Riksrevisjonen

Revisjonsrapport for 2017 om styringssystem for informasjonssikkerhet i Fylkesnemndene for barnevern og sosiale saker

Mottaker: Barne- og likestillingsdepartementet

Revisjonen er en del av Riksrevisjonens kontroll av disposisjoner i henhold til *lov om Riksrevisjonen* § 9 første ledd og *instruks om Riksrevisjonens virksomhet* § 3b. Revisjonen er gjennomført i samsvar med ISSAI 400/4000, INTOSAIs internasjonale prinsipper og standarder for etterlevelsesrevisjon.

Forsideillustrasjon: Riksrevisjonen

Innhold

1 Sammendrag

Fylkesnemndene for barnevern og sosiale saker (fylkesnemndene) har først og fremst som oppgave å fatte vedtak etter *lov om barneverntjenester* (barnevernloven), blant annet i saker om omsorgsovertakelse av barn og tiltak for barn med atferdsvansker. For å gjennomføre oppgavene sine har fylkesnemndene behov for å forvalte personopplysninger om barn, blant annet ved saksbehandling og lagring av informasjon, i forhandlings- og vedtaksmøter, ved frakt av dokumenter utenfor nemndenes lokaler og ved kommunikasjon med eksterne. Det at det foreligger en barnevernssak, medfører utvidet taushetsplikt og gjør at det er behov for beskyttelse. Sikker håndtering av opplysninger om barnet er avgjørende (konfidensialitet). For at tiltakene som settes inn, skal ha høy og riktig kvalitet, er det også avgjørende at opplysningene som blir lagt til grunn i sakene, er pålitelig (integritet).

Fylkesnemndene har med bakgrunn i en tjenesteavtale og vedlikeholdsavtale, satt driften av IKT-infrastrukturen sin og saksbehandlingssystemet ProSak ut til Bufetat. Tjenesteutsettingen har vært gjennomført i flere år, også før Sentralenheten for fylkesnemndene (Sentralenheten) overtok den administrative styringen fra Barne- og likestillingsdepartementet i 2010.

Riksrevisjonen har over flere år påpekt mangler i styring av informasjonssikkerheten i offentlig sektor, blant annet hos Bufetat. Det er også påpekt tilfeller hvor informasjonssikkerhet ikke ble fulgt godt nok opp når IKT-tjenester ble satt ut.[1]

Et styringssystem for informasjonssikkerhet skal hjelpe ledelsen og virksomheten for øvrig til å få tilstrekkelig styring på og kontroll med informasjonssikkerheten gjennom systematisk internkontroll på området. Det skal bidra til at virksomheten velger riktige sikkerhetstiltak, og at de valgte løsningene blir evaluert og forbedret om nødvendig. Styringssystemet skal også bidra til at det blir stilt nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Styringssystemet skaleres til virksomhetens behov, sikkerhetskrav, prosesser, størrelse og struktur.[2] Fylkesnemndenes behov for å sikre informasjon er primært knyttet til sikring av personopplysninger etter krav i *lov om behandling av personopplysninger* (personopplysningsloven). Skaleringen må på den ene siden ta hensyn til at fylkesnemndene behandler personopplysninger i barnevernssaker med utvidet taushetsplikt,[3] og på den andre siden at virksomheten er relativt liten og får IKT-tjenester levert fra en annen statlig virksomhet som håndterer samme type opplysninger. Ved tjenesteutsetting skal en skriftlig avtale med tjenesteleverandøren legge grunnlaget for at personopplysninger blir behandlet med tilfredsstillende informasjonssikkerhet. I avtalen må det stilles krav til sikringstiltak, og det må følges opp at tjenesteleverandøren leverer det som er avtalt.

Målet med revisjonen er å kontrollere om fylkesnemndene har et styringssystem for informasjonssikkerhet som oppfyller kravene i *forskrift om elektronisk kommunikasjon med og i forvaltningen* (eForvaltningsforskriften) og som ivaretar krav i personopplysningsloven.

Revisjonen har i tidsrommet fra juni 2017 til februar 2018 gjennomført dokumentanalyse, møter og observasjoner og analysert uttrekk fra fylkesnemndenes IKT-systemer.

Revisjonskriteriene inkluderer eForvaltningsforskriften § 15 som blant annet stiller krav om styring og kontroll med informasjonssikkerhet i statlige forvaltningsorganer. I tillegg personopplysningsloven § 13 om informasjonssikkerhet for informasjonssystemer som behandler personopplysninger, jf. *forskrift om*

[1] Jf. Dokument 1 (2016–2017) om styringssystemet for informasjonssikkerhet hos blant annet Bufetat, Dokument 1 (2017–2018) om bruk av Valutaregisteret og Dokument 1 (2016–2017) om DSS som tjenesteleverandør for departementene.
[2] ISO 27001 punkt 0.1 Generelt.
[3] Jf. forvaltningsloven § 13 og barnevernloven § 6-7.

behandling av personopplysninger (personopplysningsforskriften) kapittel 2. Det er også benyttet anbefalinger og beste praksis som følger av *NS-ISO/IEC 27001:2017* (ISO 27001) og *NS-ISO/IEC 27002:20*17 (ISO 27002), og anbefaling fra Nasjonal Sikkerhetsmyndighet (NSM), Center of Internet Security (CIS), Datatilsynet og andre relevante aktører. Det kan være utfordrende for fylkesnemndene å vurdere hvordan styringssystemet skal utformes slik at det er tilpasset virksomhetens egenart og samtidig tilfredsstiller regelverket. Fylkesnemndene har startet arbeidet med å utvikle et helhetlig styringssystem for informasjonssikkerhet.

Hovedfunn i revisjonen:

- Fylkesnemndene har ikke et styringssystem for informasjonssikkerhet og har ikke stilt krav til, fulgt opp eller evaluert informasjonssikkerheten i tjenester som er satt ut.
- Sikkerhetstiltak hos tjenesteleverandøren er ikke i henhold til beste praksis.
- Fylkesnemndene følger ikke opp at internkontrollen er innrettet slik at informasjonen i systemene er tilstrekkelig sikret.

Utkast til rapport ble forelagt Barne- og likestillingsdepartementet i brev av 6. april 2018. Departementet har i brev av 26. april 2018 gitt kommentarer til innholdet i rapportutkastet, som det er tatt hensyn til i endelig rapport. Innspill fra departementet om skjerming av informasjon, er benyttet i Riksrevisjonens vurderinger av hvilken informasjon som unntas offentlighet. Departementet har videre uttalt at rapportutkastet inneholder viktige funn som departementet vil følge opp i sitt videre arbeid.

2 Innledning

Fylkesnemndene er et domstollignende og uavhengig statlig organ som avgjør nærmere bestemte saker etter barnevernloven, *lov om kommunale helse- og omsorgstjenester* (helse- og omsorgstjenesteloven) og *lov om vern mot smittsomme sykdommer* (smittevernloven). Fylkesnemndene har som oppgave først og fremst å fatte vedtak etter barnevernloven, blant annet i saker om omsorgsovertakelse av barn og tiltak for barn med atferdsvansker.[4]

I arbeidet sitt forvalter fylkesnemndene personopplysninger om barn, blant annet ved saksbehandling og lagring av informasjon i etatens fagsystem ProSak, i forhandlings- og vedtaksmøter, ved frakt av dokumenter utenfor nemndenes lokaler og ved kommunikasjon med eksterne.[5] Ved barnevernssaker er det behov for beskyttelse. Da gjelder utvidet taushetsplikt, og sikker håndtering av opplysninger om barnet er avgjørende (konfidensialitet).[6] Det er også avgjørende at de opplysningene som blir lagt til grunn i sakene, er pålitelige (integritet), slik at det er mulig å sette inn tiltak med høy og riktig kvalitet.

Offentlige virksomheter har ansvar for å beskytte informasjonen de forvalter.[7] Dette gjelder også når informasjonen blir forvaltet ved bruk av IKT-systemer.[8] I takt med digitaliseringen av offentlig forvaltning blir det stadig viktigere og mer nødvendig med gode styringssystemer for informasjonssikkerhet som kan gi beskyttelse av sensitiv informasjon.[9]

Et styringssystem for informasjonssikkerhet skal hjelpe ledelsen og virksomheten for øvrig til å få tilstrekkelig styring på og kontroll med informasjonssikkerheten gjennom systematisk internkontroll på

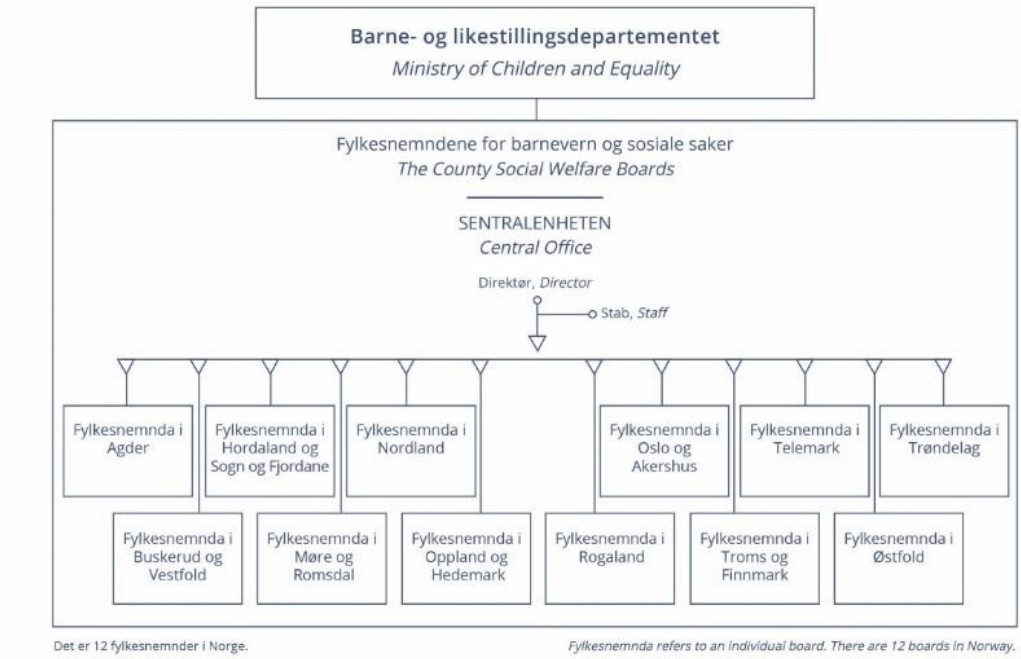
[4] Jf. Barne- og likestillingsdepartementets og fylkesnemndenes hjemmesider.
[5] *Risikovurdering av informasjonssikkerhet*, referat fra møte 3. desember 2015.
[6] Jf. barnevernloven § 6-7 om taushetsplikt og lovkommentar 357. Taushetsplikten gjelder også fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted.
[7] Jf. blant annet forvaltningsloven §§ 13, 13c og 13f.
[8] Jf. forvaltningsloven § 15 a (elektronisk kommunikasjon).
[9] Nasjonal strategi for informasjonssikkerhet har definert sensitiv informasjon til å være informasjon som det av ulike hensyn er viktig å beskytte.

området. Det skal bidra til at virksomheten velger riktige sikkerhetstiltak, og at de valgte løsningene blir evaluert og forbedret om nødvendig. Styringssystemet skal også bidra til at det blir stilt nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Styringssystemet skaleres til virksomhetens behov, sikkerhetskrav, prosesser, størrelse og struktur.[10] Fylkesnemndenes behov for å sikre informasjon er primært knyttet til sikring av personopplysninger etter krav i personopplysningsloven. Skaleringen må på den ene siden ta hensyn til at fylkesnemndene behandler personopplysninger i barnevernssaker med utvidet taushetsplikt,[11] og på den andre siden at virksomheten er relativt liten og får IKT-tjenester levert fra en annen statlig virksomhet som håndterer samme type opplysninger. Ved tjenesteutsetting skal en skriftlig avtale med tjenesteleverandøren legge grunnlaget for at personopplysninger blir behandlet med tilfredsstillende informasjonssikkerhet. I avtalen må det stilles krav til sikringstiltak, og det må følges opp at tjenesteleverandøren leverer det som er avtalt.

De enkelte nemndene var inntil 2010 administrativt underlagt Barne- og likestillingsdepartementet.[12] Da fylkesnemndene ble etablert som selvstendig forvaltningsorgan i 2010, overtok Sentralenheten for fylkesnemndene (Sentralenheten) den administrative styringen fra departementet.[13] Sentralenheten er direktoratsnivået i etaten og har ansvar for den faglige og administrative ledelsen av 12 nemnder, inkludert fellesfunksjoner, jf. figur 1. Fylkesnemndene har totalt 135 medarbeidere. Av disse er 12 stillingshjemler hos Sentralenheten. I tillegg til fast ansatte har nemndene knyttet til seg sakkyndige, advokater med flere.[14]

Figur 1 Organisasjonskart for fylkesnemndene



Kilde: fylkesnemndene.no

[10] ISO 27001 punkt 0.1 Generelt.
[11] Jf. forvaltningsloven § 13 og barnevernloven § 6-7.
[12] *Årsrapport 2009 Fylkesnemndene*, utarbeidet av Barne-, likestillings- og integreringsdepartementet.
[13] Forvaltningsdatabasen, Enheter.
[14] Verifisert referat fra møte mellom fylkesnemndene og Riksrevisjonen den 22. september 2017.

Fylkesnemndene bruker hovedsakelig systemene ProSak og P360 (arkivsystem) til saksbehandling. Systemene ble tatt i bruk i 2015/2016. ProSak er utviklet av fylkesnemndene gjennom eget prosjekt hvor det er gjenbrukt, tilpasset og videreutviklet koder fra Barne-, ungdoms- og familieetaten (Bufetat) sitt egenutviklede system, BiRK. Bufetat er tjenesteleverandør og har ansvar for å drifte fylkesnemndenes systemer.

Riksrevisjonen har over flere år påpekt mangler i styring av informasjonssikkerheten i offentlig sektor, blant annet hos Bufetat. Det er også påpekt tilfeller hvor informasjonssikkerhet ikke ble fulgt godt nok opp når IKT-tjenester ble satt ut.[15]

3 Revisjonens mål og problemstillinger

Målet med revisjonen
Målet med revisjonen er å kontrollere om fylkesnemndene har et styringssystem for informasjonssikkerhet som oppfyller kravene i eForvaltningsforskriften og som ivaretar krav i personopplysningsloven.

Problemstillinger
For å svare på målet med revisjonen er det utarbeidet følgende tre problemstillinger:

1 Har fylkesnemndene etablert et grunnlag for å planlegge sikkerhetstiltak som bidrar til tilfredsstillende informasjonssikkerhet?

  Denne problemstillingen omfatter fylkesnemndenes arbeid med å utarbeide sikkerhetsmål og sikkerhetsstrategi og arbeid med klassifisering og risikovurderinger for sikring av personopplysninger. Dette inkluderer også databehandleravtale ved utsetting av IKT-tjenester.

2 Har fylkesnemndene sikret at det gjennomføres systematiske tiltak som bidrar til tilfredsstillende informasjonssikkerhet for personopplysninger i ProSak og P360?

  Problemstillingen omfatter et utvalg sikkerhetstiltak som påvirker sikkerheten for personopplysninger i ProSak og P360 med underliggende infrastruktur.

3 Har fylkesnemndene fulgt opp at sikkerhetsstrategien og tiltakene gir tilfredsstillende informasjonssikkerhet?

  Denne problemstillingen omfatter rutiner for hendelses- og avvikshåndtering og hvordan fylkesnemndene følger opp at styringssystemet fungerer etter hensikten. Dette inkluderer også oppfølging av avtalte sikkerhetstiltak hos tjenesteleverandøren.

4 Metoder

Revisjonskriteriene som framgår av kapittel 5 har betydning for hvilke revisjonsbevis revisjonen innhenter, og hvilke metoder som blir brukt for å svare på målet og problemstillingene.

Revisjonen har i tidsrommet fra juni 2017 til februar 2018 gjennomført dokumentanalyse, møter og observasjoner og analysert uttrekk fra fylkesnemndenes IKT-systemer.

[15] Jf. Dokument 1 (2016–2017) om styringssystemet for informasjonssikkerhet hos blant annet Bufetat, Dokument 1 (2017–2018) om bruk av Valutaregisteret og Dokument 1 (2016–2017) om DSS som tjenesteleverandør for departementene.

Den 6. februar 2018 avholdt revisjonen et oppsummeringsmøte med fylkesnemndene for å avklare faktagrunnlaget for hver problemstilling.

4.1 Problemstilling 1 og 3 – planlegging og oppfølging av sikkerhetstiltak

For å svare på problemstillingene er det gjennomført dokumentanalyse og møter.

Dokumentanalyse
Formålet med dokumentanalysen er å undersøke om fylkesnemndene har gjennomført og dokumentert krav til arbeidet med informasjonssikkerhet, klassifisering, risikoanalyser, interne revisjoner og evalueringer i tråd med regelverk og anbefalinger i anerkjente standarder.

Dokumentanalysen omfatter relevante dokumenter fylkesnemndene har lagt fram:

- *Retningslinjer for informasjonssikkerhet ved Sentralenheten for Fylkesnemndene for barnevern og sosiale saker*[16]
- *Regler for bruk av ikt-utstyr i fylkesnemndene*[17]
- *De 10 bud for informasjonssikkerhet hos fylkesnemndene*
- ROS-analyser for de ulike nemndene
- beredskapsplaner for de ulike nemndene
- retningslinjer for behandling av taushetsbelagte opplysninger i de ulike nemndene
- tjenesteavtale inkludert databehandleravtale med Bufetat

I tillegg er det vurdert om det finnes policy, retningslinjer og rutiner for sikkerhetstiltak på de områdene revisjonen omfatter.

Andre relevante dokumenter på områdene som er kontrollert i revisjonen, er beskrevet under det aktuelle området i punkt 6.1 og 6.3.

Møter
Revisjonen gjennomførte møter med aktuelle nøkkelpersoner hos Sentralenheten og Bufetat den 22. september og 14.–15. november 2017. Formålet med møtene var å sikre korrekt forståelse av mottatt dokumentasjon, få utfyllende informasjon og gjøre aktuelle avklaringer. For problemstilling 1 og 3 gjaldt møtene følgende områder:

- sikkerhetsmål og sikkerhetsstrategi
- identifisering og klassifisering av informasjonsaktiva
- risikostyring
- databehandleravtalen med Bufetat og oppfølging av denne
- avvikshåndtering
- sikkerhetsrevisjoner
- evaluering og oppfølging av styringssystemet

Referat fra møtene er verifisert.

[16] Datert 24. mai 2017.
[17] Fra 2012, gjelder alle nemndenes bruk av fylkesnemndenes IKT-utstyr.

4.2 Problemstilling 2 – gjennomføring av sikkerhetstiltak

For å svare på problemstillingen er det gjennomført møter, analyser av uttrekk fra fylkesnemndenes systemer og observasjoner. I tillegg er rutiner og styrende dokumenter gjennomgått.

Revisjonen har kontrollert et utvalg tiltak med utgangspunkt i ProSak og P360, og den underliggende infrastrukturen. Sikkerhetstiltakene er valgt på bakgrunn av hva anerkjente aktører innenfor informasjonssikkerhet anser som viktigst for å redusere risiko på informasjonssikkerhetsområdet.[18] Det er lagt til grunn at fylkesnemndene gjennom styringssystemet eller i samarbeid med Bufetat har vurdert og håndtert risiko ved å implementere grunnleggende sikkerhetstiltak på følgende områder:

- tilgangskontroller
    - saksbehandlerrettigheter i ProSak/P360
    - administratorrettigheter
- logging og oppfølging av logger for ProSak/P360 og underliggende infrastruktur
- sikkerhetsoppdatering av operativsystem og programvare på PC-er, databaser og servere
- kontroll med programvare og enheter i nettverket

Revisjonen av de utvalgte sikkerhetstiltakene gir ikke et fullstendig bilde av sikkerhetstilstanden. Resultatene gir imidlertid en indikasjon på om fylkesnemndenes styring av informasjonssikkerhet fungerer etter hensikten.

Revisjonen beskriver situasjonen på tidspunktene for gjennomførte revisjonsbesøk hos Bufetat og uttrekk av data fra november 2017 til januar 2018.

Møter
For å sikre korrekt forståelse av hvordan sikkerhetsarbeidet er organisert og gjennomføres i fylkesnemndene og hos Bufetat, og for å gjøre observasjoner og gjennomgå data for analyse, avholdt revisjonen møter med nøkkelpersoner fra Sentralenheten og Bufetat 14.–15. november 2017 og 17.–18. januar 2018.

Dataanalyse og observasjoner
Revisjonen har gjort observasjoner for å få innsikt i hvordan ulike systemer hos fylkesnemndene og Bufetat blir brukt og fungerer, og om aktuelle sikkerhetstiltak er innført.

Revisjonen har mottatt data om og analysert uttrekk av

- Active Directory (AD) – katalogtjenesten som Bufetat bruker til å håndtere brukere, brukerrettigheter og ressurser i fylkesnemndenes nettverk
- installert programvare, oppdateringer av operativsystem og programvare, og brukere med administratorrettigheter fra applikasjonsserveren for ProSak og fra tre PC-er i nettverket
- tilgangsrettigheter, innstillinger og oppdateringer fra databasen til ProSak

Oppfølgingsspørsmål om resultatene fra analysene er sendt til fylkesnemndene, som har sendt svar i løpet av revisjonsperioden.

[18] Kilder til tiltak for god informasjonssikkerhet:
- The Center for Internet Security (CIS), *CIS Controls for Effective Cyber Defense*
- Nasjonal sikkerhetsmyndighet, *Ti viktige tiltak mot dataangrep*
- Australian Signals Directorate, *Top 4 / Top 35 (Strategies to Mitigate Targeted Cyber Intrusions)*

5 Revisjonskriterier

eForvaltningsforskriften § 15 stiller krav til styringen av og kontrollen med informasjonssikkerhet i statlige forvaltningsorganer.[19] Styringssystemet skal etter § 15 (4) bokstav g – når det er relevant – også inkludere prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon. Personopplysningsloven § 13 stiller krav til informasjonssikkerheten i informasjonssystemer som behandler personopplysninger.

Personopplysningsforskriften § 2-1 sier at reglene i kapitlet gjelder for behandling av personopplysninger i elektroniske systemer der det blant annet er fare for tap av anseelse og personlig integritet. Fylkesnemndene behandler saker som er svært inngripende for barna, familiene og enkeltpersonene sakene gjelder. Nemndenes behandling av personopplysninger er derfor underlagt utvidet taushetsplikt etter helse- og omsorgstjenesteloven § 12-1 og barnevernloven § 6-7. Tiltak som følger av personopplysningsforskriften kapittel 2, er aktuelle for systemer fylkesnemndene forvalter, og skal stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd.

Revisjonen har tatt utgangspunkt i personopplysningsloven og -forskriften som var gjeldende for 2017. Hvordan fylkesnemndene forholder seg til EU-forordning 2016/679 (personvernforordningen/GDPR) som trer i kraft 25. mai 2018, er ikke vurdert.

Etter eForvaltningsforskriften § 15 (2) skal forvaltningsorganet

> «ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem».

Som anerkjente standarder etter eForvaltningsforskriften vil revisjonen ta utgangspunkt i ISO 27001 og ISO 27002.[20]

5.1 Problemstilling 1 – planlegging av sikkerhetstiltak

eForvaltningsforskriften § 15 stiller blant annet følgende krav til planleggingen av sikkerhetstiltak:

- «Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.»

- «Omfang og innretning på internkontrollen skal være tilpasset risiko.»

- «I den utstrekning det er relevant skal sikkerhetsstrategien og internkontrollen for øvrig også adressere, og om nødvendig stille krav til, bl.a.: […] prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, jf. § 5 og § 26, se også personopplysningsloven § 13 og personopplysningsforskriften kap. 2»

ISO 27001 punkt 5.2 gir anbefalinger om innholdet i en overordnet policy som skal gi føringer for styringen av informasjonssikkerhet, og ISO 27002 punkt 5.1.1 gir mer detaljerte anbefalinger om

[19] Jf. forvaltningsloven § 15a.
[20] Jf. referansekatalogen til DIFI.

formål, ansvarsforhold og temaspesifikke policyer som videre pålegger implementering av sikkerhetstiltak.

Kravene til internkontroll på informasjonssikkerhetsområdet forutsetter at det etableres både organisatoriske og tekniske sikkerhetstiltak.[21] Tiltakene som treffes, skal stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd, jf. personopplysningsforskriftens § 2-1. Etter forskriftens § 2-4 skal det føres oversikt over hva slags personopplysninger som behandles. Sikringen av konkrete personopplysninger avhenger av hvilke trusler opplysningene er utsatt for. På bakgrunn av risikovurderinger skal det bestemmes hvilke tiltak som er nødvendige for å sikre virksomhetens personopplysninger, jf personopplysningsforskriften § 2-1 og 2-4. ISO 27001 punkt 6.1.2 gir detaljerte anbefalinger om gjennomføringen av risikovurderinger.

Forholdet mellom en behandlingsansvarlig og en databehandler skal være regulert i en databehandleravtale, jf. personopplysningsloven § 15.[22] Det skal framgå av avtalen at databehandleren plikter å gjennomføre slike sikringstiltak som følger av personopplysningsloven § 13. Etter personopplysningsforskriften § 2-15 skal den behandlingsansvarlige etablere klare ansvars- og myndighetsforhold overfor leverandører. Ansvars- og myndighetsforhold skal beskrives i avtalen. Datatilsynets veileder for databehandleravtale gir veiledning om hva en slik avtale skal inneholde.

5.2 Problemstilling 2 – gjennomføring av sikkerhetstiltak

eForvaltningsforskriften § 15 (4) bokstav g sier at i den grad det er relevant, skal sikkerhetsstrategien og internkontrollen ivareta, og om nødvendig stille krav til, blant annet prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon. Tilsvarende stiller personopplysningsloven § 13 blant annet følgende krav til sikkerhetstiltak ved behandling av personopplysninger:

- «Den behandlingsansvarlige og databehandleren[23] skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.»

- «For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene.»

Nærmere krav til organisatoriske og tekniske sikkerhetstiltak framgår av personopplysningsforskriften kapittel 2. Følgende tiltak må vurderes opp mot sannsynligheten for og konsekvensen av sikkerhetsbrudd, jf. § 2-1 (2):

- tiltak som sikrer at medarbeidere hos den behandlingsansvarlige bare bruker informasjonssystemet for å utføre pålagte oppgaver og selv er autorisert for slik bruk (tilgangsstyring), jf. § 2-8 (1)
- tiltak som sikrer at autorisert bruk av informasjonssystemet registreres, jf. § 2-8 (3), og sikkerhetstiltak som skal gjøre det mulig å oppdage forsøk på uautorisert bruk (logging), jf. § 2-14
- tiltak mot ødeleggende programvare (sikkerhetsoppdatering), jf. § 2-13
- tiltak som skal gjøre det mulig å hindre uautorisert bruk av informasjonssystemet (kontroll med programvare og enheter), jf. § 2-14

[21] Ot.prp. nr. 92 (1998–99) Om personopplysningsloven, kapittel 16, kommentarer til enkeltparagrafer, § 13.
[22] Staten er ett rettssubjekt. En avtale mellom to statlige virksomheter har derfor ikke samme kontraktsrettslige virkninger som en avtale mellom to selvstendige rettssubjekter. Partene kan for eksempel ikke reise søkmål knyttet til avtalen.
[23] Jf. personopplysningsloven § 2 nr. 4 og 5: «behandlingsansvarlige: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes». «databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige».

ISO 27002 punkt 9.1.1, 9.2, 9.4.3, 12.4.1, 12.6.1, 12.6.2 og 13.1.1 gir detaljerte anbefalinger for gjennomføring av sikkerhetstiltak (tilgangsstyring, logging, sikkerhetsoppdatering og kontroll med programvare og enheter).

Revisjonen er også basert på anbefalinger fra Nasjonal sikkerhetsmyndighet (NSM), Center of Internet Security's (CIS) *Critical Security Controls* og andre anbefalinger fra relevante aktører og leverandører.

5.3 Problemstilling 3 – evaluering og oppfølging

eForvaltningsforskriften § 15 (4) bokstav g stiller krav til at internkontrollen om nødvendig også skal ta for seg prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon. Personopplysningsloven § 14 stiller krav om å vedlikeholde informasjonssikkerheten:

> «Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.»

Personopplysningsforskriften gir nærmere krav til vedlikehold av tiltak. Følgende tiltak må vurderes opp mot sannsynligheten for og konsekvensen av sikkerhetsbrudd, jf. § 2-1 (2):

- å gjennomføre jevnlige sikkerhetsrevisjoner av bruken av informasjonssystemet, jf. § 2-5
- å behandle bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd som avvik, med det formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse, jf. § 2-6

Videre gir ISO 27002 i punktene 9.1, 9.2 og 9.3, kapittel 10, punkt 15.2.1 og punkt 16.1 detaljerte anbefalinger for vedlikehold av informasjonssikkerheten (jevnlig gjennomgang og evaluering av styringssystemet, interne revisjoner, korrigerende tiltak, oppfølging av leverandørers tjenesteleveranser og informasjonssikkerhetshendelser).

Revisjonskriteriene er spesifisert nærmere under hvert av de aktuelle områdene i kapittel 6 *Funn* og i vedlegg.

6 Funn

I dette kapitlet presenteres revisjonskriterier og funn for hvert av områdene under de tre problemstillingene revisjonen dekker.

Det er i tillegg utarbeidet et vedlegg som gir en mer detaljert framstilling av revisjonsfunn i rapportens punkt 6.2. Vedlegget er unntatt offentlighet fordi kunnskap om innholdet vil kunne lette gjennomføring av straffbare handlinger, jf. *lov om rett til innsyn i dokument i offentlig virksomhet* (offentlighetsloven) § 24 (3).

6.1 Problemstilling 1 – planlegging av sikkerhetstiltak

6.1.1 Sikkerhetsmål og sikkerhetsstrategi

Ifølge eForvaltningsforskriften § 15 (1) skal mål og strategi for informasjonssikkerhet i virksomheten være beskrevet (sikkerhetsmål og sikkerhetsstrategi) og danne grunnlaget for virksomhetens internkontroll (styring og kontroll) på informasjonssikkerhetsområdet.

ISO 27001 punkt 5.2 angir at en sikkerhetspolicy bør inneholde en forpliktelse til å oppfylle aktuelle krav til informasjonssikkerhet og en forpliktelse til kontinuerlig forbedring av styringssystemet. Videre anbefaler ISO 27002 punkt 5.1.1 at virksomheten beskriver formål og ansvarsforhold knyttet til styring av informasjonssikkerheten.

Revisjonen viser:

- Fylkesnemndene har ikke et overordnet styringsdokument for informasjonssikkerhet.
- Når det gjelder informasjonssikkerhet i elektroniske systemer, er det lagt opp til at krav til sikkerheten i fylkesnemndenes systemer skal bygge på Bufetats styringssystem for informasjonssikkerhet[24]

Fylkesnemndene har ikke en overordnet beskrivelse av hvordan de skal oppfylle aktuelle krav til informasjonssikkerhet, eller hvordan de skal gjennomføre kontinuerlig forbedring av informasjonssikkerheten. Overordnede formål, prinsipper for klassifisering, risikostyring, hendelseshåndtering, leverandørforhold, interne revisjoner og ansvarsforhold for styring av informasjonssikkerhet er heller ikke beskrevet.

6.1.2 Identifisering og klassifisering av informasjonsaktiva/-verdier

Ifølge eForvaltningsforskriften § 15 (4) bokstav g skal sikkerhetsstrategien og internkontrollen også stille nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon. Personopplysningsforskriften § 2-4 stiller krav om at det skal føres oversikt over hva slags personopplysninger som behandles.

Revisjonen viser:

- Fylkesnemndene har identifisert at de har skjermingsverdige personopplysninger i saks- og ansettelsesforhold.
- Det er ikke dokumentert en helhetlig oversikt over, eller en klassifisering av informasjonsaktiva/-verdier, og heller ikke en prosedyre for behandling av slike.

Dokumentanalysen viser at fylkesnemndene ikke har rutiner eller prosedyrer for klassifisering av aktiva eller dokumentert klassifisering av informasjonsaktiva/-verdier.

Sentralenheten og alle nemndene har gjennomført ROS-analyser av uønskede hendelser, blant annet taushetsbelagte opplysninger på avveie.[25] ROS-analysene omhandler primært fysisk sikring av informasjon. I beredskapsplanen for flere av nemndene står det:

> «Fylkesnemnda har et spesielt ansvar for å sikre den enkeltes personvern. Personopplysninger som fremkommer i saks- eller ansettelsesforhold, skal håndteres og oppbevares slik at de skjermes mot innsyn og tyveri. Faglig og administrativt produseres også kunnskap og informasjon som krever skjerming mot uønsket innsyn og tyveri. Datamaskiner krever skjerming mot tyveri og sabotasje.»[26]

6.1.3 Risikostyring

Ifølge eForvaltningsforskriften § 15 (3) skal internkontrollen ha et omfang og en innretning som er tilpasset risikoen. ISO 27001 punkt 6.1.2 angir at det skal defineres og etableres en prosess for risikovurdering av informasjonssikkerheten.

[24] Verifisert referat fra revisjonsbesøk 14.–15. november 2017.
[25] ROS-analyse punkt 3 «Analyse av uønskede hendelser».
[26] Blant annet beredskapsplaner for Troms og Finnmark, Trøndelag, Hordaland og Sogn og Fjordane.

Revisjonen viser at det ikke er etablert en helhetlig prosess for risikovurdering av informasjonssikkerhet i fylkesnemndene som kan gi grunnlag for å vurdere omfanget av og innretningen på internkontrollen:

- Det er gjennomført ROS-analyser i de enkelte nemndene og Sentralenheten med hovedvekt på fysisk sikkerhet, og det er gjennomført en risikovurdering ved utvikling av saksbehandlingssystemet ProSak.
- Det er ikke gjennomført en risikovurdering rettet mot fylkesnemndenes IKT-infrastruktur, som er satt ut til Bufetat.

Sentralenheten opplyser at det er gjennomført en ROS-analyse for hver nemnd med hovedvekt på fysisk sikkerhet.[27] En felles ROS-analyse for informasjonssikkerhet er ennå ikke godkjent, og det er derfor ikke etablert noe systematisk arbeid på dette området. Det ble gjort en felles risikovurdering i fylkesnemndene i desember 2015, hvor nemndenes største risikoer innenfor informasjonssikkerhet og beskyttelse av personopplysninger ble gjennomgått. Hovedvekten i risikovurderingen lå på taushetsbelagt informasjon i fysiske dokumenter og fysisk sikkerhet, men informasjon på PC-er i salene, bruk av e-post og faks ble også vurdert.[28]

I 2017 ble det i tillegg gjennomført en risikovurdering av informasjonssikkerheten i Sentralenheten.[29] I beskrivelsen av formålet med risikovurderingen i Sentralenheten heter det:

> «Fylkesnemndenes tilknytning til Bufdirs styringssystemer for ikt og drift samt utvikling av ikt innebærer at arbeidet med informasjonssikkerhet i egen virksomhet avgrenses til fysisk sikring av taushetsbelagt informasjon og kunnskap, kompetanse og kultur blant de ansatte».

Det foreligger en risikovurdering av ProSak fra februar 2015 som er utført av Infosec Norge AS for fylkesnemndene.[30] Dokumentanalysen viser at risikovurderingen gjelder fase 1 av utviklingen av ProSak. Risikovurderingen «konkluderer med at det må gjennomføres tiltak for å bringe risikoen ned på et akseptabelt nivå, slik at kravene til informasjonssikkerhet blir ivaretatt». Blant annet må sikkerhetsløsningen som etableres, «hindre tilgang til andre URL, hindre direkte kommunikasjon mellom eksterne nettverk og ProSak og sanntidskontroll mot ødeleggende programvare». Sentralenheten opplyser at tiltakene fra denne vurderingen er inkludert i utviklingen av systemet, og det foreligger dermed ingen oversikt over tiltakene og om disse er iverksatt.[31] Planen var at en ny sikkerhetsrevisjon etter innføringen av Saksportalen ville vise iverksettingen av tiltakene fra 2015-rapporten. Denne sikkerhetsrevisjonen er utsatt som følge av at også Saksportalen er utsatt.

Ved revisjonsbesøk hos Bufetat har etaten opplyst at de ikke gjennomfører risikovurderinger rettet spesielt mot fylkesnemndenes systemer, men vurderer risikoer i sine egne systemer, som tilsvarer dem fylkesnemndene bruker. For styringssystemet til Bufetat er det utarbeidet egne maler og rutiner. Tilsvarende maler og rutiner finnes foreløpig ikke for fylkesnemndenes systemer, men vil bli utarbeidet som en del av fylkesnemndenes eget styringssystem, som nå er påbegynt.

[27] Verifisert referat fra møte mellom fylkesnemndene og Riksrevisjonen den 22. september 2017.
[28] *Risikovurdering av informasjonssikkerhet*, referat fra møte 3. desember 2015.
[29] *Risikovurdering Informasjonssikkerhet*, udatert men henviser til krav i tildelingsbrev fra BLD for 2017.
[30] *Risikovurdering av ProSak*, InfoSec, februar 2015.
[31] Verifisert referat fra revisjonsbesøk 14.–15.november 2017.

6.1.4 Databehandleravtale med Bufetat

Ifølge eForvaltningsforskriften § 15 (4) bokstav g skal sikkerhetsstrategien og internkontrollen også stille nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Personopplysningsloven § 13 stiller krav om at den behandlingsansvarlige og databehandleren gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet. Etter § 15 kan en databehandler ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. I avtalen skal det også gå fram at databehandleren plikter å gjennomføre slike sikringstiltak som følger av lovens § 13. Personopplysningsforskriften § 2-15 krever at den behandlingsansvarlige skal etablere klare ansvars- og myndighetsforhold overfor leverandører. Ansvars- og myndighetsforhold skal beskrives i avtale. Datatilsynet har utgitt en veileder om hva en databehandleravtale skal og bør inneholde for å oppfylle kravene til tilfredsstillende informasjonssikkerhet.[32] Veilederen påpeker at detaljeringsgraden i avtalen bør reflektere avtalens omfang og om det behandles sensitive personopplysninger.

Revisjonen viser at fylkesnemndene har en databehandleravtale med Bufetat som inneholder flere av elementene som Datatilsynet anbefaler, men at avtalen mangler bestemmelser om sikkerhetsrevisjoner og hva databehandleren skal ha på plass av sikringstiltak for å gi tilstrekkelig informasjonssikkerhet. Det er ikke godt nok dokumentert hvordan prosessene og kommunikasjonen mellom Sentralenheten og Bufetat skal foregå.

Tjenesteutsettingen av drift er regulert i en tjenesteavtale mellom fylkesnemndene og Bufetat datert 5. juni 2015, hvor databehandleravtalen er et bilag. Databehandleravtalen er sammenlignet med kravene i Datatilsynets veileder for utforming av en slik avtale. Dokumentanalysen viser at databehandleravtalen inneholder mange bestemmelser om hva en avtale skal omfatte for å oppfylle kravene om informasjonssikkerhet. Dette gjelder kravene om

- hva som er formålet med å behandle personopplysningene
- hvordan personopplysningene skal behandles
- databehandlerens bruk av underleverandører

Gjennomgangen viser at databehandleravtalen mangler bestemmelser om

- sikkerhetsrevisjoner
  Den behandlingsansvarlige skal avtale med databehandleren at det skal gjennomføres sikkerhetsrevisjoner jevnlig for systemer som omfattes av avtalen. I henhold til Datatilsynets veileder kan en slik revisjon omfatte en gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede tiltak. Databehandleravtalen inneholder ingen bestemmelser om hvor ofte sikkerhetsrevisjoner skal foretas.

- tilfredsstillende informasjonssikkerhet hos databehandleren
  Ifølge veilederen må avtalen klargjøre hva databehandleren skal ha på plass av sikringstiltak for å ivareta konfidensialitet, integritet og tilgjengelighet for behandling av personopplysninger, jf. personopplysningsforskriftens kapittel 2. I databehandleravtalens punkt 4 om informasjonssikkerhet heter det at «ikt-seksjonene i BSA[33] har et selvstendig ansvar for informasjonssikkerhet. Ikt-seksjonene i BSA forholder seg til enhver tid gjeldende sikkerhetsbestemmelser i Bufetat.» Dokumentanalysen av databehandleravtalen viser at avtalen ikke konkretiserer ytterligere hva dette innebærer.

[32] Datatilsynet – «Veileder databehandleravtale», publisert 26.05.2009, oppdatert 13.6.2017. Ingen innholdsmessige endringer i veilederen for aktuelle punkter.
[33] BSA – Bufetats senter for administrasjon og utvikling i Tønsberg.

Dokumentanalysen viser videre at krav og rapportering som framkommer i avtalene med Bufetat, ikke dokumenterer godt nok hvordan prosessene og kommunikasjonen mellom virksomhetene skal foregå.

6.1.5 Temaspesifikke policyer og retningslinjer

Ifølge eForvaltningsforskriften § 15 (1) skal sikkerhetsstrategien danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

ISO 27002 punkt 5.1.1 anbefaler at sikkerhetsstrategien understøttes av temaspesifikke policyer, som videre pålegger implementering av sikringstiltak for informasjonssikkerhet, og som er strukturert for å dekke behovene til bestemte målgrupper innenfor en organisasjon eller for å ta opp bestemte tema.

Revisjonen viser at fylkesnemndene delvis har utarbeidet temaspesifikke policyer og retningslinjer for informasjonssikkerhet som skal danne grunnlag for hvilke sikkerhetstiltak som skal implementeres:

- Gjennomførte ROS-analyser i Sentralenheten og alle nemndene danner grunnlaget for virksomhetens internkontroll for sikkerhet og beredskap, og det foreligger retningslinjer for håndtering av dokumenter med taushetsbelagt informasjon og regler for de ansattes bruk av IKT-utstyr.
- Fylkesnemndene har opprettet et sentralt sikkerhetsforum, men dette omfatter ikke IKT-teknisk sikkerhet, fordi dette anses dekket gjennom avtalene med Bufetat.
- For sikkerhetstiltak som gjennomføres hos Bufetat, har fylkesnemndene stilt lite krav til policyer, retningslinjer og rutiner. Gjennom avtalene med Bufetat er det også lite dokumentert hvordan prosessene og kommunikasjonen om sikkerhetstiltak skal foregå. Fylkesnemndene har basert seg på Bufetats styringssystem.

Sentralenheten

Sentralenheten har utarbeidet *Retningslinjer for informasjonssikkerhet ved Sentralenheten for Fylkesnemndene for barnevern og sosiale saker.*[34] Retningslinjene omhandler primært hvordan Sentralenheten skal behandle fysiske dokumenter med taushetsbelagte personopplysninger i sine lokaler. Videre framgår det at *Regler for bruk av ikt-utstyr i fylkesnemndene*, som er en del av tjenesteavtalen med Bufetat,[35] gjelder for elektronisk lagrede personopplysninger. Sentralenhetens dokument gir også retningslinjer for lagring i sikker sone, håndtering av passord, låsing og avlogging fra datamaskinen, håndtering av e-post og tekstmeldinger med taushetsbelagte opplysninger, bruk av telefaks, skanning av dokumenter, bruk av det elektroniske arkivet P360 og håndtering av informasjonssikkerhetsbrudd. Det framgår av dokumentet at det skal ses i sammenheng med risikovurderingen, men det står ingenting om hvilken risikovurdering det gjelder.

Det er også utarbeidet et dokument, *De 10 bud for informasjonssikkerhet hos fylkesnemndene*, som er en kortfattet, punktvis oversikt over informasjonssikkerhet.[36] Blant annet er det vist til at IKT-brukere er ansvarlige for å følge *Regler for bruk av ikt-utstyr i fylkesnemndene.*

De enkelte nemndene

I rapportering fra fylkesnemndene til departementet 30. mai 2014 om sikkerhet og beredskap går det fram at Sentralenheten har pålagt nemndene å gjennomføre ni sikkerhetstiltak etter

[34] Datert 24. mai 2017.
[35] Fra 2012, gjelder alle nemndenes bruk av fylkesnemndenes IKT-utstyr. Reglene er et krav fra Bufetat etter tjenesteavtalen bilag 1, *Krav fra ikt-seksjonene i BSA*, og dokumentet er laget etter mal fra Bufetats styringssystem. I verifisert referat fra revisjonsbesøk 14.–15.november 2017 framgår det at retningslinjene er utdaterte, og at Bufetat skal oppdatere dem.
[36] Udatert.

minimumsstandarder. Ett av disse er å skjerme personopplysninger. Personsikkerheten framstår som det mest sentrale i alle tolv nemndene, deretter at det er en «risikoutfordring at fylkesnemndene behandler så mange opplysninger som er av sensitiv karakter». Det framgår også at det er «iverksatt tiltak for å bedre skjermingen og oppbevaringen av disse dokumentene».

Rapportering for 2015 viser blant annet at det dette året ble utarbeidet en felles mal som ble formidlet til alle nemndene, slik at hvert kontorsted kunne gjøre en ROS-analyse ut fra sine lokale forhold. Videre viser den at gjennomgangen som ble gjort i 2015, var den første systematiske analysen av sikkerhet og beredskap i virksomheten. I ROS-analysene har det blitt gjort analyser av uønskede hendelser som brann, innbrudd/tyveri, strømbrudd, vannlekkasje, personskade / medisinske problemer, trusler, taushetsbelagte opplysninger på avveie og negativ medieoppmerksomhet. Rapportering for 2016 viser at det i etterkant av en fagdag om sikkerhet og beredskap i januar 2016 ble utarbeidet en mal for tiltakskort med instruksjoner for håndtering av uønskede situasjoner som kan oppstå. Tiltakskortene plasseres slik at de er lett tilgjengelige.[37]

Alle de tolv fylkesnemndene har utarbeidet beredskapsplaner som har til hensikt å forberede medarbeiderne på uønskede hendelser og krisesituasjoner som kan oppstå. De skal hindre eller begrense skader på mennesker, miljø og materiell. Halvparten av beredskapsplanene omhandler også skjerming av personopplysninger.[38]

I tillegg viser rapporteringen for 2016 at fylkesnemndene i løpet av 2016 ferdigstilte etableringen og implementeringen av retningslinjer for behandling av taushetsbelagte opplysninger i hver nemnd. Bakgrunnen for dette var både pålegg fra Datatilsynet og risikoen knyttet til håndteringen av sensitive personopplysninger. Sentralenheten planla å følge opp arbeidet i 2017.[39] Det er utarbeidet egne retningslinjer for elleve av tolv nemnder. Retningslinjene inneholder rutiner for å sikre taushetsbelagte opplysninger ved håndtering av informasjon og dokumenter i og utenfor nemndas lokaler, ved bruk av PC, post, telefon, e-post, telefaks med mer.[40]

Sentralenheten opplyser at det i 2017 ble opprettet et sikkerhetsforum med sikkerhetsansvarlige fra hver nemnd, i tillegg til Sentralenhetens stabssjef og systemeier. Etter første møte i forumet i august 2017 ble det nedsatt en arbeidsgruppe som skal jobbe med en ny sentral rutine for informasjonssikkerhet som skal være grunnlag for alle nemndene. Forumet omfatter ikke IKT-teknisk sikkerhet, ettersom dette anses dekket gjennom avtalene med Bufetat.[41]

Bufetat
Som nevnt i punkt 6.1.1 bygger fylkesnemndene på Bufetats styringssystem for informasjonssikkerhet når det gjelder informasjonssikkerheten i elektroniske systemer.

Bufetat har utarbeidet policyer, retningslinjer og rutiner som benyttes i driften av etatens egne systemer. Det er ikke tatt stilling til hvilke av disse som eventuelt også gjelder for drift av fylkesnemndenes systemer.

Fylkesnemndene og Bufetat har etablert prosesser og kommunikasjon på flere av områdene som er omfattet av revisjonen, og for sikkerhetsoppdateringer (patching) benyttes en felles rutine. Det er ikke utarbeidet noen beskrivelse av krav til og gjennomføring av følgende sikkerhetstiltak:

[37] Årsrapport 2015 og 2016 punkt 4.2.2 «Sikkerhet og beredskap», ROS-analyse punkt 3 «Analyse av uønskede hendelser».
[38] For eksempel for Rogaland, Troms og Finnmark, Trøndelag, Østfold, Hordaland og Sogn og Fjordane, Møre og Romsdal.
[39] Årsrapport 2016 punkt 4.2.3 «Informasjonssikkerhet» jf. årsrapport fra 2014 punkt 4.4 «Vesentlige forhold for styring og kontroll i virksomheten», e-post fra fylkesnemndene til BLD datert 7. november 2016 «Bestilling - innhenting av informasjon om fellesføring i tildelingsbrev 2016 - om informasjonssikkerhet».
[40] Rutinebeskrivelser for behandling av personopplysninger og taushetsbelagt informasjon - Drammen, Kristiansand, Moss, Skien, Stavanger, Bergen, Bodø, Lillehammer, Molde, Oslo og Trondheim.
[41] Verifisert referat fra møte mellom fylkesnemndene og Riksrevisjonen den 22. september 2017. Ny sentral rutine, datert 5. februar 2018.

- tilgangsstyring for
    - saksbehandlere i ProSak og P360
    - brukere med administratorrettigheter[42] på PC-er, databaser, servere og nettverk
    - passord
- logging og oppfølging av logger
- styring av programvare
- styring av enheter i nettverket

Når det gjelder revisjoner og evaluering av sikkerhetstiltak, er det ikke utarbeidet policyer, retningslinjer og rutiner. Se også punkt 6.2 om gjennomføring av sikkerhetstiltak og punkt 6.3 om etterkontroll og evaluering.

6.2 Problemstilling 2 – gjennomføring av sikkerhetstiltak

Revisjonen har undersøkt om fylkesnemndene har etablert sikkerhetstiltak for systemene ProSak og P360 med underliggende infrastruktur.

Oppsummert viser kontrollene at sikkerhetstiltak for applikasjonene ProSak og P360 gjennomføres i tråd med anbefalinger, men at flere sikkerhetstiltak for underliggende infrastruktur (PC, database, applikasjonsserver og nettverk) ikke gjennomføres som anbefalt. Sikkerhetstiltakene som er kontrollert, er tilgangskontroller, logging, sikkerhetsoppdatering og kontroll med programvare og enheter i nettverket.

6.2.1 Tilgangsstyring

Personopplysningsforskriften § 2-8 (1) krever at medarbeidere hos den behandlingsansvarlige bare skal bruke informasjonssystemet for å utføre pålagte oppgaver, og selv må være autorisert for slik bruk.

ISO 27002 punkt 9.2 anbefaler at virksomheten har etablert en formell prosess for registrering, endring og sletting av tilganger ved tiltredelse, fratredelse eller endring i arbeidsforholdet.

ISO 27002 punkt 9.1.1 anbefaler at tilgang til informasjon og systemer begrenses i henhold til tjenstlig behov, det vil si at medarbeidere ikke bør gis tilgang til mer enn de trenger for å utføre oppgavene sine. Ved utvidede tilgangsrettigheter bør det benyttes en annen dedikert brukerkonto enn den som brukes for vanlige aktiviteter i virksomheten.

Nasjonal sikkerhetsmyndighet (NSM) anbefaler at sluttbrukere ikke tildeles utvidede rettigheter som lokal administrator på PC-er, og framhever dette som et av de fire viktigste tiltakene mot dataangrep.[43] NSM anbefaler videre at i de tilfeller der en sluttbruker har behov for utvidede rettigheter, bør dette håndteres særskilt og kompenserende tiltak vurderes. Dersom sluttbrukeren er gitt utvidede rettigheter på PC-en, er det lettere for en angriper å ta kontroll over PC-en. Videre gir utvidede rettigheter en angriper flere muligheter for kartlegging og angrep videre inn i systemene fra PC-en. Det er også en risiko at sluttbrukeren kan installere programvare med kjente sårbarheter som ikke er ønskelige i virksomhetens nettverk.

ISO 27002 punkt 9.4.3 anbefaler at virksomheten har et system som sikrer passordkvalitet og jevnlig bytte av passord. Brukere bør ha individuelle kontoer med eget passord for å ivareta ansvarlighet.

[42] Med «administratorrettigheter» menes brukere som har rettigheter til å administrere PC-er, databaser, serverer og nettverk. Dette er de sterkeste rettighetene til systemene.
[43] Nasjonal sikkerhetsmyndighet: *Fire effektive tiltak mot dataangrep* (sjekkliste nr. 1).

Microsoft anbefaler å stille strenge krav til autentisering ved bruk av kontoer med administratorrettigheter.[44]

Revisjonen viser:

- Fylkesnemndene har ikke utarbeidet policy, retningslinjer eller rutiner for tilgangsstyring eller gjennomgang av rettigheter, jf. punkt 6.1.5.
- Det er etablert en formell prosess for tildeling av rettigheter slik ISO 27002 anbefaler for saksbehandlerrettigheter i ProSak og P360, men ikke for administratorrettigheter for PC, database, server og AD.
- Administratorrettigheter i fylkesnemndenes infrastruktur er ikke begrenset og kontrollert slik det anbefales etter ISO-standarden og av Microsoft. Se vedlegg for nærmere detaljer.
- Passordkravene til fylkesnemndene er svakere enn forutsatt, og det er ikke stilt strenge passordkrav for brukere med administratorrettigheter, slik det er anbefalt.
- Det er ikke etablert etterkontroll av tilganger.

Tilgang til ProSak/P360 for saksbehandlere
Når nye brukere skal opprettes og eksisterende brukere skal endres eller deaktiveres i fylkesnemndenes systemer, sender Sentralenheten en bestilling via et nettskjema til Bufetats brukerstøtte. Brukerstøtten oppretter brukere og aktiverer enkelte rettigheter i AD, blant annet muligheten til å åpne saksbehandlersystemene. Bestilling og kvittering registreres i Bufetats brukerstøttesystem. Rettigheter i ProSak og P360 registreres og vedlikeholdes av Sentralenheten. En analyse av rettighetene viser at ProSak og P360 er ajourholdt, men at det finnes brukere i AD som er sluttmeldt av Sentralenheten, men som ikke er deaktivert.

Passord
Passord styres i AD, og AD bekrefter brukere ved pålogging til både ProSak, P360, database, servere og nettverk. Uttrekk av AD viser at de samme kravene til passord gjelder for brukerkontoer med administratorrettigheter som for vanlige brukerkontoer. Bufetat opplyser at fjerntilkobling til fylkesnemndenes nettverk krever tofaktorautentisering. Sentralenheten opplyser at passordkravene til fylkesnemndene skal være like strenge som Bufetats egne krav. Ved en feil var det likevel satt opp svakere krav til passord for fylkesnemndene.

Etterkontroll av brukere og tildelte rettigheter
Observasjoner viser at det ikke er etablert etterkontroll av brukere og tildelte rettigheter, herunder utvidede rettigheter og passord. Dette gjelder for både ProSak/P360, PC-er, database, server og AD.

6.2.2 Logging

Personopplysningsforskriften § 2-8 (3) krever at autorisert bruk av informasjonssystemet skal registreres. Videre krever § 2-14 at sikkerhetstiltak skal gjøre det mulig å oppdage forsøk på uautorisert bruk av systemer med personopplysninger.

ISO 27002 punkt 12.4.1 anbefaler å produsere hendelseslogger som registrerer brukeraktiviteter (inkludert påloggingsinformasjon og bruk av privilegier), avvik, feil og informasjonssikkerhetshendelser. Videre anbefales det at logger oppbevares og gjennomgås regelmessig, og at logginformasjon beskyttes mot misbruk og uautorisert tilgang.

Revisjonen viser:

[44] Microsoft: *Best Practices for Securing Active Directory*.

- Fylkesnemndene har ikke utarbeidet policy, retningslinjer eller skriftlige rutiner for logging og gjennomgang av logger for ProSak eller fylkesnemndenes nettverk, jf. punkt 6.1.5.
- Det er i hovedsak etablert logger, men disse gjennomgås ikke systematisk.
- For fylkesnemndene er det ikke etablert etterkontroll av logging.

Fylkesnemndene opplyser at det er etablert logger for ProSak hvor det skal være mulig å kontrollere autorisert og eventuell uautorisert bruk av systemet. Slik kontroll av logger er ikke systematisert og gjennomføres ikke regelmessig. For underliggende infrastruktur er det bare delvis etablert logging og oppfølging av loggene.

En etterkontroll av logging er aktuelt når det er stilt krav om logging og loggene benyttes aktivt i virksomheten. For fylkesnemndene er det bare delvis definert hva som skal logges, og hvordan logger skal følges opp. Det er heller ikke vurdert om praksisen for logging og oppfølgingen av logger fra ProSak, databasen eller nettverk er god nok.

6.2.3 Sikkerhetsoppdatering

Personopplysningsforskriften § 2-13 krever at det skal treffes tiltak mot ødeleggende programvare. ISO 27002 punkt 12.6.1 anbefaler at virksomheten iverksetter tiltak for å håndtere risiko forbundet med tekniske sårbarheter.

Nasjonal sikkerhetsmyndighet (NSM) anbefaler at sikkerhetsoppdateringer for installert programvare anvendes så fort som mulig fordi kunnskap om nyoppdagede sårbarheter spres og utnyttes raskt.[45] NSM framhever dette tiltaket som et av de fire viktigste tiltakene mot dataangrep.[46] Center for Internet Security anbefaler at virksomheter tar i bruk verktøy som automatisk oppdaterer operativsystem og annen programvare for alle systemer.[47] Sikkerhetsoppdateringer beskytter virksomhetene mot sårbarheter som kontinuerlig oppdages i programvare. Revisjonen viser:

- Det er utarbeidet rutiner for oppdatering av operativsystem og programvare fra Microsoft, men ikke for sikkerhetsoppdatering av database og tredjeparts programvare.
- Verktøy for sikkerhetsoppdatering og oppfølging av tredjeparts programvare ikke har vært tilgjengelig i revisjonsperioden.
- Sikkerhetsoppdateringer er i varierende grad installert.

Bufetat opplyser at det benyttes to system for oppdatering og oppfølging av operativsystem og programvare. På grunn av overføring til en ny versjon av det ene systemet, har dette ikke vært tilgjengelig i perioden for revisjonen. Bufetat har ingen alternativer for oppfølging av tredjeparts programvare. Enheter med programvare som ikke er tilstrekkelig sikkerhetsoppdatert, er sårbare for kompromittering.

6.2.4 Kontroll med programvare og enheter i nettverket

Personopplysningsforskriften § 2-14 krever at sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet.

Programvare

ISO 27002 punkt 12.6.2 anbefaler at det etableres og håndheves strenge regler for hvilken programvare sluttbrukere kan installere på virksomhetens enheter i nettverket. NSM anbefaler at bare

[45] NSMs grunnprinsipper for IKT-sikkerhet, versjon 1.0, punkt 3.2
[46] Nasjonal sikkerhetsmyndighet: *Fire effektive tiltak mot dataangrep* (Sjekkliste nr. 1)
[47] The Center for Internet Security (CIS): *Critical Security Controls (CSC) for effective cyber defense*, punkt 4.

godkjent programvare kjøres på virksomhetens enheter, og at det bare installeres programvare som har nødvendig funksjonalitet for å understøtte virksomhetens forretningsprosesser.[48] NSMs anbefalinger samsvarer med standarden fra Center for Internet Security.[49] Bakgrunnen for anbefalingene er at dataangrep ofte innebærer installasjon av ondsinnet programvare.

Revisjonen viser:

- Fylkesnemndene har ikke utarbeidet policy, retningslinjer eller skriftlige rutiner for styring av programvare i nettverket, jf. punkt 6.1.5.
- Fylkesnemndene har delvis iverksatt tiltak for å begrense installering og kjøring av programvare som ikke er autorisert.
- Det ser ut til å være installert lite programvare på PC-er og servere.
- Det er ikke etablert etterkontroller for å verifisere at tiltakene som er iverksatt, fungerer etter hensikten.

Uttrekk fra tre PC-er viser at det i hovedsak er installert standard programvare, og det ser ut til å være installert begrenset med programvare på fylkesnemndenes servere.

Enheter i nettverket

ISO 27002 punkt 13.1.1 anbefaler at det implementeres prosedyrer for styring av nettverksutstyr, og at tilkobling til nettverket bør begrenses. CIS' *Critical Security Controls 1 – Inventory of Authorized and Unauthorized Devices* anbefaler at det etableres en oversikt over autorisert utstyr, at bare autorisert utstyr får tilgang til virksomhetens nettverk, og at uautorisert utstyr blir oppdaget og hindret tilgang.

Revisjonen viser:

- Fylkesnemndene har ikke utarbeidet policy, retningslinjer eller skriftlige rutiner for styring av enheter i nettverket, jf. punkt 6.1.5.
- Det er etablert tiltak for å begrense muligheten for bruk av uautoriserte enheter i fylkesnemndenes nettverk.
- Det ikke er etablert etterkontroller for å verifisere at tiltakene begrenser hvilke enheter som kan logge seg på nettverket.

Det er bare enheter registrert i fylkesnemndenes AD som vil bli godkjent i nettverket. Videre må brukerne ha gyldig brukernavn og passord for å kunne kommunisere med systemene. For besøkende og andre eksterne er det satt opp et trådløst gjestenett som bare gir tilgang til internett.

PC-er som ikke er i bruk, skal i henhold til rutiner bli deaktivert. En analyse av uttrekk fra fylkesnemndenes AD viser at PC-er ikke blir deaktivert i henhold til rutinene og derfor feilaktig vil bli oppfattet som gyldige enheter i nettverket.

[48] NSMs grunnprinsipper for IKT-sikkerhet, versjon 1.0, punkt 2.3.
[49] The Center for Internet Security (CIS): *Critical Security Controls (CSC) for effective cyber defense*, punkt 2.

6.3 Problemstilling 3 – evaluering og oppfølging

6.3.1 Hendelses- og avvikshåndtering / informasjonssikkerhetshendelser

Ifølge eForvaltningsforskriften § 15 (4) bokstav g skal sikkerhetsstrategien og internkontrollen også stille nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

ISO 27002 punkt 16.1 anbefaler å etablere prosesser for å sikre rapportering, behandling, reaksjon på og læring av informasjonssikkerhetshendelser. ISO 27002 punkt 16.1.6 anbefaler at erfaringer fra informasjonssikkerhetshendelser bør brukes for å redusere sannsynligheten for eller konsekvensen av framtidige hendelser.

Etter personopplysningsforskriften § 2-6 skal bruk av det enkelte informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd behandles som avvik. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.

Revisjonen viser:

- Det er ikke et enhetlig system for rapportering, håndtering og analyse av hendelser og avvik.
    - Fylkesnemndene har etablert prosedyrer for avviksbehandling ved Sentralenheten og i nemndene. Prosedyrene gjelder primært håndtering av fysiske dokumenter med taushetsbelagt informasjon.
    - Prosedyrer for håndtering av avvik hos tjenesteleverandøren Bufetat har primært vært rettet mot avvik i tilgjengelighet og responstid. Avvik i den tekniske informasjonssikkerheten skal varsles, men det er ikke prosedyrer for systematisk dokumentasjon av dette.
- Avvikshåndteringssystemet til fylkesnemndene har ikke fungert godt nok. Fylkesnemndene har satt i gang et forbedringsarbeid på området. Jf. også manglende overordnede prinsipper for hendelseshåndtering som er beskrevet i punkt 6.1.1.

Avvikshåndtering i Sentralenheten

Dokumentet *Retningslinjer for informasjonssikkerhet ved Sentralenheten for Fylkesnemndene for barnevern og sosiale saker*[50] gir prosedyrer for arbeidet med informasjonssikkerhetsbrudd i Sentralenheten. I henhold til dokumentet er et avvik definert som en uønsket hendelse og

> «oppstår når det ikke er samsvar mellom den praksisen som blir utøvd, og det som følger av lover, forskrifter, regelverk eller av interne prosedyrer. Uønskede hendelser kan også omfatte feil som følge av svakhet i teknologi som medfører at teknologien ikke fungerer som forutsatt.»

Retningslinjer for håndtering av informasjonssikkerhetsbrudd i Sentralenheten viser at den omfatter ansvarsroller for oppfølging av hendelser og prosesser for å innrapportere, analysere og håndtere informasjonssikkerhetshendelser. Alle ansatte i Sentralenheten er ansvarlige for å registrere avvik som definert i prosedyren. Den som melder avviket, skal manuelt fylle ut Sentralenhetens standardmal for avviksmelding.[51] Når malen er fylt ut, skal stabssjefen varsles snarest mulig om meldingen. Stabssjefen har ansvar for å håndtere avviket i henhold til prosedyren, inkludert rapportere tilbake til melderen om status og påse at avviket blir lukket etter håndtering. Stabssjefen har også ansvaret for å sammenstille, analysere og rapportere avvik til Sentralenhetens direktør.

[50] Dokument datert 24. mai 2017.
[51] *Mal – registrering og håndtering av avvik*. Malen er ikke godkjent.

Avvikshåndtering i nemndene
Alle nemndene har beskrevet prosedyrer for håndtering av uønskede hendelser i sine beredskapsplaner. Avvik skal rapporteres i et eget skjema til den daglige lederen i nemnda. Ved alvorlige avvik skal daglig leder rapportere videre til Sentralenheten. Skjemaet er et Excel-dokument for «Logging av hendelser innen sikkerhet og beredskap». Det framgår:

> «Dette skjemaet er utarbeidet for å lage en systematisk oversikt over hendelser som oppstår. Med hendelser menes f.eks. saker med tilstedeværelse av politi, trusselsituasjoner og liknende. Hendelsene skal logges fortløpende. Ved behov for lengre beskrivelser kan referatet lagres i P360. Ved alvorlige hendelser skal direktøren og Sentralenheten varsles.»

Skjemaet viser felter for nemnd, dato, saksnummer i ProSak, en kort beskrivelse av hendelsen, saksnummer i P360 (ved behov) og eventuelle tiltak. Sentralenheten opplyser at praksisen for avvikshåndtering i de ulike nemndene varierer, og at rapporteringen ikke har fungert etter hensikten.

Sentralenheten opplyser at avvikssystemet i Sentralenheten og i nemndene primært er rettet mot håndtering av fysiske dokumenter med taushetsbelagt informasjon (fysisk sikkerhet), men at det også gjelder informasjonssikkerhet generelt.[52]

Avvikshåndtering i Bufetat
Ifølge databehandleravtalen skal fylkesnemndene varsles ved avvik i den tekniske informasjonssikkerheten. Sentralenheten opplyser at det ikke er en formalisert og systematisk rapportering fra Bufetat for oppfølging av informasjonssikkerhet. Fylkesnemndene får rapportering om feilmeldinger, men ingen rutinemessig melding ved sikkerhetsbrudd. Bufetat opplyser at de ikke har hatt avvik i den tekniske informasjonssikkerheten i 2017, og det er dermed ikke rapportert avvik.

Tjenesteavtalen mellom Bufetat og fylkesnemndene har bestemmelser om avvikshåndtering og systematisk oppfølging av avvik som gjelder tilgjengelighet og responstid.

Sentralenheten erkjenner at systemet for håndtering av avvik i fylkesnemndene ikke er godt nok. Det er satt i gang et arbeid for å forbedre prosedyren og sikre at terskelen for å melde avvik blir lavere, men arbeidet med et nytt avvikshåndteringssystem ligger på is inntil nytt styringssystem hos fylkesnemndene er på plass.

6.3.2 Sikkerhetsrevisjoner av organisering og sikkerhetstiltak

I tillegg til krav om internkontroll etter eForvaltningsforskriften § 15 (2) skal sikkerhetsstrategien og internkontrollen etter § 15 (4) bokstav g også stille nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

ISO 27001 punkt 9.2 angir at det skal gjennomføres interne revisjoner med planlagte intervaller for å kontrollere om styringssystemet oppfyller interne krav, og at det implementeres og vedlikeholdes på en hensiktsmessig måte. Etter personopplysningsforskriften § 2-5 skal det jevnlig gjennomføres sikkerhetsrevisjoner av bruken av informasjonssystemet. Personopplysningsforskriften § 2-5 (2) fastsetter at en sikkerhetsrevisjon skal omfatte en vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartnere og leverandører. Videre sier (4) at resultatet fra en sikkerhetsrevisjon skal dokumenteres.

[52] Verifisert referat fra møte mellom fylkesnemndene og Riksrevisjonen den 22. september 2017 og revisjonsbesøk 14.-15. november 2017. Skjemaet er fra 2017. Referatene gjelder også avsnittene under «avvikshåndtering i Bufetat».

Revisjonen viser at fylkesnemndene ikke har gjennomført jevnlige sikkerhetsrevisjoner av organiseringen, sikkerhetstiltakene og bruken av leverandører:

- Det er utført revisjoner i form av ROS-analyser med hovedvekt på fysisk sikkerhet og risikovurdering av ProSak som kan gi grunnlag for å vurdere tiltak, men disse er ikke knyttet opp mot interne krav i et overordnet styringssystem, jf. punkt 6.1.1 og 6.1.3.
- Sikkerhetsrevisjoner eller annen oppfølging av sikkerhetstiltak er ikke regulert i databehandleravtalen med Bufetat, jf. punkt 6.1.4, og det er ingen systematisk oppfølging av avvik i den tekniske informasjonssikkerheten hos Bufetat, jf. punkt 6.2 og 6.3.1.

Utover det som er nevnt over, er det ikke dokumentert rutiner eller gjennomført andre evalueringer eller internrevisjoner. Revisjonen mangler dermed grunnlag for å vurdere om styringssystemet er i samsvar med interne krav, og om organiseringen, sikkerhetstiltakene og bruken av leverandører er implementert og vedlikeholdt på en hensiktsmessig måte.

6.3.3 Oppfølging av databehandleravtalen med Bufetat

ISO 27002 punkt 15.2.1 anbefaler at organisasjoner regelmessig bør overvåke, gjennomgå og revidere leverandørers tjenesteleveranser. Overvåking og gjennomgang av leverandørers tjenester bør sikre at betingelsene og vilkårene for informasjonssikkerhet i avtalene overholdes, og at informasjonssikkerhetsbrudd og -problemer håndteres på riktig måte.

Revisjonen viser:

- Fylkesnemndene har fulgt opp tjenesteavtalen og databehandleravtalen med Bufetat primært når det gjelder tilgjengelighet og funksjonalitet i ProSak.
- Det er ikke etablert en formalisert og systematisk rapportering fra Bufetat om oppfølgingen av den tekniske informasjonssikkerheten.

Formålet med tjenesteavtalen er blant annet å «regulere ansvar og samarbeid mellom BSA og fylkesnemndene med hensyn til daglig drift, endringer, testing, vedlikehold, oppgraderinger mv.» Tjenesteavtalens bilag 1 har en oversikt over fylkesnemndenes krav til tjenester. Avtalen følges opp gjennom et årlig statusmøte hvor det rapporteres om:

- tilgjengelighet/respons
- feilmeldinger
- tidsbruk
- henvendelser

Det foreligger referat fra statusmøtene for 2014–2016,[53] og fylkesnemndene opplyser at statusmøtet for 2017 vil bli avholdt i uke 47. Fylkesnemndene ved Sentralenheten har ansvaret for å kalle inn til og skrive referat fra møtene. Rapportering om henvendelser[54] vurderes av Sentralenheten og følges opp hvis henvendelsene er av en slik art at de må følges opp. I tillegg skal Bufetat rapportere om avvik og henvendelser dersom fylkesnemndene ber om det. Med «avvik» menes her avvik i tilgjengelighet i henhold til bilag 1 til tjenesteavtalen. Det har ikke vært avvik av en slik karakter at fylkesnemndene har sett behov for å be om avviksrapportering utover rapporteringen i statusmøtet.

Bufetat har satt som krav at alle ansatte i fylkesnemndene setter seg inn i hvordan utstyr og programvare skal benyttes, og at de følger *Regler for bruk av ikt-utstyr i fylkesnemndene*. I referat fra statusmøte for 2016 står det at reglene er utdaterte, og at Bufetat skal oppdatere dem. De er ikke oppdatert per november 2017.

[53] Referat fra statusmøter 17. oktober 2014, 15. oktober 2015 og 1. desember 2016.
[54] *Rapport henvendelser FBS 2016*.

I tillegg til det årlige statusmøtet avholdes det arbeidsmøter ved behov. I 2017 er det gjennomført flere arbeids-/prosjektmøter der temaet blant annet har vært funksjonaliteten i ProSak.

Fylkesnemndene skal etter databehandleravtalen varsles ved avvik i den tekniske informasjonssikkerheten, jf. punkt 6.3.1 over om hendelses- og avvikshåndtering. Bufetat opplyser at de ikke har hatt avvik i den tekniske informasjonssikkerheten i 2017, og det er dermed ikke rapportert avvik. Videre framgår det at det ikke er etablert en formalisert og systematisk rapportering fra Bufetat når det gjelder oppfølging av informasjonssikkerhet.[55]

6.3.4 Gjennomgang av styringssystemet

Etter eForvaltningsforskriften § 15 (2) skal forvaltningsorganet ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystemer for informasjonssikkerhet. Ifølge ISO 27001 punkt 9.1 skal virksomheten evaluere prestasjonen til og virkningen av styringssystemet for informasjonssikkerhet. Ledelsen skal etter punkt 9.3 gjennomgå styringssystemet for informasjonssikkerhet jevnlig for å sikre at det fortløpende er velegnet, tilstrekkelig og virkningsfullt. Videre angis i kapittel 10 at virksomheten skal reagere på eventuelle avvik og innføre korrigerende tiltak. Virksomheten skal kontinuerlig forbedre egnetheten, tjenligheten og virkningen til styringssystemet for informasjonssikkerhet.

Revisjonen viser:

- Fylkesnemndene får ikke på en formalisert og systematisk måte rapportering om informasjonssikkerhet fra tjenesteleverandøren Bufetat.
- Fylkesnemndene foretar enkelte risikovurderinger og ROS-analyser som grunnlag for å kunne vurdere tiltak for informasjonssikkerhet.
- Det ikke er dokumentert at arbeidet med informasjonssikkerhet evalueres og følges opp systematisk. Fylkesnemndene har startet arbeidet med å utvikle et helhetlig styringssystem for informasjonssikkerhet.

ROS-analysene som ble gjennomført i 2015, var de første systematiske analysene av sikkerhet og beredskap i virksomheten, jf. omtale i punkt 6.1.1. I etterkant av en fagdag om sikkerhet og beredskap i 2016 ble det utarbeidet en mal for tiltakskort med instruksjoner for håndtering av ulike uønskede situasjoner som kan oppstå hos nemndene. ROS-analysene omhandler som nevnt i punkt 6.1.2 identifisering og klassifisering av informasjonsaktiva og punkt 6.1.3 om risikostyring, primært fysisk sikring av informasjon. Det er opplyst at det skal gjennomføres nye ROS-analyser med frist i september 2017. I tillegg er det i 2017 gjennomført en risikovurdering av informasjonssikkerheten i Sentralenheten som er avgrenset til fysisk sikring av taushetsbelagt informasjon i dokumenter og på PC-er.[56]

Det ble i 2015 også gjennomført en egen risikovurdering som del av utviklingen av ProSak. Tiltakene fra denne risikovurderingen er ivaretatt i utviklingen av ProSak, men det foreligger ingen oversikt over tiltakene eller hvordan disse er iverksatt. Planen var at en ny sikkerhetsrevisjon etter innføringen av Saksportalen ville vise iverksettingen av tiltakene fra 2015-rapporten. Denne sikkerhetsrevisjonen er utsatt ettersom innføringen av Saksportalen er utsatt.[57]

Fylkesnemndene har også vurdert betydningen av endringer som følge av den nye personvernforordningen i EU som trer i kraft 25. mai 2018.[58] Vurderingen anbefalte en grundigere

[55] Verifisert referat fra møte mellom fylkesnemndene og Riksrevisjonen den 22. september 2017 og revisjonsbesøk 14.-15. november 2017, tjenesteavtalen og bilag 4 til tjenesteavtalen.
[56] *Risikovurdering Informasjonssikkerhet,* udatert men henviser til krav i tildelingsbrev fra BLD for 2017.
[57] Verifisert referat fra møte mellom fylkesnemndene og Riksrevisjonen den 22. september 2017.
[58] *Personvernforordningen* - internt notat fylkesnemndene, datert 18. april 2017.

juridisk gjennomgang av forordningen og hvilke konsekvenser de nye reglene medfører for fylkesnemndene. Dessuten har fylkesnemndene for 2017, etter tildelingsbrev fra departementet, laget en tiltaksplan for tiltaksområde 5 fra *Handlingsplan for informasjonssikkerhet i statsforvaltningen*, «Kunnskap, kompetanse og kultur».[59]

Som omtalt i punkt 6.1.3 om risikostyring er det ikke gjennomført risikovurdering rettet mot fylkesnemndenes IKT-infrastruktur, som er en tjeneste som er satt ut til Bufetat. I punkt 6.3.3 om oppfølging av databehandleravtalen med Bufetat omtales at det heller ikke er etablert en formalisert og systematisk rapportering fra Bufetat når det gjelder oppfølging av den tekniske informasjonssikkerheten.

Utover de nevnte ROS-analysene og risikovurderingene er det ikke dokumentert at det er etablert rutiner for eller gjennomført evalueringer, internrevisjoner, ledelsesgjennomgang eller oppdatering og forbedring av et styringssystem for informasjonssikkerhet.

Sentralenheten opplyser at fylkesnemndene ikke har hatt noen systematisk evaluering av styringssystemet for informasjonssikkerhet, men har et mål om å få dette på plass så snart det lar seg gjøre. Behovet for å få på plass nødvendige dokumenter og systemer er identifisert.[60]

7 Konklusjoner

Fylkesnemndene har først og fremst som oppgave å fatte vedtak etter barnevernloven, blant annet i saker om omsorgsovertakelse av barn og tiltak for barn med atferdsvansker. For å gjennomføre oppgavene sine har fylkesnemndene behov for å forvalte personopplysninger om barn, blant annet ved saksbehandling og lagring av informasjon, i forhandlings- og vedtaksmøter, ved frakt av dokumenter utenfor nemndenes lokaler og ved kommunikasjon med eksterne. Det at det foreligger en barnevernssak, medfører utvidet taushetsplikt og gjør at det er behov for beskyttelse. Sikker håndtering av opplysninger om barnet er avgjørende (konfidensialitet). For at tiltakene som settes inn, skal ha høy og riktig kvalitet, er det også avgjørende at opplysningene som blir lagt til grunn i sakene, er pålitelig (integritet).

Offentlige virksomheter har ansvar for å beskytte den informasjonen de forvalter. Etter hvert som offentlig forvaltning blir mer og mer digitalisert, blir det stadig viktigere og mer nødvendig med gode styringssystemer for informasjonssikkerhet og beskyttelse av sensitiv informasjon. Etableringen av et styringssystem for informasjonssikkerhet skal hjelpe ledelsen og virksomheten for øvrig til å ha tilstrekkelig styring på og kontroll med informasjonssikkerheten, gjennom systematisk internkontroll på området. Det skal medvirke til at virksomheten velger riktige sikkerhetstiltak, og sørge for at de valgte løsningene blir evaluert og forbedret om nødvendig.

Målet med revisjonen er å kontrollere om fylkesnemndene har et styringssystem for informasjonssikkerhet som oppfyller kravene i eForvaltningsforskriften og som ivaretar krav i personopplysningsloven.

Fylkesnemndene har ikke et styringssystem for informasjonssikkerhet som samsvarer med eForvaltningsforskriften § 15 og anerkjente standarder, og som i tilstrekkelig grad oppfyller kravene i personopplysningsloven. Fylkesnemndene har blant annet ikke et overordnet styringsdokument med sikkerhetsmål og -strategi som sikrer ledelsen et grunnlag for å planlegge sikkerhetstiltak. Manglende

[59] *Informasjonssikkerhet - Tiltaksliste 2017*, sist oppdatert 27. april 2017.
[60] Verifisert referat fra møte mellom fylkesnemndene og Riksrevisjonen den 22. september 2017, og *Rapport om mangler innen informasjonssikkerhet* - internt notat fylkesnemndene, datert 13. november 2017.

styring og ledelsesinvolvering kan føre til at virksomheten ikke gjennomfører nødvendige analyser av sikringsbehov før tiltakene iverksettes.

Styringssystemet og internkontrollen skal også bidra til at det blir stilt nødvendige krav til prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon. Svakheter i gjennomføring av sikkerhetstiltak indikerer at det ikke er etablert et godt nok grunnlag for å vurdere omfang og innretning på internkontrollen, enten ved at tiltak ikke er iverksatt eller at svakhetene i etablerte tiltak ikke er identifisert. Manglende sikkerhetstiltak kan føre til uheldige konsekvenser for enkeltpersoner og samfunnet. Det kan også skade omdømmet til offentlige virksomheter.

Fylkesnemndene er en relativt liten virksomhet og har, med bakgrunn i en tjenesteavtale og vedlikeholdsavtale, satt driften av IKT-infrastrukturen sin og applikasjonen ProSak ut til Bufetat. Ved tjenesteutsetting skal en skriftlig avtale med tjenesteleverandøren legge grunnlaget for at personopplysninger behandles med tilfredsstillende informasjonssikkerhet. For elektronisk informasjonsforvaltning bygger fylkesnemndene på at Bufetat ivaretar informasjonssikkerhet gjennom å benytte sitt styringssystem, uten at dette er fulgt opp eller evaluert. Databehandleravtalen med Bufetat stiller ikke krav om hvilke sikringstiltak databehandleren skal etablere for behandling av personopplysninger, eller krav om oppfølging av sikkerhetstiltak.

Det kan være utfordrende for fylkesnemndene å vurdere hvordan styringssystemet skal utformes slik at det er tilpasset virksomhetens egenart og samtidig tilfredsstiller regelverket. Fylkesnemndene har startet arbeidet med å utvikle et helhetlig styringssystem for informasjonssikkerhet.

Revisjonens konklusjoner er basert på personopplysningsloven og -forskriften som var gjeldende for 2017. Den nye personopplysningsloven med bakgrunn i EU-forordning 2016/679 (personvernforordningen/GDPR) som trer i kraft 25. mai 2018, viderefører dette regelverket. Det nye regelverket inneholder flere detaljreguleringer og tilstramminger, i tillegg til noen nye prinsipper. Blant annet stilles det strengere krav til databehandlere og nye krav til avvikshåndtering.[61] Funnene i revisjonen vil derfor være relevante også etter at den nye personopplysningsloven begynner å gjelde.

7.1 Problemstilling 1 – planlegging av sikkerhetstiltak

Revisjonen har undersøkt om internkontrollen ivaretar og stiller nødvendige krav til prosedyrer for fylkesnemndenes sikring av personopplysninger som gjelder barnevernssaker. Revisjonens konklusjon er at fylkesnemndene i stor grad har etablert et grunnlag for å planlegge og gjennomføre sikkerhetstiltak når det gjelder fysisk sikring av informasjon hos Sentralenheten og i nemndene, men at dette grunnlaget i stor grad mangler for IKT-tekniske sikkerhetstiltak, som er tjenesteutsatt til Bufetat. Konklusjonen er basert på følgende:

- Fylkesnemndene har ikke et overordnet styringsdokument for informasjonssikkerhet i samsvar med de kravene eForvaltningsforskriften § 15 stiller til en sikkerhetsstrategi (sikkerhetspolicy) med sikkerhetsmål. Når det gjelder informasjonssikkerhet i elektroniske systemer, har fylkesnemndene basert seg på at dette ivaretas i Bufetats styringssystem for informasjonssikkerhet.

- Fylkesnemndene har ikke dokumentert en helhetlig oversikt over informasjonsaktiva/-verdier eller klassifisering av slike, slik det stilles krav om i personopplysningsforskriften § 2-4, jf. eForvaltningsforskriften § 15 (4), men har identifisert at de har skjermingsverdige personopplysninger i saks- og ansettelsesforhold.

[61] Jf. Datatilsynets veiledning og punktliste *Nye personvernregler fra 2018. Hva betyr det for din virksomhet?*

- Fylkesnemndene har ikke etablert en helhetlig prosess for risikovurdering av informasjonssikkerhet som anbefalt i ISO 27001 punkt 6.1.2 som kan gi grunnlag for å vurdere om internkontrollens omfang og innretning er tilpasset risiko i tråd med eForvaltningsforskriften § 15 (3). Det er gjennomført ROS-analyser i de enkelte nemndene og Sentralenheten med hovedvekt på fysisk sikkerhet. I tillegg er det gjennomført risikovurdering ved utvikling av saksbehandlingssystemet ProSak, men det er ikke gjennomført noen risikovurdering rettet mot fylkesnemndenes IKT-infrastruktur, som er tjenesteutsatt til Bufetat.

- Fylkesnemndene har en databehandleravtale med Bufetat som inneholder flere av elementene som Datatilsynet anbefaler, men stiller ikke krav til hva databehandleren skal ha på plass av sikringstiltak for behandling av personopplysninger eller krav om oppfølging av sikkerhetstiltak. Manglende krav om sikringstiltak og oppfølging av disse gjør at fylkesnemndene som behandlingsansvarlig ikke sikrer at Bufetat som databehandler gjennomfører sikringstiltak etter personopplysningsloven § 13, jf. § 15, og ivaretar således heller ikke kravene i eForvaltningsforskriften § 15 (4) bokstav g.

- Fylkesnemndene har delvis utarbeidet temaspesifikke policyer og retningslinjer for informasjonssikkerhet etter kravene i eForvaltningsforskriften § 15, jf. ISO 27002 punkt 5.1.1, som skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. For sikkerhetstiltak som gjennomføres hos Bufetat, har fylkesnemndene i liten grad stilt krav til policyer, retningslinjer og rutiner. Gjennom avtalene med Bufetat er det også lite dokumentert hvordan prosessene og kommunikasjonen om sikkerhetstiltak skal foregå. Fylkesnemndene har basert seg på Bufetats styringssystem, uten at dette er tilpasset, fulgt opp eller evaluert.

7.2 Problemstilling 2 – gjennomføring av sikkerhetstiltak

Revisjonen har omfattet et utvalg sikkerhetstiltak i elektroniske systemer for å gi en indikasjon på om styringssystemet bidrar til at internkontrollen ivaretar og stiller nødvendige krav til prosedyrer for fylkesnemndenes sikring av personopplysninger og for oppfølging av at iverksatte sikkerhetstiltak fungerer etter hensikten. Sikkerhetstiltakene er valgt ut på bakgrunn av hva anerkjente aktører innenfor informasjonssikkerhet anser som viktigst for å redusere risiko. Svakheter i gjennomføring av utvalgte sikkerhetstiltak kan indikere at det ikke er etablert et godt nok grunnlag for å vurdere omfang og innretning på internkontrollen, enten ved at tiltak ikke er iverksatt eller at svakhetene i etablerte tiltak ikke er identifisert og korrigerende tiltak iverksatt. Revisjonens konklusjon er at fylkesnemndene ikke godt nok har gjennomført systematiske sikkerhetstiltak for å bidra til å sikre tilfredsstillende informasjonssikkerhet. Konklusjonen er basert på følgende:

- Fylkesnemndene etterlever ikke kravene i personopplysningsforskriften § 2-8 om at bruk av informasjonssystemet skal være autorisert og etter tjenstlig behov. Særlig gjelder dette for brukere med administratorrettigheter.

- Fylkesnemndene etterlever ikke personopplysningsforskriften §§ 2-8 (3) og 2-14, som stiller krav om at autorisert bruk av informasjonssystemet skal registreres, og at sikkerhetstiltak skal gjøre det mulig å oppdage forsøk på uautorisert bruk. Det mangler tilstrekkelig logging i databasen for ProSak, og gjennomgangen av logger er ikke systematisert for å oppdage eventuell uautorisert bruk av systemer.

- Fylkesnemndene etterlever ikke fullt ut kravene som stilles i personopplysningsforskriften § 2-13 om tiltak mot ødeleggende programvare, ettersom aktuelle sikkerhetsoppdateringer ikke er installert i tråd med anbefalinger.

- Fylkesnemndene etterlever ikke fullt ut kravene i personopplysningsforskriften § 2-14 om sikkerhetstiltak som skal hindre uautorisert bruk av informasjonssystemet. Tiltak for å hindre installering og kjøring av uautorisert programvare og kontroll med enheter i nettverket gjennomføres delvis som anbefalt.

7.3 Problemstilling 3 – evaluering og oppfølging

Revisjonen har undersøkt om de valgte løsningene blir evaluert og forbedret dersom det er nødvendig, og hvordan fylkesnemndene følger opp at sikkerhetstiltak som er besluttet, faktisk er iverksatt og fungerer etter hensikten. Dette inkluderer også oppfølging av avtalte sikkerhetstiltak hos tjenesteleverandøren. Revisjonens konklusjon er at fylkesnemndene ikke godt nok følger opp at sikkerhetsstrategi og -tiltak gir tilfredsstillende informasjonssikkerhet. Konklusjonen er basert på følgende:

- Fylkesnemndenes avvikshåndteringssystem har ikke fungert godt nok, og det er ikke et enhetlig system for rapportering, håndtering og analyse av hendelser og avvik, slik det stilles krav om i personopplysningsforskriften § 2-6, jf. eForvaltningsforskriften § 15 (4) bokstav g. Det er etablert prosedyrer for avviksbehandling ved Sentralenheten og i nemndene. Prosedyrene gjelder primært håndtering av fysiske dokumenter med taushetsbelagt informasjon. Prosedyrer for håndtering av avvik hos tjenesteleverandøren Bufetat har primært vært rettet mot avvik i tilgjengelighet og responstid. Avvik i den tekniske informasjonssikkerheten skal varsles, men det er ikke prosedyrer for systematisk dokumentasjon av dette.

- Fylkesnemndene har i liten grad gjennomført jevnlige sikkerhetsrevisjoner av organisering, sikkerhetstiltak og bruk av leverandør, slik det stilles krav om i personopplysningsforskriften § 2-5, jf. eForvaltningsforskriften § 15 (4) bokstav g.

- Fylkesnemndene gjennomfører ikke overvåkning og gjennomgang av Bufetats tjenester helt etter anbefalingene for å sikre at betingelsene og vilkårene for informasjonssikkerhet i avtalene overholdes, og at informasjonssikkerhetsbrudd og -problemer kan håndteres på riktig måte, jf. eForvaltningsforskriften § 15 (2). Fylkesnemndene har gjennomført oppfølging av tjenesteavtalen og databehandleravtalen med Bufetat primært når det gjelder tilgjengelighet og funksjonalitet i ProSak. Det er ikke etablert en formalisert og systematisk rapportering fra Bufetat om oppfølgingen av den tekniske informasjonssikkerheten.

- Fylkesnemndene har ikke dokumentert en systematisk evaluering og oppfølging av et styringssystem for informasjonssikkerhet slik det er anbefalt, og etterlever ikke kravene til internkontroll i eForvaltningsforskriften § 15 (2). Det er foretatt enkelte risikovurderinger og ROS-analyser for å kunne vurdere tiltak for informasjonssikkerhet i Sentralenheten og nemndene, men fylkesnemndene får ikke en formalisert og systematisk rapportering fra Bufetat om informasjonssikkerhet.