STORTINGET

Innst. 318 S

(2023–2024)

Innstilling til Stortinget
fra kontroll- og konstitusjonskomiteen

Dokument 3:11 (2023–2024)

Innstilling fra kontroll- og konstitusjonskomiteen om Riksrevisjonens undersøkelse av Informasjonssikkerhet i forskning innenfor kunnskapssektoren

Til Stortinget

1. Sammendrag

1.1 Innledning

Sikkerhetssituasjonen innenfor høyere utdannings- og forskningssektoren har blitt mer utfordrende de siste årene. Antallet registrerte dataangrep mot sektoren økte kraftig på verdensbasis både i 2020 og 2021. Sikkerhetssituasjonen ble ytterligere skjerpet da Russland invaderte Ukraina i 2022. I sine risikovurderinger for 2020, 2021, 2022 og 2023 har PST, Etterretningstjenesten og NSM pekt på at norske forskningsmiljøer er utsatte etterretningsmål. Direktoratet for høyere utdanning og kompetanse (HK-dir) rapporterer også om en sikkerhetssituasjon preget av større trusler og flere hendelser i Norge.

I tillegg til trusselen fra utenlandsk etterretning vil også kriminelle aktører ha interesse for forskningsdata og -systemer. Politiets trusselvurdering 2023 anser løsepengevirus rettet mot bedrifter og virksomheter som den største kriminalitetstrusselen mot IT-sikkerhet og digital infrastruktur. I sin risiko- og tilstandsvurdering for 2023 vurderer HK-dir at risikoen for løsepengevirus, som fører til brudd på informasjons- og personopplysningssikkerheten, er høy innenfor forsknings- og utdanningssektoren.

En sentral årsak til at sektoren er interessant for angripere, er at den inneholder store informasjonsverdier i form av forskningsdata. Svak sikring av forskningsdata kan potensielt få store økonomiske konsekvenser, føre til spredning av sensitive opplysninger som personopplysninger og forretningshemmeligheter og gjøre at virksomhetene taper omdømme. Noen universiteter og høyskoler forsker på områder som er viktige for å sikre nasjonale interesser, for eksempel forskning på olje og energi, elektronisk kommunikasjon (ekom), forsvarsmateriell og annen flerbruksteknologi.

Det er et viktig prinsipp for offentlig finansierte forskningsdata at disse skal være «så åpne som mulig, så lukkede som nødvendig». Prinsippet innebærer en forventning om at forskningsdata skal tilrettelegges for åpen tilgang så framt ikke hensynet til sikkerhet, personvern, immaterielle rettigheter, forretningshemmeligheter og lignende tilsier at dataene må skjermes. Virksomhetene må finne en balanse mellom disse hensynene. Samtidig begrenser ikke trusselen mot forskning seg kun til sensitive kunnskapsområder. En angriper kan også gjøre utilgjengelig eller slette andre viktige forskningsdata eller manipulere dataene. Mer generelt vil tilliten til forskning svekkes hvis det mistenkes at eksterne aktører har hatt tilgang til forskningen og resultatene av den.

Målet med undersøkelsen har vært å vurdere

- hvordan forskningsinstitusjoner under Kunnskapsdepartementet sikrer forskningsdata mot dataangrep, og
- hvordan departementet ivaretar sitt overordnede ansvar for informasjonssikkerhet i høyere utdanning og forskning.

Med forskningsinstitusjoner under Kunnskapsdepartementet mener Riksrevisjonen universiteter, høyskoler og andre virksomheter under departementet som driver med forskning.

Undersøkelsen har blant annet tatt utgangspunkt i følgende vedtak og forutsetninger fra Stortinget:

- Lov om behandling av personopplysninger
- Lov om helseregistre og behandling av helseopplysninger
- Lov om medisinsk og helsefaglig forskning
- Lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v.
- Lov om nasjonal sikkerhet
- Bevilgningsreglementet
- Reglement for økonomistyring i staten
- Innst. 275 S (2020–2021) Innstilling fra justiskomiteen om Samfunnssikkerhet i en usikker verden, jf. Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden
- Innst. 187 S (2017–2018) Innstilling fra justiskomiteen om IKT-sikkerhet. Et felles ansvar, jf. Meld. St. 38 (2016–2017) IKT-sikkerhet. Et felles ansvar
- Prop. 1 S (2018–2019) Kunnskapsdepartementet, jf. Innst. 12 S (2018–2019)
- Instruks for departementenes arbeid med samfunnssikkerhet

Riksrevisjonen har gjennomført undersøkelser hos til sammen ti forskningsinstitusjoner under Kunnskapsdepartementet. For alle virksomhetene har Riksrevisjonen undersøkt tekniske og organisatoriske sikkerhetstiltak, og systematikken i arbeidet med informasjonssikkerhet. I tre av virksomhetene har Riksrevisjonen gått mer i dybden, og blant annet gjennomført inntrengingstester.

Et sentralt metodisk grep i undersøkelsen er å sammenligne det Riksrevisjonen har funnet i alle de ti virksomhetene med god praksis, som framgår av anerkjente standarder for informasjonssikkerhet. Riksrevisjonen har i hovedsak tatt utgangspunkt i følgende standarder:

- Center for Internet Security (2021) CIS Controls, version 8
- Nasjonal Sikkerhetsmyndighet (2020) Grunnprinsipper for IKT-sikkerhet, versjon 2.0
- Informasjonsteknologi – Sikringsteknikker – Tiltak for informasjonssikring, NS-ISO/IEC 27002:2017
- NS-ISO/IEC 27001:2017 – Ledelsessystemer for informasjonssikkerhet.

De tre virksomhetene i dybdeundersøkelsene ble informert om alle svakheter Riksrevisjonen fant gjennom inntrengingstestene, like etter at disse var gjennomført. Alle de ti virksomhetene fikk en presentasjon av svakheter som ble avdekket gjennom kartlegging av tekniske sikkerhetstiltak.

Undersøkelsen omfatter i hovedsak perioden 2019–2022.

Rapporten ble forelagt Kunnskapsdepartementet ved brev 29. september 2023. Departementet har i brev 27. oktober 2023 gitt kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i rapporten og i Riksrevisjonens dokument.

Riksrevisjonen har hatt en dialog med Kunnskapsdepartementet om hvilke opplysninger som bør utelates fra dette dokumentet, og om behov for skjerming av opplysninger i den mer detaljerte forvaltningsrevisjonsrapporten. I den forbindelse har Riksrevisjonen også fått råd fra Nasjonal sikkerhetsmyndighet (NSM).

Rapporten, riksrevisorkollegiets oversendelsesbrev til departementet 23. november 2023 og statsrådens svar 8. desember 2023 følger som vedlegg til Riksrevisjonens dokument.

1.2 Konklusjoner

- Forskningsdata i forskningsinstitusjonene under Kunnskapsdepartementet er ikke i tilstrekkelig grad sikret mot dataangrep.
  - Inntrengingstester mot tre virksomheter ga full kontroll over IT-infrastruktur ved to av dem, og kontroll over forskeres IT-utstyr og skylagring ved det tredje.
  - Det er stor variasjon i gjennomføringen av tekniske sikkerhetstiltak, og mange av virksomhetene har vesentlige svakheter.
  - Det er svakheter i organisatoriske sikkerhetstiltak som er etablert for å beskytte forskningsdata.
- Virksomhetene har i stor grad lagt rammene for informasjonssikkerhetsarbeidet, men oppnår ikke ønsket sikkerhetsnivå på grunn av mangler i gjennomføringen.
- Kunnskapsdepartementet har justert virkemiddelbruken de siste årene, men det er en del utfordringer i sektoren som dagens virkemidler ikke treffer.
  - Styringsmodellen for informasjonssikkerhet har gjort at den enkelte forskningsvirksomhet har fått tettere oppfølging.
  - Kunnskapsdepartementet har i begrenset grad lyktes med å nå målet med informasjonssikkerhetssatsningen, og virkemidlene treffer i for liten grad virksomhetene som har størst behov for støtte.
- Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og risikoreduserende tiltak som er besluttet på sektornivå, blir ikke fulgt opp.

1.3 Overordnet vurdering

- Det er kritikkverdig at forskningsdata i virksomheter under Kunnskapsdepartementet ikke er tilstrekkelig sikret mot dataangrep, gitt kravene i lovverket og de mulige konsekvensene av at sensitive data kommer på avveier.
- Virksomhetene har ikke god nok oversikt over forskningsdata som trenger beskyttelse. Dette er ikke tilfredsstillende.
- Tross forbedringer i undersøkelsesperioden, arbeider mange virksomheter i for liten grad systematisk med informasjonssikkerhet, og styrene i virksomhetene fyller ikke i stor nok grad rollen de skal ha. Dette er ikke tilfredsstillende.
- Kunnskapsdepartementet har gjennomført flere tiltak i perioden 2019–2022 som blant annet har ført til økt oppmerksomhet om informasjonssikkerhet i virksomhetene. Samtidig er det ikke tilfredsstillende at virkemidlene i for liten grad treffer virksomhetene som har størst behov for støtte.
- Det er ikke tilfredsstillende at departementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og at risikoreduserende tiltak ikke blir fulgt opp.

1.4 Utdyping av konklusjoner

1.4.1 Forskningsdata i forskningsvirksomhetene under Kunnskapsdepartementet er ikke i tilstrekkelig grad sikret mot dataangrep

Forskningsdata skal i hovedsak tilrettelegges for åpen tilgang, men hensyn til sikkerhet, personvern, immaterielle rettigheter, forretningshemmeligheter og lignende tilsier i en del tilfeller at forskningsdata ikke kan gjøres helt åpent tilgjengelige. En rekke lover og regler stiller krav til hvordan slike data skal sikres. Lovverket stiller også konkrete krav til virksomhetene om at de skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er tilpasset risikoen. For å oppnå dette bør virksomhetene følge faglige standarder som angir god praksis.

Etter Riksrevisjonens vurdering er forskningsdata i virksomheter under Kunnskapsdepartementet ikke tilstrekkelig sikret mot dataangrep, gitt kravene i lovverket.

1.4.1.1 Inntrengingstester mot tre forskningsinstitusjoner ga full kontroll over IT-infrastruktur ved to av dem og kontroll over forskeres IT-utstyr og skylagring ved det tredje

Forskningsinformasjon og kunnskap generert av forskning kan være av stor interesse både for etterretningsorganisasjoner og kommersielle virksomheter. Det samles også inn store mengder, til dels sensitive, forskningsdata om personer som mange aktører kan ha interesse av og kan forsøke å utnytte blant annet i kriminell virksomhet. Riksrevisjonen gjennomførte inntrengingstester mot tre forskningsinstitusjoner for å teste hvor godt forskningsdata var beskyttet. Målet i testene var å få tilgang til sensitive forskningsdata, enten ved å få kontroll over IT-infrastruktur eller ved å utnytte tilgangsrettighetene den enkelte forsker har.

Inntrengingstestene ved to av virksomhetene ga full kontroll over IKT-infrastrukturen som benyttes av ansatte og studenter i deres daglige arbeid. Ved en av dem ble dette oppnådd den første dagen av inntrengingstesten, og det ble funnet flere veier som kunne gi slik kontroll.

Oppnådd kontroll innebar at Riksrevisjonen kunne administrere alle brukerkontoer, PC-er og servere. Med slik tilgang kunne Riksrevisjonen tildele seg selv alle ønskede rettigheter og skaffe tilgang til all informasjon lagret i dette nettverket, inkludert sensitiv forskningsinformasjon. Med de oppnådde rettighetene, hadde det også vært mulig å endre, slette eller kryptere all informasjon dersom motivasjonen hadde vært økonomisk vinning eller sabotasje.

Ved den tredje forskningsinstitusjonen fikk Riksrevisjonen kontroll med de fleste PC-er benyttet av ansatte, noe som ga muligheter til å hente ut eller manipulere informasjon lagret lokalt på PC-er og på eiernes skylagringsløsning. Denne skylagringsløsningen kan ut fra retningslinjer benyttes for sensitive forskningsdata (opp til nivået «fortrolig») ved flere av forskningsinstitusjonene. Tilgangen oppnådd kunne videre vært brukt til et målrettet angrep mot utvalgte forskere med kunnskap og tilgang til informasjon som angriperen ønsker tilgang til. Riksrevisjonen fikk ikke kontroll med servere og datanettverk generelt ved den tredje forskningsinstitusjonen, fordi de sentrale delene av IT-infrastrukturen er bedre beskyttet.

Et av formålene med inntrengingstestene var å undersøke virksomhetenes evne til å oppdage aktiviteter i et dataangrep. Riksrevisjonen gjorde ingen forsøk på å skjule de simulerte angrepene, men produserte mye nettverkstrafikk og kjente tegn på angrep. Ved to av virksomhetene ble få eller ingen av aktivitetene i inntrengningstestene oppdaget. Ved den siste virksomheten ble inntrengingstesten oppdaget den fjerde testdagen, og de fleste aktivitetene ga spor i logger som kunne gi virksomheten et bilde av hvordan angrepet hadde blitt gjennomført og hvilke systemer som var berørte.

Noe sensitiv forskningsinformasjon er lagret i særskilte tjenester som er satt opp for å gi informasjonen bedre beskyttelse. Disse tjenestene har ikke vært omfattet av inntrengingstesten. Kontrollen oppnådd over forskeres brukerkontoer og IT-utstyr kunne imidlertid

vært brukt som utgangspunkt for et angrep for å få tilgang også til informasjon som forskere har lagret her.

De tre virksomhetene som ble testet har alle planlagt og til dels gjennomført en rekke tiltak som øker deres sikkerhet i etterkant av undersøkelsene. De konkrete svakhetene som ble utnyttet i inntrengingstestene er utbedret.

Inntrengingstestene ga full kontroll i to virksomheter blant annet fordi det benyttes svake passord, mange brukerkontoer tildeles store rettigheter, og det er svakheter i beskyttelsen av nettverk. I tillegg ble lite oppdaget fordi overvåkningen var mangelfull. Kontroll av sikkerhetstiltak omtalt nedenfor viser at disse svakhetene er vanlige i virksomhetene i sektoren. Det gir grunn til å tro at inntrengingstester ved andre virksomheter i sektoren kunne gitt lignende resultater. Etter Riksrevisjonens vurdering viser dette at mange av forskningsinstitusjonene ikke er godt nok beskyttet mot dataangrep.

1.4.1.2 Det er stor variasjon i gjennomføringen av tekniske sikkerhetstiltak, og mange av virksomhetene har vesentlige svakheter

Forskningsinstitusjonene skal gjennomføre tekniske sikkerhetstiltak for å oppnå en egnet sikring av sine IKT-systemer og informasjonen som er lagret. Tekniske sikkerhetstiltak skal bidra til å forebygge at dataangrep lykkes. Det er også viktig å ha tiltak for å oppdage de angrep man ikke klarer å forebygge.

For å få et bredere bilde enn det som inntrengingstestene kunne gi, har Riksrevisjonen undersøkt tekniske sikkerhetstiltak ved ti forskningsinstitusjoner. Undersøkelsen viser at sentrale anbefalinger i NSMs Grunnprinsipper for IKT-sikkerhet, som anses som god praksis, ikke følges av mange av de undersøkte virksomhetene. Undersøkelsen viser:

1. **Mangelfull kontroll med brukerkontoer og tilgangsrettigheter:** Flere av virksomhetene har mange brukerkontoer med høye rettigheter og tilgangsrettigheter som ikke reflekterer arbeidsdeling ved drift av systemer. Dette gjør det lettere for en angriper å eskalere rettigheter og få kontroll med all IKT-infrastrukturen når et fotfeste er etablert.
2. **Svake krav til brukerautentisering:** Krav til passord varierer, og det er ofte ikke satt sterkere krav til passord for kontoer som har høye rettigheter. Lave krav gjør det mulig å gjette eller knekke passord. Tofaktor-autentisering er innført mange steder, men det gjelder ikke alle tjenester og påloggingsmuligheter.
3. **Mangelfull sårbarhetsstyring av IT-utstyr og programvare:** De fleste virksomhetene har på plass rutiner for sikkerhetsoppdatering av programvare for å fjerne kjente sårbarheter, men flere virksomheter har ikke god helhetlig sårbarhetsstyring som kan hindre og oppdage sårbarheter. Dette øker risikoen for at en angriper kan finne og utnytte sårbarheter i et dataangrep.
4. **Det er svakheter i nettverkssikkerheten:** Universitetene og høyskolene i undersøkelsen er åpne virksomheter, samtidig som det er svakheter i sikkerhetstiltak for å beskytte egne nettverk.
5. **Mangelfull logging og overvåkning:** Det er mangler i datagrunnlaget for å oppdage og håndtere dataangrep ved at det ofte logges mindre enn anbefalt. Enkelte av virksomhetene har etablert et godt grunnlag for å oppdage dataangrep, men flere har enklere overvåkningsløsninger og mindre kapasitet til å gjennomgå overvåkningsdata.

Nivået på sikkerhetstiltakene i forskningsvirksomhetene varierer imidlertid betydelig, og de har også ulike sikkerhetsmessige utfordringer. Enkelte gjennomfører i stor grad systematiske sikkerhetstiltak og er mer robuste mot dataangrep, men har utfordringer med å sikre at tiltak gjennomføres konsekvent i hele virksomheten. Flere virksomheter har imidlertid kommet kortere, har klare mangler i tekniske sikkerhetstiltak og begrenset evne til å oppdage dataangrep.

Undersøkelsen viser forbedringer i tekniske sikkerhetstiltak de seneste årene, som kan ha sammenheng med økt oppmerksomhet om risikoen i sektoren og i samfunnet generelt. For eksempel er tofaktorautentisering innført for mange tjenester, og ekstern sårbarhetsskanning er etablert av Sikt – Kunnskapssektorens tjenesteleverandør.

For flere av forskningsinstitusjonene er påviste svakheter i tekniske sikkerhetstiltak av en slik karakter at det vil ta tid å nå et tilfredsstillende sikkerhetsnivå. Etter Riksrevisjonens vurdering er det for store svakheter i grunnleggende tekniske sikkerhetstiltak i mange av forskningsvirksomhetene og dermed viktig med et systematisk arbeid for å oppnå en bedre beskyttelse mot dataangrep.

1.4.1.3 Det er svakheter i organisatoriske sikkerhetstiltak som er etablert for å beskytte forskningsdata

For at en virksomhet skal oppnå et egnet sikkerhetsnivå må de tekniske sikkerhetstiltakene omtalt over kombineres med sikkerhetstiltak i organisasjonen og rettet mot den enkelte bruker av IT-systemer. For alle de ti virksomhetene har Riksrevisjonen derfor gjennomgått utvalgte organisatoriske sikkerhetstiltak som er ment å beskytte forskningsdata, og undersøkt om disse er i tråd med god praksis. Undersøkelsen viser flere svakheter i gjennomføringen av disse tiltakene:

– **Virksomhetene har ikke god nok oversikt over forskningsdata.** Dette innebærer at de mangler grunnlag til å vurdere hva som bør beskyttes, og hvordan dette bør gjøres. Virksomhetene har i liten

grad oversikt over andre sensitive forskningsdata enn de som omfatter personopplysninger. De fleste virksomhetene har en relativt god oversikt over personopplysninger i forskning, men oversiktene er ikke komplette.

- **Det gis lite veiledning om sikker behandling av forskningsdata utover personopplysninger.** Ni av ti virksomheter gir føringer om klassifisering av informasjon etter konfidensialitet, og tillatte lagringsløsninger. Disse virksomhetene har også utarbeidet rutiner for behandling av personopplysninger i forskning. Det er gjennomgående lite veiledning rundt klassifisering og lagring av andre sensitive forskningsdata.
- **Opplæring og bevisstgjøring om informasjonssikkerhet og håndtering av forskningsdata er lite systematisk ved de fleste av virksomhetene.** Alle virksomhetene har gjennomført enkeltstående opplæringstiltak og tilbyr noe støtte innenfor informasjonssikkerhet og personvern hvor forskere, veiledere og studenter kan få hjelp ved behov. Likevel tyder undersøkelsen på at forskerne i varierende grad kjenner til regler om informasjonssikkerhet, og at mange opplever klassifisering av data som skal beskyttes, som vanskelig.
- **IT-systemer driftet lokalt i fakulteter, institutter og lignende omfattes ofte ikke av virksomhetenes sentrale retningslinjer og rutiner.** Det er i liten grad stilt krav eller gitt føringer om sikkerhetstiltak til lokale driftsansvarlige for drift av disse systemene. Lokale driftsansvarlige har også i liten grad laget skriftlige retningslinjer eller andre kravdokumenter for løsningene de drifter. Omfanget av lokal drift varierer mellom virksomhetene. Undersøkelsen viser imidlertid at trenden går i retning av sentralisering av IT-drift og/eller skjerping av kravene til lokale IT-miljøer.
- **Sikkerheten hos leverandører av IT-løsninger blir i liten grad fulgt opp av virksomhetene.** Virksomhetene har tjenesteutsatt store deler av databehandlingen i forskning, undervisning, administrasjon og formidling. Mange av virksomhetene oppgir at de gjør vurderinger av informasjonssikkerhet hos leverandørene ved innkjøp av nye IT-løsninger, men det er svært begrenset oppfølging i etterkant av dette.

Undersøkelsen viser at det er gjort forbedringer i gjennomføringen av disse organisatoriske sikkerhetstiltakene de siste årene. Spesielt har virksomhetene, som en oppfølging av den nye personopplysningsloven i 2018, arbeidet med å kartlegge og forbedre rutiner for behandling av personopplysninger. Arbeidet med andre organisatoriske sikkerhetstiltak har imidlertid virksomhetene kommet kortere med. Etter Riksrevisjonens vurdering er det særlig et behov for bedre sikkerhetstiltak for å identifisere og beskytte forretningssensitiv informasjon og informasjon som kan være av interesse for fremmede stater.

1.4.2 Virksomhetene har i stor grad lagt rammene for informasjonssikkerhetsarbeidet, men oppnår ikke ønsket sikkerhetsnivå på grunn av mangler i gjennomføringen

Virksomhetene skal ha et ledelsessystem for informasjonssikkerhet. Ledelsessystemet skal sette planlegging, gjennomføring, kontroll/evaluering og oppfølging av informasjonssikkerhetsarbeidet i system. Systemet skal sikre at passende sikkerhetstiltak gjennomføres og tilfredsstillende sikkerhet oppnås.

Undersøkelsen viser at de fleste virksomhetene har lagt rammene for arbeidet med informasjonssikkerhet ved å etablere de overordnede dokumentene i et ledelsessystem. Alle virksomhetene i undersøkelsen unntatt én hadde dokumentert et ledelsessystem på undersøkelsestidspunktet. Arbeidet med informasjonssikkerhet har fått mer oppmerksomhet de siste årene, og ansvaret for dette arbeidet i virksomhetene er i hovedsak klarlagt.

Selv om arbeidet med informasjonssikkerhet har kommet lenger, er det fortsatt mangler i implementeringen av ledelsessystemene i virksomhetene. De viktigste utfordringene er

- **ledelsessystem.** Implementeringen av ledelsessystemet på et konkret nivå er ofte mangelfull, selv om overordnede policyer er vedtatt. Bare tre av de ti virksomhetene stiller for eksempel tydelige krav i temaspesifikke policyer til tekniske sikkerhetstiltak som Riksrevisjonen har kontrollert i denne undersøkelsen. Der det ikke stilles konkrete krav, blir det i stor grad opp til den enkelte IT-ansatte å vurdere hva som er tilstrekkelig sikkerhet.
- **gjennomføring av besluttede tiltak.** Planer for å iverksette strategier ut fra policyer som ledelsen har vedtatt, er ofte mangelfulle fordi de ikke dekker hele virksomheten, plangrunnlaget er mangelfullt og tidsfrist og ansvar for oppgaver ikke er definert. Samtidig viser undersøkelsen at virksomhetene har utfordringer med å gjennomføre tiltak som er besluttet.
- **risikostyring.** Undersøkelsen viser at det gjøres langt færre risikovurderinger enn hva virksomhetene selv setter krav om, og at det i liten grad gjennomføres systematiske risikovurderinger av IT-infrastruktur. Videre bygger ikke overordnede risikovurderinger klart på informasjon fra mer detaljerte risikovurderinger av de enkelte IT-

systemer mv. Svakhetene i risikostyringen gjør at mange av virksomhetene har et dårlig grunnlag for å vurdere hvilke sikkerhetstiltak som skal implementeres, og for å gjennomføre vedtatte tiltak.

- **evalueringer og etterkontroller av sikkerhetstilstanden.** I de fleste virksomhetene er det begrenset med kontroll og evalueringer av arbeidet med informasjonssikkerhet og personvern samt av hvordan forskningsdata behandles. Noen virksomheter har ikke satt krav om kontroller og evalueringer i ledelsessystemet. Andre har satt krav, men sliter med å gjennomføre vedtatte kontroller og evalueringer. Dermed har mange av virksomhetene lite kunnskap om ledelsessystemet og sikkerhetstiltakene fungerer som forutsatt, og om hva som faktisk er sikkerhetstilstanden i virksomheten.
- **avklaringer om roller og ansvar.** Selv om ansvar på et overordnet nivå er avklart i de fleste virksomheter, er det eksempler på at arbeidet med informasjonssikkerhet har blitt hemmet av at det mangler en overordnet/samlende rolle. I flere virksomheter er det noe uklarhet både om hvilke tekniske sikkerhetstiltak som skal implementeres, og hvem som har ansvaret for å følge opp at tiltakene blir iverksatt i IT-driften. I flere virksomheter er det ikke klart hvem som har ansvaret for organisatoriske sikkerhetstiltak som opplæring og bevisstgjøring.
- **kompetanse og ressurser.** Det er store forskjeller mellom virksomhetene med hensyn til tilgang til ressurser og kompetanse om informasjonssikkerhet. Det varierer mellom virksomhetene hvor mye ressurser de kan sette av til informasjonssikkerhet, og i hvilken grad de har mulighet til å tiltrekke seg spesialistkompetanse. Kompetanse og ressurser er nødvendig for å identifisere og iverksette nødvendige sikkerhetstiltak.
- **ledelsens informasjonsgrunnlag.** I syv av ti virksomheter har toppledelsen gjennomgått status for ledelsessystemet og sikkerhetstilstanden ett eller flere av årene i undersøkelsesperioden. Innholdet i gjennomgangene varierer imidlertid betydelig, og få av virksomhetene bruker resultatet fra risikoarbeidet eller statusen for gjennomføring av tiltaksplaner i særlig grad. Dermed har ledelsen ofte ikke et fullstendig bilde av hvordan sikkerhetstilstanden er, og et svakt grunnlag for å kunne vurdere tiltak.
- **styrets rolle.** I flere virksomheter mottar styret lite av informasjonen de trenger for å ivareta sin rolle som det organet med det øverste ansvaret for informasjonssikkerheten. I noen virksomheter er det heller ikke definert hva som er styrets rolle og ansvar i ledelsessystemet, eller det er uklart hvilken informasjon styret skal motta.

Det er stor variasjon i virksomhetenes arbeid med informasjonssikkerhet. Dette er til dels naturlig da de har svært ulik størrelse, ulikt omfang av forskningsdata og ulik kompleksitet i IT-infrastruktur. Hvordan utfordringene i punktlisten ovenfor skal tas tak i, må være tilpasset virksomhetene.

Selv om informasjonssikkerhet har fått mer oppmerksomhet de senere årene og ledelsessystem er utarbeidet i virksomhetene, gjenstår det betydelig arbeid for å implementere systemene fullt ut slik at de oppnår ønsket sikkerhetsnivå. Styret har det øverste ansvaret for å håndtere risikoen for informasjonssikkerheten og for at virksomheten har systemer som hindrer at sensitive forskningsdata i virksomheten kommer på avveier. Etter Riksrevisjonens vurdering mottar de fleste styrene for lite informasjon om informasjonssikkerhetsrisikoen til å kunne ta stilling til sikkerhetsnivået. Trusselsituasjonen i sektoren er betydelig skjerpet de siste årene, og etter Riksrevisjonens vurdering er det viktig at styrene tar sitt ansvar for å påse at virksomhetene har god nok informasjonssikkerhet.

1.4.3 Kunnskapsdepartementet har justert virkemiddelbruken de siste årene, men det er en del utfordringer i sektoren som dagens virkemidler ikke treffer

Departementet har ansvar for å avklare sentrale roller og ansvarsområder på informasjonssikkerhetsområdet og sørge for at den overordnede organiseringen og virkemiddelbruken på området er ressurseffektiv. Departementet har videre ansvar for å følge opp at underliggende virksomheter jobber for å nå mål og oppfylle krav på informasjonssikkerhetsområdet. Det innebærer blant annet å gi føringer på området og sørge for at virksomhetene gir dem et tilstrekkelig informasjonsgrunnlag for styringen. Departementet bør også vurdere hensiktsmessige virkemidler overfor de aktørene i sektoren der departementet mangler direkte styringslinjer.

I 2019 satte Kunnskapsdepartementet i gang et fireårig informasjonssikkerhetsprogram i universitets- og høyskolesektoren. Målet med programmet var å styrke informasjonssikkerheten i sektoren. Programmet skulle forbedre sektorens evne til å forebygge, oppdage og håndtere trusler mot forskningsnettet, og det skulle inkludere tiltak som analyseverktøy og kompetanseheving.

Sentrale resultater av satsingen er at det ble etablert

- en styringsmodell for informasjonssikkerhet, hvor ansvaret ble gitt til HK-dir – Direktoratet for høyere utdanning og kompetanse
- et Cybersikkerhetssenter for høyere utdanning og forskning, eduCSC, hvor ansvaret er gitt til Sikt – Kunnskapssektorens tjenesteleverandør

1.4.3.1 Styringsmodellen for informasjonssikkerhet har gjort at den enkelte forskningsvirksomhet har fått tettere oppfølging

Gjennom styringsmodellen er HK-dir – Direktoratet for høyere utdanning og kompetanse gitt ansvaret for den løpende sektorstyringen av informasjonssikkerhet og personvern i til sammen 29 virksomheter direkte underlagt departementet. Kunnskapsdepartementet har fastsatt en overordnet Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning, som sammenfatter krav og føringer på området. HK-dir gjennomfører årlige kartleggingsmøter med virksomhetene hvor de tar utgangspunkt i krav og føringer i policyen, og leverer forslag til konkrete tilbakemeldinger som departementet kan bruke i sin oppfølging av virksomhetene.

HK-dir gir også konkrete anbefalinger til virksomhetene om det videre arbeidet med informasjonssikkerhet og personvern. En del av virksomhetene som er undersøkt, oppgir at de har hatt nytte av HK-dirs kartlegging, og at det har bidratt til å rette virksomhetenes oppmerksomhet mot informasjonssikkerhet og sette retning for arbeidet. Dette er særlig tilfellet for de minste virksomhetene.

Undersøkelsen viser at departementet har fulgt opp virksomhetene som er omfattet av styringsmodellen gjennom etats- og eierstyringen. Departementet har også brukt pedagogiske virkemidler overfor enkelte virksomheter i sektoren der styringsmulighetene er mer begrensede. De har gitt anbefalinger til private høyskoler som ikke er omfattet av styringsmodellen, gjennom tilskuddsbrev.

Etter Riksrevisjonens vurdering er det positivt at Kunnskapsdepartementet er tydelig om hvilke krav og føringer som gjelder for underliggende virksomheter, og følger opp dette gjennom styringsmodellen. Dette har bidratt til større oppmerksomhet om informasjonssikkerhetsarbeidet i virksomhetene som er omfattet av styringsmodellen. Samtidig har personvernforordningen blitt innført og trusselbildet skjerpet etter konkrete hendelser i sektoren. Det er også positivt at departementet bruker pedagogiske virkemidler overfor enkelte virksomheter i sektoren der departementet ikke har en direkte styringslinje.

Departementet har ikke uttrykt forventninger om hvordan universiteter og høyskoler skal følge opp informasjonssikkerheten i selskapene de eier. Departementet framholder at de på generelt grunnlag forventer at universiteter og høyskoler utøver sitt eierskap på en god måte og etterlever gjeldende lover og krav. Undersøkelsen viser at de tre største universitetene ikke har gitt føringer eller forventninger til informasjonssikkerheten gjennom eierdialogen til selskaper som driver med forskning eller teknologioverføring. Riksrevisjonen vil understreke at de samme forventningene til informasjonssikkerhet må legges til grunn, uavhengig av hvordan universitetene og høyskolene har valgt å organisere forskningsvirksomheten.

1.4.3.2 Kunnskapsdepartementet har i begrenset grad lyktes med å nå målet med informasjonssikkerhetssatsingen, og virkemidlene treffer i for liten grad virksomhetene som har størst behov for støtte

Som ledd i fireårssatsingen fikk Sikt (den gang Uninett) ansvar for å etablere et analysesenter og ta rollen som sektorvist responsmiljø for å forbedre sektorens evne til å håndtere trusler. Videre fikk de ansvaret for å få på plass rådgivningstjenester som skulle bistå sektoren i å implementere ledelsessystemer for informasjonssikkerhet på en helhetlig måte, og for å etablere et program for kompetanseheving innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og øvrige ansatte i sektoren. Leveransene fra Sikt ble samlet i et eget Cybersikkerhetssenter for høyere utdanning og forskning, eduCSC. Senteret tilbyr også tjenester til virksomheter i sektoren som ikke er underlagt Kunnskapsdepartementet.

For å dekke ulike behov i virksomhetene har eduCSC fra 2023 etablert ulike abonnementer, eller «pakker» av tjenester, som kunder av senteret kan velge blant. Enkelte tjenester leveres som tilleggstjenester. Både prismodell og tjenesteinnholdet er forankret i Digitaliseringsstyret, som er øverste nivå i universitets- og høyskolesektorens samstyringsmodell for digitalisering. Digitaliseringsstyret har bestemt at abonnementet «basispakken» skal være obligatorisk for alle høyskoler og universiteter. Det har foreløpig vært utfordrende for eduCSC å få senteret finansiert via brukerbetaling. Sikt anslår at senteret vil gå cirka ti millioner kroner i underskudd det første året med ny prismodell.

Undersøkelsen viser at leveransen eduCSC har kommet lengst med, er rollen som sektorvist responsmiljø. På dette området har departementet sørget for et rammeverk for håndtering av IT-sikkerhetshendelser i sektoren.

Når det gjelder evnen til å oppdage dataangrep, vurderer Sikt at denne har vært uendret i perioden. Dette skyldes at felles infrastruktur og logganalyse som eduCSC har kjøpt inn som del av satsingen, ikke tas i bruk, og at overvåking av nettverk ved hjelp av sensorer er lagt til abonnementet «plusspakken», mens flertallet av virksomhetene har valgt «basispakken».

Leveransene fra eduCSC med dårligst måloppnåelse er tiltakene innenfor rådgivningstjenester og kompetanseheving. Rådgivningstjenester er blant senterets tilleggstjenester, og så langt har få virksomheter valgt å be-

nytte seg av dette tilbudet. De mest konkrete leveransene innenfor kompetanseheving er

- de to forumene for informasjonssikkerhet, CISO-forum og IRT Community
- utarbeidelse av en veileder
- revisjoner av enkelte andre veiledere
- gjennomføring av enkelte webinarer

Både HK-dir og Sikt vurderer at omfanget av rådgivning og kompetanseheving som tilbys er mindre enn tiden før fireårssatsingen.

Samtidig viser undersøkelsen at mange virksomheter ikke klarer å gjennomføre anbefalte sikkerhetstiltak. Flere virksomheter har blant annet svak evne til å oppdage dataangrep. Departementets virkemiddelbruk ved opprettelse av eduCSC ser foreløpig ikke ut til å ha avhjulpet dette problemet.

Spesielt evnen til å oppdage dataangrep avhenger av sterkt spesialisert kompetanse. eduCSC overvåker i dag kommunikasjonen inn og ut av virksomhetene, men senteret overvåker ikke virksomhetenes egne nettverk og systemer.

Flere virksomheter sliter også med andre tekniske sikkerhetstiltak, som tilgangsstyring og intern sårbarhetsskanning. Det varierer mellom virksomhetene om de bygger intern kompetanse på dette, og noen virksomheter er avhengig av støtte for å gjennomføre sikkerhetstiltak. Innhentede data viser at mange virksomheter leier inn konsulenter til å sette opp systemer og lignende, også med tanke på sikkerhet.

De fire største universitetene har gått sammen om et eget sikkerhetssamarbeid, BOTT Digital Sikkerhet, og ønsker at færrest mulig av tjenestene til eduCSC burde være obligatoriske. De fire har en del felles utfordringer, og etter Riksrevisjonens vurdering en del å lære av hverandre. At de fire største universitetene samarbeider, løser imidlertid ikke problemene som sektoren som helhet har på informasjonssikkerhetsområdet.

Riksrevisjonen vurderer det som positivt at departementet har etablert et cybersikkerhetssenter med tjenester til hele sektoren, også til virksomheter i sektoren der departementet mangler direkte styringslinjer. Per dags dato greier imidlertid ikke eduCSC å treffe behovene til virksomhetene. Departementet har i stor grad overlatt vurderingene av hva eduCSC skal tilby til de underliggende virksomhetene, gjennom universitets- og høyskolesektorens samstyringsmodell for digitalisering. Etter Riksrevisjonens vurdering styres imidlertid senterets tjenestetilbud i dag i for stor grad av den enkelte virksomhets etterspørsel og betalingsvilje, og i for liten grad av behovene til sektoren som helhet.

Kunnskapsdepartementet har definert rollene til de sentrale aktørene i sektoren innenfor informasjonssikkerhetsområdet. Undersøkelsen viser imidlertid at det i praksis er uklarheter i forholdet mellom Kunnskapsdepartementet, HK-dir og Sikt når det gjelder styring og gjennomføring av informasjonssikkerhetstiltak i sektoren.

Departementet har videre gitt NOKUT ansvar for å føre uavhengig kontroll med informasjonssikkerheten i sektoren. Undersøkelsen viser at NOKUT verken gjennomfører eller har kapasitet til å gjennomføre dette. Det er heller ikke avklart hvordan slike kontroller skal gjennomføres.

Samlet sett vurderer Riksrevisjonen derfor at organiseringen og virkemiddelbruken på området for sektoren som helhet er mindre ressurseffektiv og målrettet enn den kunne ha vært.

1.4.4 Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og risikoreduserende tiltak som er besluttet på sektornivå, blir ikke fulgt opp

Departementet skal utarbeide og vedlikeholde systematiske risiko- og sårbarhetsanalyser, ta stilling til sikkerhetsnivået i egen sektor samt iverksette nødvendige kompenserende tiltak. Departementet skal også sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater. Hvor ofte og i hvilken utstrekning et område som informasjonssikkerhet bør evalueres, må bestemmes ut fra blant annet risiko og vesentlighet, samt kvaliteten på og omfanget av øvrig rapportering. Mer generelt har departementet overordnet ansvar for blant annet at virksomhetene bruker ressurser effektivt, og at det gjennomføres kontroll med virksomhetene.

Som del av styringsmodellen for informasjonssikkerhet har HK-dir fra og med 2019 levert årlige risiko- og tilstandsvurderinger til departementet. Gjennom disse mottar departementet informasjon om trusler og sårbarheter. Her sammenfatter HK-dir informasjon fra kartleggingene i virksomhetene, vurderer virksomhetenes modenhetsnivå innenfor informasjonssikkerhet og personvern og sannsynligheten for at virksomhetene etterlever kravene som er formulert i Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. HK-dir trekker også inn informasjon fra andre kilder, slik som statistikk om IT-sikkerhetshendelser i forskningsnettet fra sektorvist responsmiljø (eduCSC) og risiko- og trusselvurderinger fra nasjonale myndigheter. På bakgrunn av dette utarbeider HK-dir også årlige risikohåndteringsplaner på sektornivå med forslag til tiltak for å håndtere risikoen. Kunnskapsdepartementet tar stilling til og slutter seg til planene.

Men HK-dir baserer risiko- og tilstandsvurderinger på virksomhetenes egenrapportering og gjør ingen

form for sikkerhetstesting eller kontroller av den faktiske sikkerhetstilstanden. Verken HK-dir eller andre gjennomfører tester for å kartlegge den faktiske statusen eller om tiltakene institusjonene oppgir, er implementert og fungerer i praksis. Informasjonen departementet mottar fra HK-dir, dreier seg i hovedsak om virksomhetenes arbeid med organisatoriske sikkerhetstiltak, men sier lite om virksomhetenes tekniske sikkerhetstiltak og om tiltakene har effekt. Funnene fra de tekniske testene og inntrengingstestene i undersøkelsen viser at det er svakheter i de tekniske sikkerhetstiltakene hos alle virksomhetene.

Flere av virksomhetene i undersøkelsen har kjøpt inntrengingstester fra private konsulentselskaper/revisjonsfirmaer, men departementet får ikke informasjon om resultatene fra disse testene. Det er også en mulighet at eduCSC gjennomfører for eksempel inntrengingstester, men dette har senteret ikke kapasitet til per i dag.

Som nevnt har departementet gitt NOKUT ansvar for å føre uavhengig kontroll med informasjonssikkerheten i sektoren, men NOKUT gjennomfører ikke noen slike kontroller per i dag. NOKUT har heller ikke et kompetansemiljø innenfor informasjonssikkerhetstesting.

Samtidig viser undersøkelsen at risikoreduserende tiltak på sektornivå som er identifisert, og som departementet er orientert om, ikke blir gjennomført. Dette gjelder tiltak som inntrengingstesting og revisjoner av den enkelte virksomhets arbeid med informasjonssikkerhet og personvern og med kompetanseheving overfor virksomhetene. Ansvaret for å følge opp flertallet av tiltakene er gitt til Sikt ved Cybersikkerhetssenter for forskning og utdanning (eduCSC). En del av tiltakene har ikke blitt gjennomført, og har heller ikke vært realistiske å gjennomføre, da de i praksis har forutsatt både at Sikt/eduCSC etablerer nye tjenester og at virksomhetene i sektoren betaler for gjennomføringen.

Undersøkelsen viser at virksomhetene mangler oversikt over egne informasjonsverdier i forskning som ikke er personopplysninger. Departementet har igangsatt et kartleggingsarbeid med utgangspunkt i sikkerhetsloven for å få bedre oversikt over informasjonsverdier i sektoren det er særlig viktig å beskytte. Dette arbeidet er ikke ferdigstilt.

Riksrevisjonen vurderer det som positivt at Kunnskapsdepartementet har etablert en prosess for risikostyring av sektoren som gir informasjon om arbeidet med informasjonssikkerhet i virksomhetene som er omfattet av styringsmodellen. Samtidig mottar departementet lite systematisk informasjon om de tekniske sikkerhetstiltakene som er iverksatt ute i virksomhetene, og om virkningen av tekniske og organisatoriske sikkerhetstiltak. Kunnskap om den faktiske sikkerhetstilstanden og verdiene i sektoren er viktig for at departementet skal kunne målrette krav og tiltak slik at sektoren er bedre i stand til å forbedre sikkerheten.

1.5 Anbefalinger

Riksrevisjonen anbefaler at Kunnskapsdepartementet

- avklarer samarbeidet mellom departementet, HK-dir og Sikt om informasjonssikkerhet, og avklarer hva NOKUTs rolle skal være
- gjennomgår virkemiddelbruken og vurderer tiltak som i større grad treffer forskningsvirksomhetene som har størst behov for støtte
- sikrer et godt informasjonsgrunnlag om sikkerhetstilstanden og verdiene i sektoren, og følger opp at risikoreduserende tiltak på sektornivå blir gjennomfør.
- påser at forskningsvirksomhetene
  - sørger for at ledelsessystem for informasjonssikkerhet blir implementert fullt ut slik at styret og toppledelse har oversikt over sikkerhetstilstanden, kan sikre at besluttede tiltak gjennomføres og at tiltakene faktisk forbedrer sikkerheten slik som forutsatt
  - sørger for bedre oversikt over forskningsdata som skal beskyttes
  - iverksetter tekniske og organisatoriske sikkerhetstiltak som de anser nødvendige, for å redusere risikoen for at dataangrep lykkes

1.6 Statsrådens svar

Dokument 3:11 (2023–2024) Informasjonssikkerhet i forskning innenfor kunnskapssektoren ble oversendt statsråden i Kunnskapsdepartementet.

Svaret fra statsråden følger i sin helhet som vedlegg til Riksrevisjonens dokument.

2. Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Kari Henriksen, Frode Jacobsen og Kirsti Leirtrø, fra Høyre, lederen Peter Frølich og Svein Harberg, fra Senterpartiet, Nils T. Bjørke, fra Fremskrittspartiet, Carl I. Hagen, fra Sosialistisk Venstreparti, Audun Lysbakken, fra Rødt, Seher Aydar, fra Venstre, Grunde Almeland, og fra Miljøpartiet De Grønne, Lan Marie Nguyen Berg, viser til Dokument 3:11 (2023–2024) Informasjonssikkerhet i forskning innenfor kunnskapssektoren.

Komiteen viser til Riksrevisjonens konklusjoner:

«Forskningsdata i forskningsinstitusjonene under Kunnskapsdepartementet er ikke i tilstrekkelig grad sikret mot dataangrep.[...]

Virksomhetene har i stor grad lagt rammene for informasjonssikkerhetsarbeidet, men oppnår ikke ønsket sikkerhetsnivå på grunn av mangler i gjennomføringen

Kunnskapsdepartementet har justert virkemiddelbruken de siste årene, men det er en del utfordringer i sektoren som dagens virkemidler ikke treffer.[...]

Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren og risikoreduserende tiltak som er besluttet på sektornivå, blir ikke fulgt opp»

Komiteen slutter seg til Riksrevisjonens konklusjoner.

Komiteen viser til Riksrevisjonens overordnede vurdering:

«Det er kritikkverdig at forskningsdata i virksomheter under Kunnskapsdepartementet ikke er i tilstrekkelig sikret mot dataangrep, gitt kravene i lovverket og de mulige konsekvensene av at sensitive data kommer på avveier.

Virksomhetene har ikke god nok oversikt over forskningsdata som trenger beskyttelse. Dette er ikke tilfredsstillende.

Tross forbedringer i undersøkelsesperioden, arbeider mange virksomheter i for liten grad systematisk med informasjonssikkerhet, og styrene i virksomhetene fyller ikke i stor nok grad rollen de skal ha. Dette er ikke tilfredsstillende

Kunnskapsdepartementet har gjennomført flere tiltak i perioden 2019–2022 som blant annet har ført til økt oppmerksomhet om informasjonssikkerhet i virksomhetene. Samtidig er det ikke tilfredsstillende at virkemidlene i for liten grad treffer virksomhetene som har størst behov for støtte.

Det er ikke tilfredsstillende at departementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og at risikoreduserende tiltak ikke blir fulgt opp.»

Komiteen slutter seg til Riksrevisjonens kritikk.

Komiteen viser videre til Riksrevisjonens anbefalinger:

«Riksrevisjonen anbefaler at Kunnskapsdepartementet

- avklarer samarbeidet mellom departementet, HK-dir og Sikt om informasjonssikkerhet, og avklarer hva NOKUTs rolle skal være.
- gjennomgår virkemiddelbruken og vurderer tiltak som i større grad treffer forskningsvirksomhetene som har størst behov for støtte.
- sikrer et godt informasjonsgrunnlag om sikkerhetstilstanden og verdiene i sektoren, og følger opp at risikoreduserende tiltak på sektornivå blir gjennomført.
- påser at forskningsvirksomhetene
  - sørger for at ledelsessystem for informasjonssikkerhet blir implementert fullt ut slik at styret og toppledelse har oversikt over sikkerhetstilstanden, kan sikre at besluttede tiltak gjennomføres og at tiltakene faktisk forbedrer sikkerheten slik som forutsatt.
  - sørger for bedre oversikt over forskningsdata som skal beskyttes
  - iverksetter tekniske og organisatoriske sikkerhetstiltak som de anser nødvendige, for å redusere risikoen for at dataangrep lykkes.»

Komiteen slutter seg til Riksrevisjonens anbefalinger.

Komiteen registrerer videre at statsråden mener Riksrevisjonens rapport vil være nyttig for departementets og sektorens videre arbeid på dette feltet.

3. Komiteens tilråding

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

vedtak:

Dokument 3:11 (2023–2024) – Informasjonssikkerhet i forskning innenfor kunnskapssektoren – vedlegges protokollen.

Oslo, i kontroll- og konstitusjonskomiteen, den 14. mai 2024

Peter Frølich
leder

Kirsti Leirtrø
ordfører

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets administrasjon