



Hendelses- og årsaksgjennomgang avvik informasjons-sikkerhet

Av Monica Lunde, Espen Bjorli, Katrine T. Nordby, Stian Sandbakken, Thorbjørn A. Unneberg





Statsforvalteren i Innlandet
Rapport nr. 2 | 2026

Forfatter(e): Monica Lunde, Espen Bjorli, Katrine T. Nordby, Stian Sandbakken, Thorbjørn A. Unneberg.

Godkjent av Asbjørn Lund

Tittel: Hendelses- og årsaksgjennomgang avvik informasjonssikkerhet.

ISBN: 978-82-8410-081-4

Forsidebildet:
Foto:

© 2026 Forfatterne



Rapporten er lisensiert under «Creative Commons Navngivelse – Ikke Kommersiell – Del På Samme Vilkår 3.0 Norge»-lisensen som er gjengitt her: <http://creativecommons.org/licenses/by-nc-sa/3.0/no/>

Innhold

Hovedfunn og konklusjon	4
Kortfattet presentasjon av de viktigste funnene.....	5
Mandat og hensikt	6
Metode.....	7
Rettslig grunnlag.....	7
Hovedinstruksen (HI) og STAF	8
Hendelsesforløp.....	9
Håndtering av hendelsen i november 2025	9
Vurdering av tiltak iverksatt for å håndtere hendelsen	11
Intern håndtering av avviket.....	11
Oppfølging av berørte parter	12
Læringspunkter fra hendeshåndteringen	12
Årsaksanalyse.....	13
Funn (datagrunnlag).....	13
Styringssystem, ledelse og ansvar	13
Rolle- og ansvarsfordeling	13
Kompetanse, opplæring og bevissthet.....	14
Styrte prosesser, rutiner og etterlevelse	14
Implementering av endringer.....	14
Innsynsrutiner og styringsbibliotek	15
Kultur, samhandling og organisasjonspraksis.....	15
Samhandling med STAF	15
Tiltak etter hendelsen	15
Vurderinger	16
Styringssystem, ledelse, roller og ansvar	16
Kompetanse, opplæring og bevissthet.....	16
Styrte prosesser, rutiner og etterlevelse	16
Kvalitets- og styringssystem	17
Kultur, samhandling og forbedring	17
Referanser	18

Hovedfunn og konklusjon

Statsforvalteren i Innlandet ble i november 2025 gjort kjent med brudd på personopplysnings-sikkerhet knyttet til bruk av programmet Foxit ved behandling av innsynsbegjæringer. Metadata og bokmerker i PDF-dokumenter var ikke fjernet, noe som gjorde at navn og personnummer kunne leses i sladdede dokumenter ved delvis innsyn.

Hendelsegjennomgangen belyser problemer som kan oppstå når svakhetene i et system sammenfaller. Det er avdekket utfordringer og svakheter på flere nivåer fra anskaffelser og implementering av ikt-systemer til innføring av felles rutiner.

Undersøkelsen viser at rutiner er fulgt av mange, og det er et relativt lite antall som har medført feil. Virksomheten har imidlertid ikke etablert et godt nok system for håndtering av innsyn og sladding. Rutiner finnes på flere plattformer, og enkelte enheter benytter egne rutiner som ikke ligger i styringsbiblioteket. Dette skaper uklarhet om gjeldende praksis og øker risikoen for ulik håndtering av innsynssaker.

Opplæring og kompetansestyring framstår i hovedsak uformell, og det er ikke systematisk verifisering av opplæring i teknisk korrekt sladding. Rolle- og ansvarsfordelingen i grensesnittet mellom faglinjen og STAF er ikke avklart i tilstrekkelig grad.

Selv om hendelsen ble håndtert raskt når den ble avdekket, har ikke virksomheten en internkontroll som i tilstrekkelig grad sikrer implementering av rutinen, systematisk opplæring og læring av avvik på tvers av avdelinger.

Reaksjoner fra berørte parter og publikum har vært svært få. Det indikerer at vi har greid å nå ut med korrekt informasjon om hendelsen og gjort gode tiltak for å begrense omfanget av avviket.

Hendelsen skyldtes ikke teknisk feil i Foxit, men en svakhet at det må gjøres en manuell fjerning av skjulte data.

Sammendrag av funn i rapporten:

- Kompetanse og opplæring: Det er god juridisk kompetanse på innsyn, men opplæring i sladding har vært uformell, samt at rutiner varierer mellom enheter og er dårlig samordnet i styringsbiblioteket.
- Det er gjennomført strakstiltak og langsiktige tiltak, inkludert stikkprøver, obligatorisk opplæring, informasjonstiltak overfor berørte og forbedrede rutiner for innsynshåndtering, herunder ledergodkjenning av delvis innsyn.
- Hendelsen avdekket behov for å styrke opplæring i innsynssaker, vedlikehold og dokumentasjon av gjennomført opplæring.
- Det er behov for en avklaring av roller og ansvar mellom SFIN og STAF.
 - Samhandling med STAF. Gjennomgående implementering av nye IKT-systemer fra STAF til embetene og sluttbruker
 - Avklare hvor slutter STAFs ansvar og hvor begynner SFINs?

Kortfattet presentasjon av de viktigste funnene

Den 20. november 2025 ble Statsforvalteren gjort kjent med avvik knyttet til brudd på personopplysningssikkerhet ved bruk av programvaren Foxit i behandlingen av innsynskrav. Avvikene har ført til at det har vært mulig å få tilgang til navn og personnummer i sladdede dokumenter som er sendt ut ved delvis innvilget innsyn. Det er gjennomført en systematisk kartlegging av omfanget av avviket, ved gjennomgang av Elements for perioden 1. april 2022 til 2. desember 2025. Embetet gjennomførte obligatorisk opplæring i håndtering av innsynsbegjæring rett i etterkant av hendelsen, for å minimere videre risikoer.

Område	Hovedfunn
Varsling eksternt	Det ble raskt besluttet at hendelsen krevde eksternt varslings. Ledermøte samme dag besluttet varslings til DFD, fagdepartement, Datatilsynet og øvrige embeter. Varsling ble gjennomført tidlig og i tråd med alvorlighetsgrad.
Informasjonsdeling	Opprettelsen av en Teams-gruppe for de som håndterte hendelsen bidro til god informasjonsdeling og felles oversikt. Det har vært godt kontakt opp mot media med åpenhet rundt fakta om hendelsen og håndtering av den.
Organisering (beredskap/kriserigg)	Kriseledelsen ble etablert raskt og fungerte godt. Stabsarbeidet var strukturert, men den interne kommunikasjonen kan bedres.
Opplæring	Opplæringen i sladding og bruk av verktøy (Foxit) har i hovedsak vært uformell. Det har manglet strukturert opplæring, særlig om hva metadata er, og opplæring i teknisk håndtering av sladding av metadata. Hendelsen har ført til større årvåkenhet. Sammen med strakstiltakene er situasjonen forbedret, men det er behov for å etablere et system for opplæring og vedlikehold av kunnskap.
Kvalitetsstyring / personvern / informasjonssikkerhet	Styringsbiblioteket hvor rutinene ligger er ikke godt nok kjent blant alle ansatte. Rutiner er spredt, ofte ikke versjonsstyrt, og enkelte brukes kun lokalt.
STAF – Statsforvalteren (roller, kommunikasjon og ansvar)	Rolle- og ansvarsfordelingen mellom SFIN og STAF er ikke tilstrekkelig klar. Det er ulik forståelse av ansvar og roller ved systeminnføring, risiko- og sårbarhet knyttet til systemene og opplæring. Kommunikasjon og implementering ved innføring av nye IKT-systemer har ikke vært systematisk og kvalitetssjekket, noe som har bidratt til å skape sårbarhet. Statsforvalteren er <i>behandlingsansvarlig</i> og STAF er <i>databehandler</i> etter

	personopplysningsloven. Databehandleravtalen mellom STAF og embetene bør gjennomgås. Disse rollene bør klargjøres.
--	--

Anbefalinger/forslag til tiltak:

Rapporten viser at flere av utfordringene skyldes manglende koordinering, uklare roller og utilstrekkelig dokumentasjon. Det anbefales å:

1. Etablere tydelig styring ved innføring av IKT-systemer

Klare prosesser for beslutning og godkjenning må på plass før nye systemer tas i bruk.

2. Sikre et dokumentert og systematisk opplæringsopplegg for innsynsbehandling og øvrige nye IKT-systemer

Alle som håndterer innsynsbegjæringer skal få nødvendig og oppdatert opplæring. Ved innføring av alle nye IKT-systemer må nødvendig opplæring gis.

3. Innføre faste og målbare kvalitetskontroller

Regelmessige kontroller skal bidra til lik praksis og forbedring over tid.

4. Tydeliggjøre roller og ansvar mellom SFIN og STAF

En klarere arbeidsdeling skal styrke samarbeidet og redusere uklarheter, herunder gjennomgå og klargjøre rollene som behandlingsansvarlig (SFIN) og databehandler (STAF)

5. Forbedre kvalitetssystemet

Som del av et forbedret kvalitetssystem så anbefales det å etablere systematiske kontroller, stikkprøver eller loggføring, samt verdi- og risikovurdering av den enkelte rutine.

6. Intern hendelseshåndtering

- Styrke kunnskapen om beredskapsplanverk og krisehåndteringsriggen. Kompetanseheving og øvelser.
- Styrket systemkompetanse i SFIN og etablerte superbrukerfunksjoner.
- Bedre erfaringsdeling både underveis og i etterkant.

Mandat og hensikt

Det ble satt ned en tverrfaglig gruppe som skulle analysere årsaker som førte til uønsket hendelse oppdaget torsdag 20.11.25. Det ble da avdekket at metadata (bokmerker) med personidentifiserbar informasjon i noen tilfeller har fulgt med ved utsendelse av sladdede dokumenter der det er gitt delvis innsyn.

Gruppen skulle identifisere årsaken til hendelsen og foreslå tiltak som kan forhindre at lignende hendelser skjer igjen og sikre læring for embetet. (Mandatet – vedlegg 1)

Analysegruppen

Navn	Enhet
Monica Lunde (Leder)	Samfunnssikkerhet og beredskap
Espen Bjorli	Barnevern og familie
Stian Sandbakken	Helse og omsorg
Katrine Tømmerdal Nordby	Juridisk
Thorbjørn A. Unneberg	Virksomhetsstyring og kommunikasjon
Ove Sund	STAF har etter avtale deltatt på to møter i den innledende fasen av hendelsesgjennomgangen, i januar 2026.

*¹Personvernombudet STAF

Metode

Vi har foretatt intervjuer og gjennomgått aktuelle dokumenter for å avdekke årsaker på systemnivå, individnivå og organisasjonsnivå, herunder rutiner, kompetanse, teknisk støtte og internkontroll. Intervjuene har hatt tre fokusområder, der vi har ønsket å få opplysninger om forhold før-, under- og etter hendelsen/avviket.

Det er gjennomført totalt 15 intervjuer med saksbehandlere, avdelingsdirektører og virksomhetsdirektører fra enheter som har vært berørt av hendelsen, samt direktører for virksomhetsområdene. Intervjuobjektene er fordelt slik: 3 VO-direktører, 5 avdelingsdirektører og 7 saksbehandlere i perioden 19.-28.januar. (Intervjuguidene – vedlegg 2).

Rettslig grunnlag

Statsforvalteren mottar og innhenter store mengder data i utførelsen av sitt oppdrag. Personopplysninger som Statsforvalteren mottar, skal behandles i tråd med personvernlovgivningen. Personopplysningsloven inneholder regler for behandling av slike opplysninger. EUs personvernforordning (GDPR) er gjort til norsk lov gjennom personopplysningsloven. Sammen utgjør de det norske personvernregelverket som har som formål å ivareta vår rett til vern av personopplysninger. Statsforvalteren er ansvarlig for at vi håndterer personopplysninger i tråd med dette regelverket.

Alle kan kreve innsyn i dokumenter i offentlig forvaltning. Når vi mottar innsynskrav i dokumenter, skal de håndteres i tråd med offentleglova. Innsyn i dokumenter i offentlig forvaltning er nedfelt i Grunnlovens kapittel om menneskerettigheter. I § 100 om ytringsfrihet står det

«Enhver har rett til innsyn i statens og kommunenes dokumenter og til å følge forhandlingene i rettsmøter og folkevalgte organer. Det kan i lov fastsettes begrensninger i denne rett ut fra hensyn til personvern og av andre tungtveiende grunner.» ([Grunnloven § 100 femte ledd.](#))

¹ Analysegruppen har også konsultert personvernombudet og annet fagpersonell, som f.eks. personvernombudet til STAF

Denne retten til innsyn, offentlighetsprinsippet, er viktig for rettssikkerheten for den enkelte og tilliten til det offentlige. Det offentlige skal ivareta både hensyn til offentlighet og hensynet til personvern i sin behandling av innsynskrav. Personopplysninger som er underlagt taushetsplikt i forvaltningsloven eller særlovgivningen skal det ikke gis innsyn i jf. offl. § 13. Dersom forvaltningen gir ut slike opplysninger, er det et brudd på offentleglova og personvernlovgivningen.

Personopplysningsloven og offentleglova gir uttrykk for to motstridende prinsipper. Personopplysningsloven gir regler for behandling av personopplysninger og stiller krav til hvordan opplysninger brukes i både privat og offentlig virksomhet, mens offentleglova gir regler om hvilke opplysninger det kan gis innsyn i det offentlige.

Forholdet mellom offentleglova og personopplysningsloven er beskrevet i personvernforordningen artikkel 86. Der står det at personopplysninger kan utleveres etter nasjonale regler om allmennoffentlighet når utleveringen er «i samsvar med» de nasjonale reglene. Denne bestemmelsen skal altså sikre at nasjonale regler om offentlighet i forvaltningen er i samsvar med retten til vern av personopplysninger. Riktig håndtering av innsynskrav er dermed en forutsetning for at retten til personvern blir ivaretatt (Personopplysningsloven, artikkel 86)).

Hovedinstruksen (HI) og STAF

HI fastsetter statsforvalterens myndighet og ansvar, ansvarsfordeling og samarbeid med STAF og krav til embetenes interne styring.

I HI pkt. 4.3 står det om hvilke krav som stilles til Statsforvalterens internkontroll: «Statsforvaltaren har eit sjølvstendig ansvar for å innrette system og rutinar for internkontroll og sjå til at nødvendige kontrolloppgåver blir utførte. Vurderingar av viktigeit og risiko skal liggje til grunn. Statsforvaltaren skal rapportere omgåande til ansvarleg departement dersom det blir avdekt vesentlege svakheiter, feil eller manglar i kritiske prosessar eller i aktivitetar i verksemda. Risikovurdering og styring på bakgrunn av dette skal skje innanfor eit samla rammeverk for styring og kontroll, sjå kap. 4.2.1. Verksemda skal jamleg og minst kvart fjerde år vurdere å innføre hendelsesgjennomgangen. Ved vesentlege endringar i risikobiletet eller i verksemda elles skal ei ny vurdering gjerast, jf. rundskriv R-117».

STAFs formelle rolle og funksjon som tjenesteleverandør og databehandlar for statsforvalterembetene

SFIN er behandlingsansvarlig for alle personopplysninger som blir behandlet hos oss. Datatilsynet fastslår at dette ansvaret innebærer at: «Den behandlingsansvarlige må derfor sørge for å etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterlevs til enhver tid.»

Statsforvalterens fellestjenester (STAF) skal levere utvikle og drifte gode administrative tjenester som understøtter statsforvalternes samfunnsoppdrag på områdene IT, digitalisering og utvikling, informasjonssikkerhet, dokumentforvaltning, brukerstøtte og kompetanse og anskaffelser. De leverer også brukerveiledninger og kompetansemateriell på disse områdene.

Statsforvalteren i Innlandet er likevel selv ansvarlig for å ivareta informasjonssikkerhet og personvern, og for å utarbeide egne rutiner som ivaretar dette.

Hendelsesforløp

Nedenfor følger en kort beskrivelse av hendelsesforløpet, basert på rapportering til Datatilsynet og DFD, logg i RAYVN og referater.

Statsforvalteren i Innlandet (SFIN) ble i november 2025 gjort oppmerksom på avvik knyttet til brudd på personopplysningsikkerhet ved bruk av programvaren Foxit i behandlingen av innsynskrav. Avvikene har ført til at det har vært mulig å få tilgang til navn og personnummer i sladdede dokumenter som er sendt ut ved delvis innvilget innsyn.

Det ble umiddelbart gjennomført en systematisk gjennomgang av saks- og arkivsystemet Elements for perioden 1. april 2022 til 2. desember 2025, for å kartlegge omfanget av avviket. Perioden ble valgt etter et risikobasert utvalg av periode, og fordi den sammenfaller med implementering av programmet FOXIT hos Statsforvalteren i Innlandet. Alle enheter gjennomførte et systematisk søk etter samme mal. Målet med kartleggingen var å avdekke antall avvik, antall berørte og antall mottakere av personsensitive opplysninger.

Definisjonen av avvik har vært «en sak der personopplysninger er tilgjengelig i sladdede dokumenter det er gitt delvis innsyn i ved behandling av innsynsbegjæring». Alle enheter har fått samme sjekkliste for kontroll av saker med delvis innsyn.

Tabellen under viser antall saker med delvis innsyn i perioden 1. april 2022 til 2. desember 2025. Av disse 1284 sakene er det avdekket 208 avvik. Avvikene er fordelt på 186 berørte personer. Svar på innsynsbegjæringer er sendt til 20 unike redaksjoner og 21 unike privatpersoner som har krevd innsyn.

Tab. Oversikt over omfang hos Statsforvalteren i Innlandet

	Antall saker med delvis innsyn	Antall avdekte avvik	Antall personer berørt av avviket	Antall medier/virkso mheter som har mottatt dokumenter	Antall privatpersoner som har mottatt dokumenter
Statsforvalteren i Innlandet	1284	208	186	20*	21*

*sum viser antall unike medier/virkso mheter

*sum viser antall unike epostadresser eller personer

Håndtering av hendelsen i november 2025

Hendelsesgjennomgangen viser at Statsforvalteren i Innlandet reagerte raskt da avviket ble kjent i november 2025. Varsling til ledelsen skjedde umiddelbart, og ledergruppen ble samlet samme dag. Kriseledelse ble etablert, og relevante eksterne aktører, herunder departement og andre embeter, ble informert. Gjennomgang av saker ble igangsatt raskt for å få oversikt og redusere

risiko. Datatilsynet ble varslet innen fristen på 72 timer etter at avviket var identifisert. DFD ble varslet samtidig.

Hendeshåndteringen har vært gjennomført av strategisk kriseledelse, koordinering gjennom stab og fortløpende avklaringer av oppgaver. Flere stabsgrupper har vært opprettet og involvert for å sikre effektiv gjennomføring. Analysearbeidet har hatt fokus på kartlegging for å sikre lik metodebruk og en felles situasjonsforståelse. Oppfølgingen har omfattet tiltak som risikovurdering, stikkprøver, systematiske søk, intern og ekstern kommunikasjon, ivaretagelse av ansatte, samt implementering av både strakstiltak og langsiktige løsninger.

Oppfølgingsplanen har inkludert:

- Strategisk kriseledelse og koordinering gjennom stab
- Bruk av flere stabsgrupper for oppgavehåndtering
- Analyse og kartlegging for lik metodebruk og situasjonsforståelse

Oppfølging og lukking av avviket har omfattet:

- Implementering av strakstiltak og langsiktige tiltak
- Stikkprøver og systematisk kartlegging av innsynssaker
- Opprettet sak i avvikssystemet
- Koordinering av talepunkter og pressemelding
- Intern informasjon og ivaretagelse av ansatte
- Utforming av informasjon og risikovurdering til berørte
- Brev til berørte og mottakere av sensitive opplysninger
- Plan for sikker håndtering av innsynsbegjæringer
- Deling av informasjon om kommunikasjon, brev med mer til andre embeter i samme situasjon.
- Obligatorisk opplæring for ansatte og ledere
- Gjennomføring av årsaks- og hendelsesgjennomgang.
- Brev til alle kommuner om å være oppmerksomme på bokmerker i dokumenter de får fra oss (feb 2026)

Utdrag fra tidslinje 20.nov – 17.des

Dato	Innhold
20. nov	Kl. 15:35 Varsel fra journalist til SFIN postmottak
21. nov	<ul style="list-style-type: none">- Helse og omsorg starter kartlegging- Avvik registrert og varslet videre til statsforvalter og ass. statsforvalter- Kriseledelsen samles og vurderer tiltak (førstemøte)- VO'ene og enheter starter kartlegging av omfang- Informasjonsmøte med STAF, DFD og andre embeter- Datatilsynet varsles kl.20.30
22.nov	Omfangskartlegging, kommunikasjonstiltak, analyse
23.nov	Møte med datatilsynet
24.nov	<ul style="list-style-type: none">- Infomøte med tillitsvalgte, info via ledere til ansatte

	<ul style="list-style-type: none"> - Rapporteringsfrist eksternt - Møte med DFD
25.nov	<ul style="list-style-type: none"> - Offentliggjøring ved pressemelding og påfølgende pressebrief - Tilgjengelighet utover kvelden – Hamar
24.- 28.nov	Obligatorisk gjennomgang av rutine for håndtering av innsyns krav og bruk av Foxit. v/ Rettssikkerhetsgruppen og STAF. Tirsdag og onsdag. (+ ett oppsamlingsheat)
10.des	Rapportering DFD og oppdatert varsel til Datatilsynet
15.des	Ledermøte
17.des	Styringsmøte DFD
Des 2025	<ul style="list-style-type: none"> - 10.12. SAMU møte - 10.12. AMU møte (bedriftshelsetjenesten var koblet på) - Møter med tillitsvalgte/HR
Des 2025 – mars 2026	Hendelses- og årsaksgjennomgang. Frist rapport 1. mars

Vurdering av tiltak iverksatt for å håndtere hendelsen

Intern varsling var mindre koordinert enn ønskelig. Funnene indikerer at dagens varslingsveier bør forbedres for å sikre en mer systematisk, forutsigbar og koordinert varsling ved alvorlige hendelser.

Ekstern varsling: Fredag 21. november ble det gjennomført innledende samtaler mellom assisterende statsforvalter, fylkeslegen og organisasjons- og HR-direktør for å vurdere håndteringen av avviket. Det var rask enighet om at situasjonen krevde ekstern varsling til relevante departementer, fagdepartement og øvrige embeter. Første møte i kriseledelsen: kl 1530 den 21. inkluderte hele ledergruppen, samt fylkesberedskapssjef, fylkeslege og Thorbjørn Unneberg.

Intern håndtering av avviket

Avviket ble oppdaget raskt som følge av informasjon fra en journalist og tidlig varsling av ledelsen. Ledelsen hadde tidlig fått oversikt over alvoret i situasjonen.

Krisen ble i hovedsak håndtert i tråd med rutiner for krisehåndtering beskrevet i beredskapsplanen for Statsforvalteren i Innlandet. Det omfatter etablering av kriseledelse og krisestab, der staben inndeles etter de funksjoner den skal ivareta med tematiske arbeidsgrupper og arbeidet koordineres gjennom staben. Krisehåndteringsriggen ivaretar planer for analyse, internt og eksternt kommunikasjons- og informasjonsbehov, iverksetting av møteserier m.m.

Det som avvek fra beredskapsplan og etablerte rutiner er opprettelsen av en felles teams-kanal for informasjonsdeling for alle involverte. Gjeldende praksis er at samordning skjer gjennom bruk

av embetets beredskapsadresse: sfinberedskap@statsforvalteren.no. På grunn av sakens karakter (personsensitive informasjon) - og på grunn av at hendelsen var intern - ble det valgt å ikke benytte beredskapsadressen, men i stedet opprette en lukket Teams-kanal der alle med en rolle i håndteringen hadde tilgang. Teamskanalen var oppfattet som en god plattform for informasjonsdeling.

Når embetet setter stab og krisestab etableres er det viktig at all aktivitet koordineres gjennom stab for å få en effektiv og koordinert krisehåndtering og unngå dobbeltarbeid. Enkelte tilbakemeldinger tyder på at dette kunne ha blitt gjort bedre, noe som kan skyldes manglende opplæring i etablert praksis og beredskapsplanverket.

Oppfølging av berørte parter

Det ble sendt ut brev til berørte parter og mottakere av sensitive opplysninger. Det var også opprettet en telefontjeneste der bl.a. berørte parter kunne ringe inn for å få mer informasjon om saken.

Reaksjoner fra berørte parter og publikum har vært svært få. Det indikerer at vi har greid å nå ut med korrekt informasjon om hendelsen og gjort gode tiltak for å begrense omfanget av avviket.

Det er framkommet en formell sak om søksmål som er svart ut, og det har ikke blitt fulgt opp av vedkommende.

Det har vært få telefoner inn til den opprettede telefontjenesten som omhandlet selve saken. Det har også vært noen oppfølgingstelefoner som ble tatt i de enkelte enhetene.

Læringspunkter fra hendelseshåndteringen

Samlet vurderes håndteringen som god gitt forutsetningene, og særlig på grunn av betydelig innsats og fleksibilitet hos de involverte og bruk av beredskapssystemet. Evalueringen viser likevel et behov for å ytterligere styrke struktur, rolleavklaringer og formelle prosesser for å sikre en enda mer robust og effektiv håndtering ved fremtidige hendelser.

Utfordringer som pekes på i intervjuene:

- Utydelige beslutningslinjer og tidvis for mange involverte i beslutningssløyfe
- Ujevn informasjonsflyt
- Manglende felles metodikk og søkekriterier for søk i arkivsystemet (Elements) i tidlig fase.
- Mangel på superbrukere for systemene i embetet
- Behov for bedre erfaringsdeling underveis i hendelsen.
- En fare for at fokuset for sterkt ble rettet internt under håndteringen, og med spørsmål om saksbehandling ble godt nok ivaretatt.

Tiltak som foreslås:

- Bedre kjennskap til beredskapsplanen, samt hvordan rolle- og ansvarsavklaring er ved krise- og hendelseshåndtering.
- Etablering av mindre og mer målrettede team med klart mandat (kan tyde på behov for bedre kjennskap til beredskapsriggen)
- Tidligere aktivering av beredskapssystemet når alvorlighetsgraden er usikker.

- Mer systematisk tilnærming til informasjonsflyt, loggføring og felles situasjonsforståelse.
- Styrket systemkompetanse og tydeligere superbrukerfunksjoner.
- Bedre struktur for erfaringsdeling både underveis og i etterkant. Forbedre innhold i møteserie

Årsaksanalyse

I dette kapitlet presenterer vi funn fra intervjuer og dokumentgjennomgang. Deretter følger de vurderinger analysegruppen har gjort på bakgrunn av disse.

Funn (datagrunnlag)

I hendelsesgjennomgangen har vi gjennomført intervjuer med ansatte og ledere i virksomheten samt gjennomgått relevante rutiner og dokumenter knyttet til håndtering av innsynsbegjæringer og sladding av dokumenter. Formålet med gjennomgangen har vært å kartlegge hvordan styring, rutiner, opplæring og etterlevelse er organisert og praktisert i virksomheten.

Vi presenterer først funnene fra intervjuer og dokumenter før vi går inn på vurderinger av funnene.

Vedlegg 3 Analyse-intervjuer

Styringssystem, ledelse og ansvar

I intervjuene oppgir flere informanter at de ikke er godt nok kjent med rutinen for håndtering av innsynsbegjæringer og sladding. Enkelte informanter er kjent med at det finnes en rutine i styringsbiblioteket, men flere oppgir at de ikke vet hvor den ligger eller at de ikke har brukt den i praksis.

Rutinen for håndtering av innsynskrav som ble vedtatt i oktober 2024, ligger i styringsbiblioteket, men intervjuene indikerer at denne ikke i tilstrekkelig grad har vært kjent og brukt i organisasjonen.

I intervjuene fremkommer det at flere enheter har utviklet egne rutiner for håndtering av innsynsbegjæringer og sladding. Gjennomgangen av rutiner viser at flere av disse ikke ligger i virksomhetens styringsbibliotek. Dette innebærer at det finnes flere parallelle rutiner i organisasjonen.

Flere informanter beskriver at praksis i stor grad er utviklet gjennom erfaring og lokale arbeidsmåter i enhetene.

Rolle- og ansvarsfordeling

Flere informanter beskriver at ansvarsfordelingen mellom linjeledelse, fag og STAF ikke fremstår som godt nok avklart, særlig i spørsmål som gjelder systeminnføring, teknisk sikkerhet og opplæring.

Det framkommer i intervjuene at det fra embetets side i flere tilfeller har vært en forventning om at STAF ivaretar sikkerhetsvurderinger og opplæring ved innføring av nye systemer. Samtidig beskriver flere informanter at dette ikke oppleves som tydelig nok avklart eller formalisert.

Flere ledere oppgir også at de ikke har tydelig definerte funksjonsbeskrivelser eller formalisert systemansvar knyttet til håndtering av innsyn og sladding. Flere informanter oppgir at kvalitetssikring og kontroll i stor grad har vært basert på erfaring, faglig skjønn og kollegial dialog.

Det framkommer i liten grad beskrivelser av systematisk dokumentert kontroll eller felles praksis for kvalitetssikring på tvers av enheter.

Det eksisterer en databehandleravtale mellom STAF og embetene. STAF eier datasystemene, mens Statsforvalteren er dataeier. I dette forholdet kan det oppstå uklarheter i rolle som bør gjennomgå og klargjøres. For eksempel embetenes rolle med tanke på risikovurderinger ved innføringer av datasystemer.

Kompetanse, opplæring og bevissthet

I intervjuene oppgir mange informanter at opplæring i håndtering av innsynsbegjæringer og sladding i stor grad har skjedd gjennom kollegabasert læring og erfaring. Det fremkommer ikke beskrivelser av et samlet eller dokumentert opplæringsløp for dette arbeidet.

Flere informanter oppgir at de ikke har fått opplæring i teknisk bruk av sladdeverktøyet eller om hva metadata er og at det kan ligge skjult i dokumenter. I intervjuene fremkommer det at flere ansatte ikke var kjent med risiko knyttet til metadata før hendelsen. Det har vært uklare rutiner for hva ledere kontrollerer ved godkjenning.

Samtidig beskriver informantene generelt god kompetanse knyttet til juridiske vurderinger etter offentleglova.

Ingen av informantene viste til systematiske ordninger for å kontrollere eller dokumentere at ansatte har gjennomført opplæring eller behersker teknisk korrekt sladding før de håndterer slike saker.

Flere informanter oppgir at det ikke finnes krav til utsjekk eller verifisering av opplæring.

Styrte prosesser, rutiner og etterlevelse

Virksomheten har en skriftlig rutine for håndtering av innsynsbegjæringer i styringsbiblioteket. Samtidig fremkommer det i intervjuene at denne rutinen ikke er kjent for alle ansatte. Flere informanter oppgir at de ikke vet hvor rutinen ligger, eller at de i praksis benytter lokale rutiner i enhetene. Gjennomgangen av dokumenter viser at rutiner for innsyn og sladding ikke er samlet i ett felles system.

Implementering av endringer

Flere informanter beskriver at innføringen av nytt sladdeverktøy ikke ble ledsaget av strukturert opplæring eller samlet risikovurdering.

Informanter beskriver også at informasjon om endringer i systemer og arbeidsmåter i hovedsak har blitt formidlet uformelt, direkte på Innafor uten noen forutgående kommunikasjon, eller ved korte meldinger, uten systematisk oppfølging i organisasjonen.

Informantene oppga at kvalitetssikring i stor grad har vært basert på erfaring, faglig skjønn og personlig oppfølging i enhetene. Flere informanter beskriver at kontroll og kvalitetssikring i praksis skjer gjennom kollegial dialog eller gjennomgang av saker i enhetene.

Innsynsrutiner og styringsbibliotek

I hendelsesgjennomgangen av innsynssaken har vi gjennomgått dokumenter og struktur i virksomhetens styringsbibliotek. Gjennomgangen viser at dokumenter i systemet er lagret på ulike nivåer. Det foreligger ikke en entydig struktur eller tydelig versjonskontroll for lagringen av dokumentene.

I styringsbiblioteket finnes dokumenter som fremstår som kladder, dokumenter som ikke er formelt godkjent, og dokumenter som fremstår som godkjente rutiner. Disse dokumenttypene ligger i flere tilfeller lagret side om side uten tydelig merking eller angivelse av versjonsstatus. Det er ingen struktur som lenker dokumenter til representative styringsdokumenter.

Gjennomgangen viser også at enkelte rutiner for håndtering av innsyn som brukes i enhetene ikke ligger i styringsbiblioteket. Flere informanter beskriver at rutiner for håndtering av innsyn og sladding finnes lokalt i enhetene og brukes i det daglige arbeidet, uten at disse er registrert eller publisert i styringsbiblioteket.

Kultur, samhandling og organisasjonspraksis

Intervjuene beskriver en organisasjon med høy faglig bevissthet og lav terskel for å diskutere faglige problemstillinger. Flere informanter oppgir at det er vanlig å involvere kolleger eller ledere dersom man er usikker på juridiske vurderinger.

Samhandling med STAF

I intervjuene pekes det blant annet på uklar rolleforståelse og at kommunikasjon ved systemendringer i enkelte tilfeller har vært fragmentert. Flere informanter oppgir også at ansvarsfordelingen mellom faglig og teknisk ansvar ikke oppleves som tydelig avklart.

Embetene har kompetanse på risikovurderinger og bør i større grad bidra inn når STAF vurderer risiko, både når det gjelder anskaffelse- og bruk av datasystemer.

Tiltak etter hendelsen

Flere informanter oppgir at hendelsen har ført til tiltak i organisasjonen. Dette omfatter blant annet felles opplæring og at flere enheter har innført dobbeltkontroll før utsendelse av dokumenter. Informanter beskriver også økt oppmerksomhet rundt metadata og teknisk dokumenthåndtering etter hendelsen.

Vurderinger

Styringssystem, ledelse, roller og ansvar

Hendelsesgjennomgangen viser at kvalitetsstyringssystemet ikke er godt nok kjent i organisasjonen. Rutinen for håndtering av innsynskrav ligger i styringsbiblioteket, men den har ikke vært tilstrekkelig kjent og brukt. Rutiner finnes til dels på flere plattformer, og det blir dermed uklart hva som til enhver tid er gjeldende praksis.

Roller og ansvar er ikke tilstrekkelig avklart, særlig i grensesnittet mellom linjeledelse, fag og STAF. Det foreligger en forventning fra embetet om at STAF ivaretar sikkerhetsvurderinger og opplæring ved systeminnføring, uten at dette er tydelig definert eller fulgt opp. Det oppleves at endringer i systemer har blitt kommunisert uten tilstrekkelig opplæring, felles risikovurdering eller tydelig ansvarsavklaring. Samtidig mangler ledere tydelig formalisert systemansvar og funksjonsbeskrivelse. Dette medfører at praksisen ikke er styrt, og at det blir for mye opp til den enkelte fagenhet hvordan man håndterer innsynssaker. Flere enheter har utviklet egne løsninger, og ledelsens gjennomgang er lite konkret når det gjelder teknisk risiko og kompetansesårbarhet.

Kompetanse, opplæring og bevissthet

Hendelsesgjennomgangen avdekker svakheter i det systematiske arbeidet med kompetansesikring. Opplæringen har i hovedsak vært uformell og kollegabasert, og det var ikke et helhetlig og dokumentert opplæringsløp for håndtering av innsynsbegjæringene og bruk av sladdeverktøy.

Det er ikke etablert mekanismer for å sikre at ansatte faktisk har forstått og behersker teknisk korrekt sladding. Det foreligger heller ingen systematisk utsjekk eller sikring av etterlevelse før ansatte håndterer slike saker.

Bevisstheten rundt juridiske vurderinger etter offentleglova er gjennomgående høy. Derimot har bevisstheten rundt teknisk risiko vært lav før hendelsen. Dette gjelder særlig forståelsen av metadata og risiko ved dokumenthåndtering i nye verktøy. Hendelsen har økt risikobevisstheten, og det er gjennomført opplæringstiltak, men kompetansestyringen bør fortsatt utvikles.

Styrte prosesser, rutiner og etterlevelse

Virksomheten har skriftlig rutine for håndtering av innsynssaker, men den er ikke kjent av alle. Ikke alle er kjent med hvor rutinen ligger (Styringsbiblioteket). Rutiner er ikke tydelig versjonsstyrt eller systematisk implementert. Flere enheter har utviklet egne rutiner, noe som øker risikoen for ulik praksis.

Implementering av nye systemer og endringer har ikke vært ledsaget av strukturert opplæring eller samlet risikovurdering. Overgangen til nytt sladdeverktøy illustrerer svakheter i endringsledelse og internkontroll.

Kontroll og kvalitetssikring har i hovedsak vært basert på kultur, erfaring og personlig årvåkenhet.

Samlet vurderer vi at virksomheten har håndteringsevne når avvik oppstår, men trenger å styrke kvalitetsstyringssystemet for bedre å kunne å sørge for systematisk sikring av kompetanse for å forebygge muligheten for at framtidige avvik kan oppstå.

Kvalitets- og styringssystem

Hendelsesgjennomgangen viser at det finnes rutiner for håndtering av innsyn og sladding, men at et helhetlig system for opplæring i rutinene mangler. Gjennomgangen viser at rutinene ofte blir gjennomgått mellom kolleger, men at det ikke ligger i et sentralt versjonsstyrt kvalitetssystem.

Når styringsbiblioteket også er for lite kjent blant ansatte, øker risikoen for avvik noe som kan føre til ulik praksis. Dagens system støtter ikke i tilstrekkelig grad drift, risikostyring og kontinuerlig forbedring. Rutiner er tilgjengelige, men ligger fragmentert og uten versjonskontroll, noe som også kan gjøre det uklart hva som er gjeldende praksis.

Når hendelsen ble oppdaget, ble den håndtert raskt. Avviket ble meldt både skriftlig og muntlig. Avvikssystemet fremstår som lite integrert i det daglige forbedringsarbeidet, og det er lav bevissthet om hvordan avvik skal meldes, analyseres og brukes systematisk.

Det er behov for å videreutvikle et system for ivaretagelse av rutiner. Rutiner bør verdi- og risikovurderes siden ikke alle er like kritiske. Statsforvalteren har i sum svært mange rutiner og derfor er det nødvendig å gjøre prioriteringer. Rutiner med høy risiko og store konsekvenser må prioriteres både når det gjelder innføring, opplæring og oppfølging.

Kultur, samhandling og forbedring

Hendelsesgjennomgangen viser at virksomheten har en kultur preget av høy faglig bevissthet og sterk ansvarsfølelse. Informanter beskriver åpenhet i faglige diskusjoner og lav terskel for å involvere kolleger og leder ved usikkerhet. Under hendelsen var det rask mobilisering, tydelig lederengasjement og omfattende innsats på tvers av funksjoner.

Samhandlingen med STAF trekkes frem som en gjennomgående utfordring. Flere beskriver uklar rolleforståelse, fragmentert kommunikasjon ved systemendringer og manglende felles risikovurdering. Uklart grensesnitt mellom faglig og teknisk ansvar har bidratt til sårbarhet.

Hendelsen har synliggjort både styrker og svakheter i organisasjon. Den har økt bevisstheten om risiko, aktualisert behovet for tydeligere ansvarslinjer og vist at virksomheten har kapasitet til å

mobilisere raskt. Samtidig viser hendelsesgjennomgangen lærings- og forbedringspunkter på tvers av enheter og virksomhetsområder i embetet.

Vedlegg

- Mandat
- Intervjuguider Toppleder, mellomleder, saksbehandler
- Analyse av intervjuene

Referanser

Beredskapsplan Statsforvalteren i Innlandet [Beredskapsplan SFIN 2.0 - 2024.pdf](#)
(Ligger på fellesområdet/generelt/beredskapsplan og tiltakskort)

Brev fra SFIN til DFD (10.12.2025) Svar på «Videre rapportering om avvik», med referanse 25/3322-27

Forslag fra Rettsikkerhetsgruppa om roller/ansvar

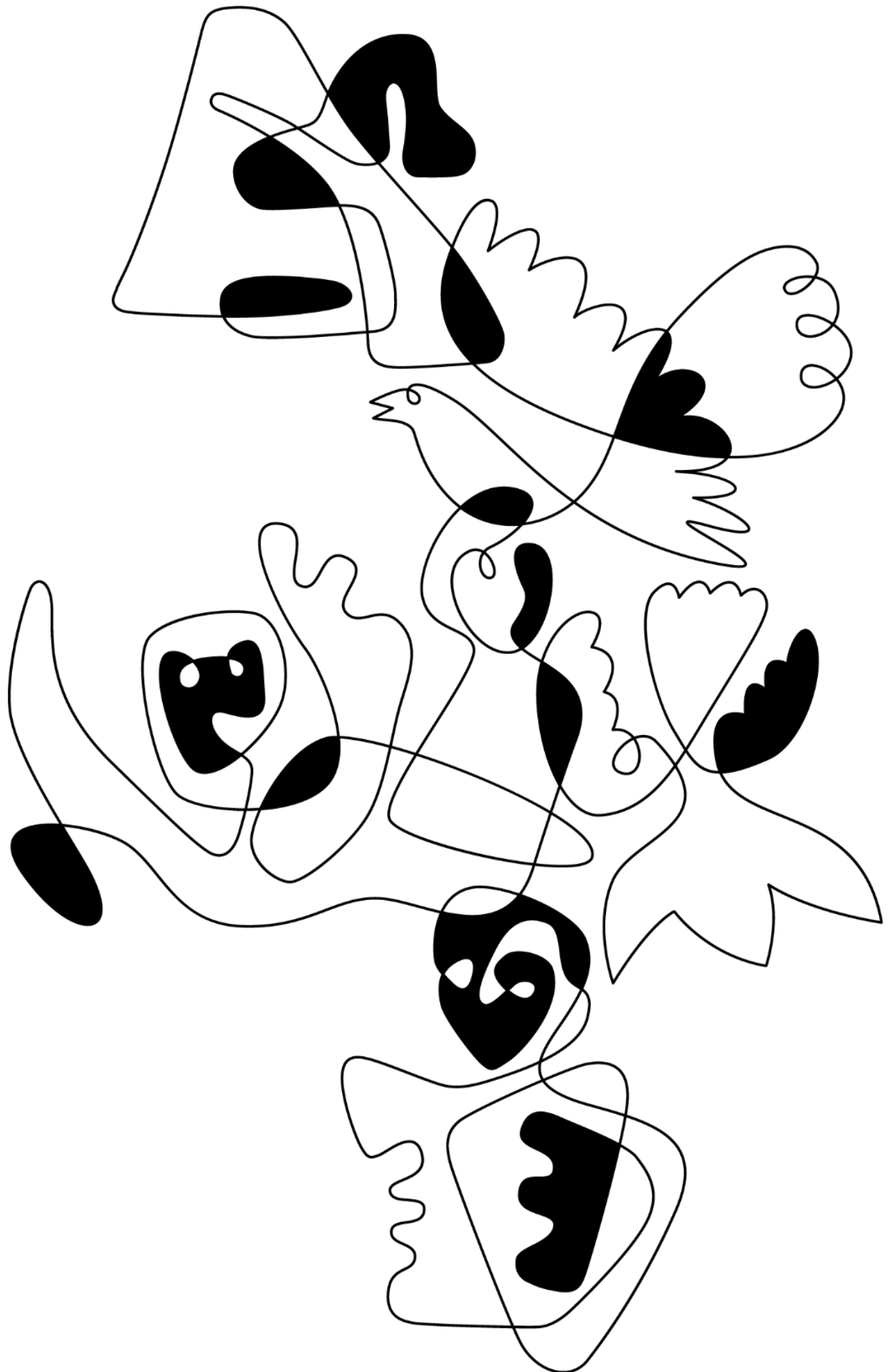
[referat-samu-10.12.2025.pdf](#)

Referater fra kriseledelse, møter i krisestab, RAYVN logg

Rutiner, lover, styringsdokument

STAF rapport til Datatilsynet (09.12.2026): «Svar på krav om redegjørelse – hendelse knyttet til håndtering av innsynskrav – november 2025».

Styringsbiblioteket



STATSFORVALTEREN I INNLANDET

Postboks 987, 2604 Lillehammer | sfinpost@statsforvalteren.no | www.statsforvalteren.no/innlandet



ISBN: 978-82-8410-081-4