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