, for både detektering, sikring og skadebegrensning ved angrep.

Ny felles plattform vil være en hybrid løsning hvor det etableres flere kjøremiljøer for behandling av skjermingsverdig ugradert og ugradert. Disse kjøremiljøene vil sammen danne ett enhetlig kjøremiljø. Dette enhetlige kjøremiljøet vil ha en rekke felles sikkerhetsmekanismer mellom moduler for behandling av henholdsvis ugradert og ugradert

skjermingsverdig informasjon, i en egen «privat sky» på bakken, samt integrasjoner for bruk av allmenne skytjenester som sikrer at departementene har tilgang på den nyeste teknologien. Det er viktig at departementenes ulike verdier sikres på riktig nivå, og at vi ikke skaper unødvendige begrensninger for oss selv. Det er nettopp dette den nye felles løsningen gir oss mulighet til. De differensierte sikkerhetsnivåene gjør at vi kan sikre verdiene våre på en hensiktsmessig måte, samtidig som vi sørger for at departementene har tilgang på effektive og moderne digitale verktøy.

Etablering og drift av én ny felles IKT-plattform istedenfor flere separate plattformer, vil sikre at vi oppnår standardisering og stordriftsfordeler, gjennom mer effektiv ressursbruk og bedre utnytelse av spisskompetansen innenfor IKT-sikkerhet og digitale tjenester. Vi går bort fra å drifte flere separate og forskjellige miljøer og løsninger, slik vi gjør i dag.

Med hilsen

Karianne Oldernes Tung

STORTINGET

VEDLEGG 8

Statsråd Karianne Oldernes Tung
Digitaliserings- og forvaltningsdepartementet
Postboks 8004 Dep
0030 Oslo

Vår ref.:	Deres ref.:	Dato:
2025/498		16.05.2025

Program for felles IKT-tjenester i departementsfellesskapet

Kontroll- og konstitusjonskomiteen viser til sak om program for felles IKT-tjenester i departementsfellesskapet og kontrollhøring mandag 12. mai 2025.

Representanten Lysbakken hadde under høringen flere spørsmål vedrørende det faglige grunnlaget for veivalgene i programmet, herunder for skiftet av målbildet vinteren 2023.

Komiteen ber om å få oversendt dokumentasjon etterspurt i høringen, om nødvendig unntatt offentlig innyn. Av hensyn til fremdriften i saken ber komiteen om å få svar innen 21. mai 2025.

Med vennlig hilsen
Kontroll- og konstitusjonskomiteen

Peter Frølich
komitéleder

Kontroll- og konstitusjonskomiteen
Stortinget
Postboks 1700 Sentrum
NO-0026 OSLO

Tlf. 23 31 30 50
NO 971 524 960

www.stortinget.no

VEDLEGG 9

DET KONGELIGE DIGITALISERINGS- OG FORVALTNINGSDEPARTEMENT

Statsråden

Stortingets kontroll- og konstitusjonskomite
0026 OSLO

Deres ref	Vår ref	Dato
	25/504-27	22. mai 2025

Sak om program for felles IKT-tjenester til departementsfelleskapet – Ber om dokumentasjon etterspurt i høringen

Jeg viser til brev fra Kontroll- og konstitusjonskomiteen datert 16. mai 2025, med bestilling av dokumentasjon som ble etterspurt i høringen, relatert til veivalgene i programmet.

Brevet er skrevet i samarbeid med forsvarsministeren.

Vi vil understreke at det faglige grunnlaget som ligger til grunn for veivalgene i program for felles IKT-tjenester til departementsfelleskapet er sammensatt og består av flere programstyredokumenter, underlag til kvalitetssikring, kvalitetssikringsrapporter m.m. Dette er en stor dokumentmengde, og vi har derfor valgt ut de dokumentene som best belyser grunnlaget for endringene i de tekniske målbildene som programmet har vært igjennom. Programmet opererer med en smidig metodikk, og foreslått teknisk løsning vil derfor bli mer og mer detaljert utover i programperioden.

Vedlagt dette brevet er følgende dokumenter:

- Opprinnelig teknisk målbilde med anskaffelse av privat skyløsning for behandling av ugradert informasjon (KS2).
    - 24.09.21 Sak 5A Privat skyløsning for U-applikasjoner (u. off.)
    - 22.10.21 Sak 6A Anskaffelse av Privat lukket skyløsning
    - Target Operating Model (TOM) – program for felles IKT v. 1.0
    - KS2 av felles IKT-tjenester for departementsfelleskapene

- Nytt teknisk målbilde basert på gjenbruk av enkeltkomponenter fra eksisterende plattformer (hovedsakelig Depnett/U)

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

    - 09.09.22 Sak 6A Teknisk arkitektur innretning og konsekvenser
    - 09.09.22 Sak 6B Overordnet behovsanalyse v. 1.0
    - Target Operating Model (TOM) – program for felles IKT v. 2.0
    - Supplerende analyse, kontrollpunkt 1 av felles IKT-tjenester for departementsfelleskapet

- Nytt teknisk målbilde etter dataangrepet mot Depnet/U.
    - 26.01.24 Sak 6A Strategisk valg av vei for etablering av ny plattform
    - 26.01.24 Sak 6A Vedlegg faseplan og anskaffelsesfase for ny løsning
    - 26.01.24 Sak 6A Vedlegg Juridisk vurdering for anskaffelse og konsekvenser for gjennomføring av ny IKT-løsning
    - 26.01.24 Sak 6A Vedlegg Revidert strategi for realisering av ny IKT-løsning.
    - Target Operating Model (TOM) – program for felles IKT v. 3.0
    - 13.05.25 Sak 6B vedlegg Sourcingstrategi ny løsning
    - Supplerende analyse, kontrollpunkt 2 av felles IKT-tjenester for departementsfelleskapet.

Dokumentene som ligger vedlagt dette brevet vil gi en vesentlig innsikt i teknisk innretning og vurderinger knyttet til IKT-systemene til departementsfelleskapet. Hvis informasjonen blir kjent for uvedkommende vil dette kunne bidra til å lette straffbare handlinger slik som etterretningsvirksomhet. Dokumentene er derfor **unntatt offentlighet med hjemmel i offentleglova § 24, tredje ledd**. Dette gjelder ikke kvalitetssikringsrapportene som allerede ligger åpent tilgjengelig.

Henvisninger til beslutninger i regjering er sladdet.

Med hilsen

Karianne Oldernes Tung

Svanemerket trykksak, 2041 0654