ROMERIKE REVISJON IKS

FOTO: ELISABETH BJØRN

FORVALTNINGSREVISJONSRAPPORT

INFORMASJONSSIKKERHET
PERSONOPPLYSNINGER I BARNEVERN OG SKOLE

LØRENSKOG KOMMUNE

JUNI 2016

INNHOLD

SAMMENDRAG I
Formål og problemstillinger i
Revisjonens oppsummering av funn i
Revisjonens samlede vurdering og konklusjon iii
Rådmannens uttalelse til rapporten iii
Anbefalinger iii
1 Innledning 1
1.1 Bakgrunn og formål 1
1.2 Problemstilling og avgrensning 1
1.3 Revisjonskriterier 2
1.4 Gjennomføring 2
1.5 Oppbygging av rapporten 2
2 Anvendte metoder i prosjektet 3
2.1 Revisjon av informasjonssikkerhet 3
2.2 Datainnsamling og datagrunnlag 3
2.3 Dataenes pålitelighet og gyldighet 4
3 Revisjonskriterier 5
3.1 Personvern 5
3.2 Internkontroll 9
3.3 Utledning av revisjonskriterier 10
4 Organisering og kommunens overordnede ansvar 11
4.1 Innledning 11
4.2 Organiseringen i Lørenskog kommune 11
4.3 Rollen som personvernombud 12
4.4 Teknologiavdelingen 13
4.5 Overordnet ansvar for personopplysninger og informasjonssikkerhet 14
4.6 Kommunens arbeid med internkontroll og informasjonssikkerhet 15
4.6.1 Tilbakeblikk 15
4.6.2 Pågående prosjekter innen IKT og internkontroll i Lørenskog 15
5 Informasjonssikkerhet - barnevernet 17
5.1 Revisjonskriterier 17

5.2 Introduksjon 17
5.3 Organisering av sikkerhetsarbeidet 19
5.3.1 Beskrivelse av sikkerhetsarbeidet 20
5.3.2 Fordeling av roller og ansvar 20
5.3.3 Rutiner for av sikkerhetsarbeidet 20
5.4 Risikovurdering 22
5.5 Tilgangskontroll 23
5.5.1 Etablerte rutiner og praksis for tilfredsstillende tilgangskontroll 23
5.5.2 Revisjonens test av tilganger 25
5.5.3 Holdninger 26
5.5.4 Tilganger i samsvar med tjenstlig behov 26
5.6 Råd og tips 27
6 Informasjonssikkerhet - grunnskolen 29
6.1 Revisjonskriterier 29
6.2 Introduksjon 29
6.3 Organisering av sikkerhetsarbeidet 31
6.3.1 Organiseringen av sikkerhetsarbeidet skal beskrives 31
6.3.2 Fordeling av roller og ansvar 32
6.3.3 Beskrivelse av sikkerhetsarbeidet, herunder roller og ansvar 33
6.4 Risikovurdering 36
6.5 Tilgangskontroll 37
6.5.1 Etablerte rutiner og praksis for tilfredsstillende tilgangskontroll 37
6.5.2 Holdningsskapende arbeid 37
6.5.3 Tilganger i samsvar med tjenstlig behov 38
6.6 Råd og tips 38
7 Vurderinger, konklusjon og anbefalinger 41
7.1 Revisjonens vurderinger 41
7.2 Samlet vurdering og konklusjon 43
7.3 Anbefalinger 43
LITTERATUR- OG KILDEHENVISNINGER 45
FIGURER OG TABELLER 46
VEDLEGG – RÅDMANNENS HØRINGSUTTALELSE 47

SAMMENDRAG

Formål og problemstillinger

Formålet med revisjonen har vært å bidra til økt fokus og regeletterlevelse innenfor personvern og informasjonssikkerhet i Lørenskog kommune. Undersøkelsen er avgrenset til personopplysninger og informasjonssikkerhet i barnevernet og to utvalgte skoler i kommunen.

Problemstillingen er formulert slik:

> **Ivaretar barnevernet og skolene i Lørenskog kommune informasjonssikkerheten når personopplysninger behandles?**

Undersøkelsen ser først og fremst på:

- Er det en klar fordeling mellom roller og ansvar i informasjonssikkerhetsarbeidet?
- Har virksomhetene oversikt over personopplysninger som behandles?
- I den grad det er gjennomført risikovurderinger, hvordan håndteres disse?
- I hvilken grad er det etablert rutiner og praksis for tilfredsstillende tilgangskontroll, og er tilgangene i samsvar med tjenstlig behov?

For å besvare denne problemstillingen har revisjonen gjennomgått tilgjengelig dokumentasjon og gjennomført intervjuer med sentrale medarbeidere på området. Nærmere om dette i kapittel 2.

Revisjonens oppsummering av funn

Undersøkelsen viser at det er behov for å etablere bedre styring og kontroll med området både på overordnet nivå i kommunen og på virksomhetsnivå, det vil si rutiner ved barnevernskontoret og skolene i henhold til personopplysningsloven. Nedenfor følger en oppsummering av revisjonskriteriene[1] og revisjonens funn. Se nærmere om dette i kapittel 5, 6 og 7.

Revisjonskriterium 1
➔ **Organisering av sikkerhetsarbeidet (personopplysningsforskriften § 2-7)** ○ Organiseringen av sikkerhetsarbeidet skal beskrives ○ Informasjonssikkerhetsarbeidet skal baseres på en klar fordeling av roller og ansvar ○ Fordelingen av roller og ansvar skal være dokumentert.

[1] Revisjonskriterier er de normer og krav som kan stilles til kommunens virksomhet på det området som er gjenstand for forvaltningsrevisjon. Se nærmere om dette i kapittel 3.

Undersøkelsen viser at Lørenskog kommune og de reviderte virksomhetene ikke har organisert sikkerhetsarbeidet på en tilfredsstillende måte. Det er ingen klar fordeling av roller og ansvar som er tilstrekkelig dokumentert. Revisjonen oppfatter at roller og ansvar er forstått av de ulike partene, men innholdet i rollene og ansvaret er ikke klart kommunisert, og fordelingen er ikke heller ikke dokumentert.

Revisjonskriterium 2

- ➔ **Risikovurdering (personopplysningsforskriften § 2-4)**
  - Det skal gjennomføres risikovurderinger med jevne mellomrom
  - Risikovurderingene skal dokumenteres
  - Resultatet av risikovurdering bør nedfelles i en aktivitetsplan eller lignende.
  - Det skal foreligge en oversikt over personopplysningene som behandles.

Lørenskog kommune og de reviderte virksomhetene har ikke etablert tilstrekkelige, ensartede rutiner for gjennomføring av risikovurderinger i henhold til personopplysningslovens bestemmelser. Risikovurderingene skal gjennomføres minimum årlig, være dokumentert og resultere i en aktivitetsplan eller tiltaksplan. I barnevernet utføres imidlertid risikovurderinger etter barnevernlovens krav.

Lørenskog kommune og de reviderte virksomhetene fører ikke en oversikt over hvilke personopplysninger som behandles, og hvor disse behandles. De enkelte ansvarlige har kunnskap om hvor det behandles personopplysninger innenfor sin virksomhet, men dette er ikke dokumentert. Dette gjelder spesielt kommunen som skoleeier og de utvalgte skolene, og i mindre grad i barnevernet som en følge av kravene i barnevernloven.

Revisjonskriterium 3

- ➔ **Tilgangskontroll (personopplysningsforskriften § 2-5 og § 2-8)**
  - Det skal være etablert rutiner og praksis for en tilfredsstillende tilgangskontroll i fagsystemet
  - Det skal gjennomføres holdningsskapende arbeid
  - Tilgang til informasjon i fagsystemet skal være i samsvar med tjenstlig behov

Det er etablert rutiner sentralt for å administrere brukere i kommunens IKT-systemer, herunder tildeling av rettigheter. Undersøkelsen viser imidlertid at administrering av brukere og rettigheter innenfor det enkelte fagsystem er fordelt til ulike systemansvarlige i kommunen, og rutinene varierer derfor fra system til system, og det kan være forskjeller mellom de ulike virksomhetene. Det er ikke tilfredsstillende rutiner for regelmessig gjennomgang av brukeres rettigheter i de enkelte fagsystemene.

Det er ikke etablert regelmessig gjennomgang av logger. Innføring av dette kan være med på å hindre og forebygge at brukere leser saker de ikke er involvert i («snoking»). Det gjør det også mulig å gjennomføre regelmessig gjennomgang av loggene for å se at alle endringer er berettiget.

Revisjonens samlede vurdering og konklusjon

Revisjonens samlede vurdering er at organisering av sikkerhetsarbeidet, risikovurderinger og tilgangskontroller knyttet til barnevern og skoler i Lørenskog kommune ikke er tilstrekkelig i henhold til de kravene som stilles i personopplysningsloven. Dette behøver ikke bety at personopplysninger behandles på en kritikkverdig måte, men det er behov for å styrke etterlevelsen i henhold til personopplysningslovens krav.

Revisjonen understreker at vi ikke har gjennomgått rutiner og praksis for hele kommunen, men gjort undersøkelser som har vært rettet mot barnevern og skole, både sentralt og ved utvalgte virksomheter. Revisjonens vurderinger og anbefalinger som knyttes til kommunens overordnede ansvar, vil imidlertid gjelde for Lørenskog kommune som skoleeier og for hele kommunen.

Revisjonen konkluderer på bakgrunn av den gjennomførte undersøkelsen slik på problemstillingen:

> *De undersøkte virksomhetene har i liten grad ivaretatt informasjonssikkerheten i tråd med kravene i personopplysningsloven.*

Rådmannens uttalelse til rapporten

Et utkast til rapport er forelagt rådmannen til uttalelse. Høringssvaret av 1.6.2016 er i sin helhet gjengitt i vedlegg til denne rapporten.

Rådmannen gir uttrykk for at rapporten anses som svært nyttig i arbeidet med å forbedre informasjonssikkerheten i Lørenskog kommune. Rådmannen mener rapporten gir en beskrivelse av informasjonssikkerheten som rådmannen kjenner seg igjen i. Han slutter seg til anbefalingene som revisjonen gir i rapporten, vil iverksette tiltak i tråd med oppfølgingspunktene og påregner at dette arbeidet vil vare ut 2017.

Anbefalinger

Revisjonen oppsummerer i alt 11 punkter som administrasjonen i kommunen bør følge opp. Disse punktene er deretter løftet opp og formulert som en anbefaling til kommunen. Det framkommer i rapportens punkt 4.6 at det pågår et omfattende prosjekt for *internkontroll* i Lørenskog kommune som blant annet vil omfatte etablering av policyer, retningslinjer og rutiner for informasjonssikkerhet og personvern. Flere av punktene nedenfor må derfor forventes fulgt opp gjennom dette arbeidet.

Oppfølgingspunkter

1. Utarbeide en overordnet beskrivelse av sikkerhetsarbeidet i Lørenskog kommune som definerer organiseringen og fordelingen av roller og ansvar i henhold til personopplysningslovens bestemmelser.
2. Beskrive innholdet i roller og ansvar for informasjonssikkerhet og personvern for de ulike behandlingsansvarlige på alle nivåer, eksempelvis direktører, barnevernsjef og rektorer ved skolene.
3. Utarbeide retningslinjer for gjennomføring av årlige risikovurderinger i virksomheter som behandler personopplysninger.
4. Utarbeide malverk for utførelse av risikovurderinger, og gjennomføre opplæring i virksomhetene om hvordan dette skal gjennomføres, dokumenteres og følges opp.
5. Etablere rutiner for å identifisere hvilke personopplysninger som behandles i kommunen og dens virksomheter. Oversikten må til enhver tid holdes oppdatert. Koordineringen av dette arbeidet bør skje sentralt i kommunen, mens virksomhetene bevisstgjøres på å melde fra om endringer når disse skjer.
6. Utarbeide sentrale veiledninger og informasjonsmateriale som virksomhetene kan benytte for å sette informasjonssikkerhet og personvern på dagsorden i sine virksomheter.
7. Etablere rutiner for regelmessig distribusjon og gjennomgang av oversikter over brukere og deres rettigheter i systemer hvor det behandles personopplysninger i de ulike virksomhetene. Gjennomgangen bør minimum gjennomføres en gang per år, helst oftere.
8. Revidere rollene/rettighetene for brukere av fagsystemet Familia innenfor barnevernet.
9. Innføre kryptering av data og trafikk innenfor sikker sone for fagsystemet Familia.
10. Gjennomgå tilgangsstrukturene for ulike brukergrupper i skolene for å definere hvilke rettigheter ansatte skal ha til de forskjellige systemene. Dette er spesielt viktig i forbindelse med utrullingen av *hypernet for Skole*.
11. Etablere skriftlige rutiner og systemer for dokumenthåndtering, herunder overføring av dokumenter mellom lærer-pc'er og det administrative nettet, slik at man kan unngå bruk av minnepinner og lagring på lærer-pc når det gjelder personopplysninger.

Revisjonens anbefaling sammenfatter revisjonsrapportens 11 oppfølgingspunkter og er:

Rådmannen må sørge for at kommunen etterlever lovens krav til informasjonssikkerhet ved behandling av personopplysninger, særlig gjelder dette å få på plass internkontroll i henhold til krav i forskriften til personopplysningsloven.

Jessheim, 3.6.2016

Nina Neset
daglig leder

Oddny Ruud Nordvik
avdelingsleder forvaltningsrevisjon
og selskapskontroll

1 INNLEDNING

1.1 Bakgrunn og formål

Med utgangspunkt i plan for forvaltningsrevisjon 2014-2016 og kontrollutvalgets vedtak[2] er det gjennomført en forvaltningsrevisjon av personvern og informasjonssikkerhet i Lørenskog kommune.

Prosjektets formål er å bidra til økt fokus og regeletterlevelse innenfor informasjonssikkerhet i Lørenskog kommune. Informasjonssikkerhet står sentralt når det gjelder å ivareta personvernet.

Informasjon som inneholder personopplysninger innhentes om og fra innbyggerne, og de må ha tillit til at kommunen behandler informasjonen den grad av sikkerhet som er påkrevd. Personopplysningene kan til dels være sensitive og lovgiver stiller krav om særlig beskyttelse i slike tilfeller. I en veileder om internkontroll og informasjonssikkerhet (Datatilsynet 2009) fremheves:

> Informasjonssikkerhet er ikke et mål i seg selv, men et middel for å oppnå tilfredsstillende kvalitet på virksomhetens tjenester. Tillit er en skjør egenskap som raskt kan bryte sammen. Bare hendelsen rammer noen kraftig nok skal det lite til for å svekke tilliten. Og problemet er at svekket tillit kan ramme hele sektoren og den kan være vanskelig å gjenopprette.
>
> Datatilsynet 2009

1.2 Problemstilling og avgrensning

Forvaltningsrevisjonen har følgende hovedproblemstilling:

> **Ivaretar barnevernet og skolene i Lørenskog kommune informasjonssikkerheten når personopplysninger behandles?**

Undersøkelsen ser først og fremst på:

- Er det en klar fordeling mellom roller og ansvar i informasjonssikkerhetsarbeidet?
- Har virksomhetene oversikt over personopplysninger som behandles?
- I den grad det er gjennomført risikovurderinger, hvordan håndteres disse?
- I hvilken grad er det etablert rutiner og praksis for tilfredsstillende tilgangskontroll, og er tilgangene i samsvar med tjenstlig behov?

Når det gjelder barnevern, har Lørenskog kommune både ansvar for barnevernet i kommunen og den interkommunale barnevernvakten[3]. Barnevernvakten omfattes ikke av undersøkelsen.

[2] Vedtak i møte 8.12.2015 sak 37/2015

[3] Barnevernvakten v/Romerike politidistrikt dekker 13 kommuner på Romerike og eies og drives av Lørenskog kommune etter vertskommuneprinsippet. Barnevernvakten er åpen på kveld og i helger.

Undersøkelsen tar videre for seg behandling av personopplysninger om elevene i skolen. Utgangspunktet var å undersøke dette i lys av utrullingen av fagsystemet *hypernet for Skole* i de kommunale skolene. Overgangen fra det gamle fagsystemet Sats til den nye web-baserte versjonen er imidlertid forsinket. Revisjonen har derfor undersøkt behandlingen av personopplysninger også i andre systemer og integrasjonen mellom systemer.

1.3 Revisjonskriterier

For å besvare problemstillingene formuleres det revisjonskriterier. Revisjonskriteriene er en samlebetegnelse på de krav, normer og standarder som benyttes som grunnlag for revisjonens vurderinger. Revisjonskriteriene skal være begrunnet i og utledet fra autoritative kilder innenfor det reviderte området.

Revisjonskriteriene i denne undersøkelsen er først og fremst utledet fra lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) og forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften).

1.4 Gjennomføring

Undersøkelsen er utført i perioden desember 2015 til mai 2016. Inger Berit Faller har vært prosjektleder og Lars-Ivar Nysterud har delvis deltatt som prosjektmedarbeider. Det er innleid ekstern bistand, med særlig kompetanse innenfor IT-revisjon og informasjonssikkerhet. Direktør Siv Irene Aasen og medarbeider Herman Vidje, IT-revisjon- og risikotjenester i BDO har bistått oss med dette.

1.5 Oppbygging av rapporten

I kapittel 2 beskrives datagrunnlaget, datainnsamlingen og anvendte metoder. I tillegg redegjøres for dataenes reliabilitet (pålitelighet) og validitet (gyldighet). Deretter, i kapittel 3, utledes revisjonskriteriene. Revisjonskriteriene oppsummeres til slutt i kapitlet og er i tillegg tatt inn innledningsvis i kapittel 5 og kapittel 6.

I kapittel 4 redegjøres for overordnet organisering og for kommunens overordnede ansvar for personvern og informasjonssikkerhet etter personopplysningsloven.

I kapitlene 5 og 6 redegjøres for revisjonens funn i henholdsvis barnevernet og skolene. Revisjonen har i denne rapporten valgt å ta med noen faglige råd og tips til de reviderte virksomhetene, og disse følger på slutten av kapittel 5 og 6.

Rapportens vurderinger, samlet vurdering og konklusjon samt anbefalinger følger i kapittel 7. Samlet vurdering og anbefalinger står også i sammendraget foran i rapporten. Rådmannens høringsuttalelse, datert 1.6.2016, omtales i sammendraget og følger i sin helhet som vedlegg.

2 ANVENDTE METODER I PROSJEKTET

Undersøkelsen er gjennomført i tråd med RSK 001 - Standard for forvaltningsrevisjon, som fastsatt av styret i Norges Kommunerevisorforbund. Standarden definerer hva som er god revisjonsskikk innen kommunal forvaltningsrevisjon.

2.1 Revisjon av informasjonssikkerhet

Undersøkelsen tar for seg revisjon som omfatter utvalgte IT-prosesser relatert til informasjonssikkerhet og personvern. Informasjonssikkerhet handler ofte om å hindre at uvedkommende får innsyn i personopplysninger, at opplysningene ikke uberettiget endres samt at opplysningene er tilgjengelige for de som trenger dem når behovet er der. Det finnes flere rammeverk og metoder når det skal gjennomføres en revisjon innenfor dette området. Intervjuer og revisjonens vurderinger bygger på Cobit 5.0 som er et rammeverk som fokuserer på god styring og kontroll med IT.

2.2 Datainnsamling og datagrunnlag

Undersøkelsen bygger på data som er samlet inn gjennom dokumentanalyse og intervjuer. Revisjonen har også foretatt en test for å se at det er samsvar mellom opplyst tilgang og faktisk tilgang til brukere med privilegerte rettigheter blant ansatte i barnevernet.

Undersøkelsen tar som nevnt for seg behandling av personopplysninger om barn i barnevernet og elevene i skolen. Utgangspunktet var å undersøke dette i lys av utrullingen av fagsystemet *hypernet for Skole*. Fordi utrullingen av dette systemet er forsinket, har revisjonen undersøkt behandlingen av personopplysninger om elevene generelt. Revisjonen valgte å undersøke dette ved to skoler, der det ble gjennomført intervjuer med ledelse og ansatte.

Utvalg
De utvalgte skolene er Rasta barneskole og Løkenåsen ungdomsskole. Valget falt på disse to skolene for å få med en barneskole og en stor ungdomsskole. I og med at vi allerede hadde intervjuet systemansvarlige for *hypernet for Skole* på kommunenivå, og disse også er ansatt som assisterende rektorer på henholdsvis Fjellsrud skole og Åsen skole, ble disse to skoler valgt bort. Det ble også tillagt vekt at ledelsen ved Rasta barneskole nylig hadde blitt skiftet ut. Revisjonens funn gjelder derfor bare de to skolene. Skoleeier har imidlertid et overordnet ansvar for informasjonssikkerheten. Revisjonens funn som gjelder skoleeier, vil derfor gjelde generelt.

Dokumentanalyse
Revisjonen har innhentet og gjennomgått aktuelle dokumenter som er innhentet fra kommunen. Vi forespurte kommunen om relevant dokumentasjon og har gjennomgått den dokumentasjonen som vi har mottatt. Som undersøkelsen vil vise var den mottatte dokumentasjonen mindre omfattende enn forventet.

Intervjuer
Som det framgår av undersøkelsen er det lite skriftlig dokumentasjon på området og det har derfor vært nødvendig å supplere med intervjuer. Revisjonen har gjennomført en rekke intervjuer med ledere i kommunens administrasjon og relevante ansatte i barnevernet og på de utvalgte skolene. Gjennom intervjuer er den skriftlige informasjonen supplert og utfylt med beskrivelser og informasjon om faktiske forhold i barnevernet. Innenfor skole viste det seg at det ikke foreligger skriftlig dokumentasjon på sektornivå og i liten grad foreligger skriftlig dokumentasjon på de utvalgte skolene. Informasjon om skolene i Lørenskog baserer seg derfor hovedsakelig på intervjuer.

Aktuelle intervjuobjekter er ansvarlige for behandling av personopplysninger på sektornivå og virksomhetsnivå i kommunen. Intervjuene er gjennomført som delvis strukturerte dybdeintervjuer. I forkant av intervjuene har revisjonen utarbeidet intervjuguider med forhåndsdefinerte spørsmål, for å sikre at intervjuene dekker de temaer som trengs for å besvare undersøkelsens problemstillinger.

Det ble gjennomført intervjuer med teknologidirektør og kommunaldirektør for oppvekst og utdanning, personvernombudet i kommunen, ansatte ved IKT-avdelingene IKT-basis drift og IKT-arkitektur og utvikling, og systemansvarlige for fagsystemet *hypernet for Skole* på kommunenivå. I tillegg er det gjennomført intervju med skolesjef og tre intervjuer på hver av de utvalgte skolene (rektor og assisterende rektor, saksbehandler og IKT-ansvarlig på den ene skolen[4] og erfarne lærere/baseleder på den andre skolen) samt at det er gjennomført fire intervjuer i barnevernet (barnevernsjef, fagkonsulent, saksbehandler, merkantil).

Det er skrevet referater av intervjuene, som igjen er verifisert av intervjuobjektene. De intervjuede har fått mulighet til å korrigere og rette opp eventuelle feil og misforståelser. Alle intervjuede har verifisert at informasjonen revisjonen har fått, er riktig. Referatene fra intervjuene har vært et avgjørende bidrag til det datagrunnlaget vi trengte for å besvare problemstillingene i undersøkelsen.

2.3 Dataenes pålitelighet og gyldighet

I enhver undersøkelse er det utfordringer når det gjelder pålitelighet og gyldighet. Pålitelige data sikres ved å være nøyaktig under datainnsamling og databehandling. Gyldighet betegner dataenes relevans for problemstillingene som er valgt.

Revisjonen mener dataene rapporten bygger på samlet sett er pålitelige og gyldige og derfor gir et forsvarlig grunnlag for revisjonens vurderinger og konklusjoner.

Høy gyldighet sikres også gjennom at referater fra intervjuene i etterkant har blitt sendt ut til verifisering hos de intervjuede. Alle referatene har blitt returnert med rettelser til revisjonen. Dermed er vi trygge på at informasjonen som har blitt brukt for å besvare problemstillingene, er korrekt.

[4] På den andre skolen er assisterende rektor også IKT-ansvarlig

3 REVISJONSKRITERIER

Revisjonskriterier er de normer og krav som stilles til kommunens virksomhet på det området som er gjenstand for en forvaltningsrevisjon. Revisjonskriteriene utgjør dermed den målestokken som kommunens praksis holdes opp mot og danner grunnlaget for revisjonens vurderinger av hvorvidt de undersøkte virksomhetene ivaretar informasjonssikkerheten på sentrale områder. Revisjonskriteriene utledes fra autoritative kilder.

I denne undersøkelsen utledes revisjonskriteriene blant annet fra personopplysningsloven, personopplysningsforskriften, veileder for sikker håndtering av personopplysninger i skolen og Datatilsynets veileder om internkontroll og informasjonssikkerhet. Revisjonskriteriene til denne revisjonen utledes i dette kapitlet og gjentas i tillegg i begynnelsen av kapitlene om barnevern og skole.

3.1 Personvern

Innledning
Før endringen i 2014 hadde ikke Norges Grunnlov noen generell beskyttelse av personvernet, annet enn § 102s beskyttelse mot vilkårlige ransakinger i private hjem. Endringene styrker vernet om flere grunnleggende menneskerettigheter, som retten til privatliv, personvern, ytringsfrihet og krav på rettssikkerhet.[5] Personvernet blir her forstått som vern om enkeltindividets privatliv, personlige integritet og private kommunikasjon (Wessel-Aas 2014). Personvern handler om retten til et privatliv og retten til å bestemme over opplysninger og vurderinger som kan knyttes til egen person. Begrepet innebærer i stor grad også vernet av individers rett til å ha innflytelse på bruk og spredning av opplysninger om seg selv. Personvern betyr også at den enkelte i størst mulig grad skal kunne bestemme over egne personopplysninger (Datatilsynet 2014). I tillegg til å være en viktig menneskerettighet er personvern også et sentralt demokratisk prinsipp.

Personopplysninger, informasjonssikkerhet og risikovurderinger
En personopplysning er opplysninger og vurderinger som kan knyttes til en enkeltperson, herunder enkeltmenneskers adferdsmønstre. Personopplysninger kan finnes i mange formater, for eksempel i tekster og dokumenter, bilder, film, video- og lydopptak. Navn, adresse, alder, telefonnummer er personopplysninger. Innhold i saksdokumenter, utredninger eller vurderinger som omhandler enkeltpersoner er også personopplysninger.

Dette innebærer en risiko for at personer kommunen har lagret opplysninger om, kan bli utsatt for krenkelser av sitt personvern. Kommunen må derfor følge personopplysningsloven med forskrift og

[5] Grunnlovens § 102: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige identitet.»

ha tilfredsstillende rutiner for både bruk og beskyttelse av slike personopplysninger (Datatilsynet 2009). Alle som er tilknyttet kommunen «må kunne stole på at bruken av IKT ikke fører til at virksomhetene mister kontrollen med hvordan opplysninger om enkeltpersoner skal håndteres» (Normann og Tranvik 2012, 14).

Flere lover pålegger kommunen plikter for sikring av personopplysninger. Forvaltningslovens bestemmelser om taushetsplikt om opplysninger som gjelder den enkeltes personlige forhold er særlig relevant, da personlige forhold er personopplysninger. Videre er arkivloven med forskrifts bestemmelser om fysisk sikring av arkivlokaler relevant, da arkivmaterialer ofte inneholder personopplysninger. I tillegg er blant annet helsepersonelloven, helseregisterloven, helseinformasjonssikkerhetsforskriften, opplæringsloven, lov om elektronisk signatur og e-forvaltningsforskriften relevante.

Personopplysningsloven skal beskytte enkeltindivider mot at deres personvern blir krenket gjennom behandling av personopplysninger, jf. personopplysningslovens § 1. Handlinger som normalt vil krenke personvernet er for eksempel (Datatilsynet 2009) at

- personopplysninger behandles i det skjulte
- flere og mer inngående personopplysning samles inn enn nødvendig
- personopplysninger ikke slettes når det ikke er behov for dem lenger
- den registrerte ikke får innsyn i opplysninger om seg selv
- personopplysningene som behandles er feilaktige
- personopplysningene tilflyter uvedkommende

Derfor krever loven at personopplysninger skal beskyttes tilfredsstillende mot uberettiget innsyn og uberettigede endringer. Samtidig skal opplysningene være tilgjengelig for de som trenger dem, når de trenger dem. Det fordrer tilfredsstillende informasjonssikkerhet. Datatilsynet definerer informasjonssikkerhet som følger:

> Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har. Deretter gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende.
>
> Dersom risikovurderingene avdekker manglende tiltak må det vurderes om nye tiltak skal iverksettes for å oppnå tilfredsstillende sikkerhetsnivå for personopplysningene. Kontrollrutiner må utarbeides og jevnlig følges, for å kontrollere at tiltakene blir fulgt opp og virker etter hensikten.
>
> Datatilsynet 2009, 8.

En risiko må i denne sammenhengen forstås som summen av sannsynligheten og konsekvensen av en hendelse som er negativ for kommunens informasjonssikkerhet. Risikovurderinger er altså en sentral del av arbeidet med sikkerhetstiltak og informasjonssikkerhet, noe som hjemles i personopplysningsforskriftens § 2-4:

> (…) Den behandlingsansvarlige skal gjennomføre risikovurderinger for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.
>
> Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger (…).
>
> Resultatet av risikovurderingen skal dokumenteres.

Nærmere om informasjonssikkerhet generelt
Kommunens informasjonssikkerhet skal ivaretar tre sentrale hensyn:

1. Sikre personopplysningenes **konfidensialitet**. Det vil si at uvedkommende skal hindres fra å få tilgang til opplysningene. Opplysningene som medisinske diagnoser og spesielle lærevansker skal ikke være tilgjengelig for andre enn de som har tjenstlige behov for å vite om dem. Dersom slike opplysninger ligger lett tilgjengelig for andre enn de som har rett til dem, foreligger et brudd på opplysningenes konfidensialitet.

2. Sikre personopplysningenes **integritet**. Det vil si å hindre at opplysningene endres eller slettes av personer som ikke er autorisert til å endre eller slette opplysningene. For eksempel skal ikke hvem som helst kunne gå inn å endre eller slette opplysninger om eksamensresultater, sykefravær eller behandlingsopplegg i kommunens IKT-system. Dersom andre sletter eller endrer disse opplysningene uten å ha lov til det, er det et brudd på opplysningenes integritet.

3. Sikre personopplysningenes **tilgjengelighet**. Det vil si å sørge for at opplysningene er tilgjengelige for dem som har rett til og behov for å bruke dem. Dersom det er svikt i dataoverføringen mellom deler av kommunehelsetjenesten eller mellom kommune-helsetjenesten og spesialisthelsetjenesten ikke kommer fram til helsepersonellet når det trengs, er det et brudd på opplysningenes tilgjengelighet.

Hensynene til konfidensialitet, integritet og tilgjengelighet må veies opp mot hverandre i arbeidet med informasjonssikkerhet. Behovene for konfidensialitet og tilgjengelighet kan for eksempel ofte være motstridende. Som Datatilsynets veileder framhever er det derfor «viktig at kryssende hensyn identifiseres, og at prioriteringer mellom forskjellige behov fremgår i beskrivelsen av akseptabelt risikonivå» (Datatilsynet 2009, 25). Revisjonen legger derfor til grunn at kommunen gjennomfører risikovurderinger, og dokumenterer disse. Det skal tydelig framgå hvordan de forskjellige sikkerhetsbehov vektes i forhold til å ivareta konfidensialitet, integritet og tilgjengelighet til de personopplysninger som lagres og brukes.

Videre, for å oppnå tilfredsstillende informasjonssikkerhet må kravene i personopplysningslovens § 13 fylles:

> Den behandlingsansvarlige og databehandleren 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. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.
>
> En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd. (…)
>
> Personopplysningsloven § 13

Hva som ligger i tilfredsstillende informasjonssikkerhet utdypes videre i personopplysningsforskriften § 2-7, andre ledd, som presiserer at «[a]nsvars og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder». Ifølge Datatilsynets veileder innebærer det at «[a]nsvar og myndighet relatert til drift av informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeidet (sikkerhetsledelse) må klarlegges» (Datatilsynet 2009, 25).

Behandling av personopplysninger og tilganger

Med behandling av personopplysninger forstås enhver bruk av personopplysninger (personopplysningsloven § 2). Grensene for en behandling faller ofte sammen med det som regnes å være et IKT-system, med tilhørende manuelle rutiner, som behandler personopplysninger.

Medarbeiderne skal være autorisert for bruk av IKT-systemet og de skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med fastlagte rutiner (personopplysningsforskriften § 2-8).

Informasjonssikkerhet i skolen

Datatilsynet (2009) skriver som nevnt at «[i]nformasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte». Senter for IKT i utdanningen (2011) utdyper de tre typene sikkerhetsbrudd som personopplysninger i skolen skal sikres mot når det gjelder brudd på:

- *Konfidensialiteten* ved å hindre at uvedkommende i eller utenfor skolen for tilgang til personopplysninger, herunder ansatte uten tjenstlig behov for opplysningene. Det er skoleeiers ansvar å tilstrebe at «ikke flere enn strengt tatt nødvendig får tilgang til spesielt sensitive eller sterkt personlige opplysninger», og skoleeier har ansvar for å treffe tiltak for å unngå brudd på opplysningenes konfidensialitet.
- *Integriteten* ved å hindre at personopplysninger ikke endres eller slettes av personer i eller utenfor skolen som ikke har fått lov til å gjøre dette. Hvis dette skjer, kan opplysningene bli feilaktige, misvisende eller ufullstendige og innebære risiko for at beslutninger fattes på sviktende grunnlag, eller at det gis et feilaktig bilde av dens om opplysningene omhandler.

- *Tilgjengeligheten* for personer i eller utenfor skolen som har rettmessig behov for tilgang til dem. Det er viktig for de ansatte i skolen at opplysningene er tilgjengelige slik at de kan gjøre jobben sin. For de som opplysningene gjelder er dette også viktig – skolen må kunne finne igjen opplysninger som gjelder elever eller foreldre når det trengs. Skoleeier må ha et bevisst forhold til hvem som skal ha tilgang til opplysninger og hvem som ikke skal ha det.

Rutiner for sikker håndtering av personopplysninger i skolen
For å sikre seg mot brudd på informasjonssikkerhet, er det nødvendig at skolen eller skoleeier lager rutiner for hvem som skal håndtere personopplysninger og hvordan dette skal foregå (Senter for IKT i utdanningen 2011). I veiledningen nevnes spesielt at det er fornuftig å tenke igjennom spørsmål om registrering, lagring, endring/sletting/arkivering og tilgang til opplysningene.

3.2 Internkontroll

En sentral del av administrasjonssjefens ansvar i kommunen er å påse at tjenesteapparatet fungerer på en hensiktsmessig måte. Administrasjonssjefen er med andre ord ansvarlig for samordning og effektivisering av hele den kommunale virksomheten. Det framgår av kommunelovens § 23 nr. 2:

> Administrasjonssjefen skal påse at de saker som legges frem for folkevalgte organer, er forsvarlig utredet, og at vedtaket blir iverksatt. Administrasjonssjefen skal sørge for at administrasjonen drives i samsvar med lover, forskrifter og overordnede instrukser, og at den er gjenstand for betryggende kontroll.

Av dette følger at administrasjonssjefen har det formelle ansvaret for å sikre betryggende kontroll, og herunder etablere tilfredsstillende rutiner for internkontroll. Med internkontroll menes det administrative kontrollansvaret, det vil si systematiske tiltak som skal sikre at virksomhetenes aktiviteter planlegges, organiseres, utføres og vedlikeholdes i samsvar med krav i eller i medhold til lov. For kommunen og kommunens virksomheters behandling av personopplysninger er personopplysningslovens § 14 særlig relevant, da den slår fast at det skal etableres internkontroll:

> 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.
>
> Den behandlingsansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda. (…)

I forbindelse med internkontroll er arbeidsdeling et viktig prinsipp. I denne sammenheng innebærer prinsippet om arbeidsdeling at den som autoriserer en tilgang (har fullmakt til å beslutte at noen skal få en tilgang) ikke samtidig er den som gir tilgangen i systemet. For øvrig bør roller i størst mulig grad bør rendyrkes og antall ansatte med utvidede rettigheter bør begrenses. I denne sammenheng innebærer dette at en person normalt ikke tildeles mer enn én rolle i et system.

3.3 Utledning av revisjonskriterier

Revisjonen legger til grunn at informasjonssikkerhetsarbeidet i Lørenskog skal baseres på en klar fordeling av roller og ansvar. Hvem som har ansvar for å gjennomføre risikovurderinger og iverksette forbedrings- og kontrolltiltak bør framgå. Rolle- og ansvarsfordelingen skal være dokumentert, og organiseringen av informasjonssikkerhetsarbeidet skal være beskrevet og dokumentert.

Videre legges til grunn at kommunens virksomheter skal identifisere og ha oversikt over hvilke personopplysninger den oppbevarer og behandler, gjennomføre risikovurderinger av hvorvidt dagens sikkerhetstiltak er tilfredsstillende, samt iverksette nye tiltak og utarbeide og følge opp kontrollrutiner. Risikovurdering og resultatet av den (tiltak) bør være dokumentert.

Den enkelte medarbeiders tilganger til datasystemet skal være i tråd med rutiner og baseres på tjenstlige behov og følges opp på en systematisk måte. For å undersøke kravet i § 2-8 i personvernforskriften om nødvendig kunnskap utledes dessuten at det må dokumenteres og gjennomføres et holdningsskapende arbeid for hensiktsmessig behandling av personopplysninger og overholdelse av bestemmelser på området, og slik bidra til ivaretakelse av personopplysningenes konfidensialitet, integritet og tilgjengelighet.

Problemstilling	Revisjonskriterier
Har de undersøkte virksomhetene ivaretatt informasjonssikkerheten på sentrale områder?	**Organisering av sikkerhetsarbeidet (personopplysningsforskriften § 2-7)** ➔ Organiseringen av sikkerhetsarbeidet skal beskrives. ➔ Informasjonssikkerhetsarbeidet skal baseres på en klar fordeling av roller og ansvar. ➔ Fordelingen av roller og ansvar skal være dokumentert. **Risikovurdering** (**personopplysningsforskriften § 2-4)** ➔ Det skal gjennomføres risikovurderinger med jevne mellomrom. ➔ Risikovurderingene skal dokumenteres. ➔ Resultatet av risikovurdering bør nedfelles i en aktivitetsplan eller lignende. ➔ Det skal foreligge en oversikt over personopplysningene som behandles. **Tilgangskontroll (personopplysningsforskriften § 2-5 og § 2-8)** ➔ Det skal være etablert rutiner og praksis for en tilfredsstillende tilgangskontroll i fagsystemet. ➔ Det skal gjennomføres holdningsskapende arbeid. ➔ Tilgang til informasjon i fagsystemet skal være i samsvar med tjenstlig behov.

4 ORGANISERING OG KOMMUNENS OVERORDNEDE ANSVAR

4.1 Innledning

Dette kapitlet gir leseren innblikk i organiseringen i Lørenskog kommune. Deretter gir kapitlet leseren oversikt over organiseringen av skolesektoren. Lørenskog kommune har utpekt personvernombud. Personvernombudet har en sentral rolle i arbeidet med personvern i henhold til lovverket, og det redegjøres for personvernombudets rolle i Lørenskog kommune.

Kapitlet gir videre innblikk i kommunens ansvar etter personopplysningsloven og det arbeidet som kommunen selv har satt i gang innenfor området intern kontroll og informasjonssikkerhet. Et av prosjektene som er satt i gang innenfor dette feltet omhandler informasjonssikkerhet ut fra en overordnet tilnærming. For å få et helhetlig perspektiv på kommunens pågående arbeid med informasjonssikkerhet, er det relevant å trekke noen linjer til dette arbeidet.

Kapitlet avslutter med å gi leseren innblikk i teknologiavdelingen, både når det gjelder organisering og noen av oppgavene som tilligger denne avdelingen.

4.2 Organiseringen i Lørenskog kommune

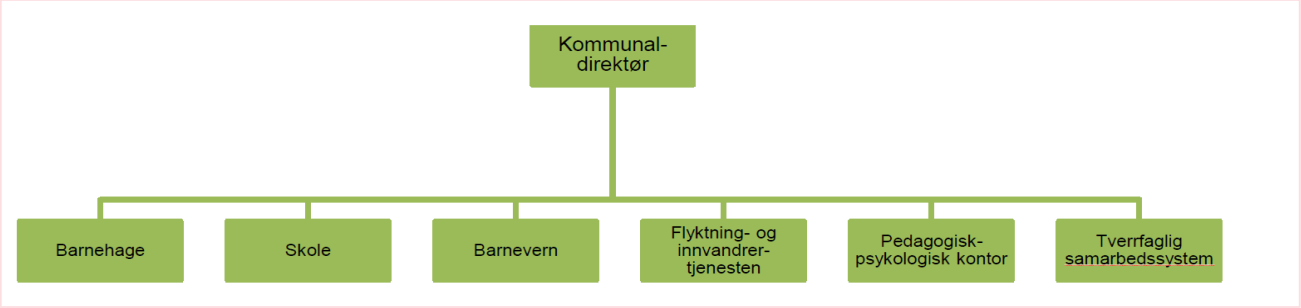
Lørenskog kommunes administrative organisering ser slik ut på overordnet nivå:

Figur 1 Administrativ organisering

Kilde: Lørenskog kommunes hjemmeside

Figuren viser at teknologiavdelingen er en av tre avdelinger under rådmannen, og videre viser oversikten at administrasjonen er inndelt fire sektorer. Blant virksomhetene som er organisert under sektor oppvekst og utdanning er *skole* som ledes av skolesjef og *barnevern* som ledes av barnevernsjef.

Figur 2 Sektor oppvekst og utdanning



Kilde: Årsmelding Lørenskog kommune 2014.

4.3 Rollen som personvernombud

I perioden 2004-2006 ble det foretatt en gjennomgang av informasjonssikkerheten på overordnet plan i kommunen[6]. I denne forbindelse valgte kommunen å utpeke et personvernombud med hjemmel i personopplysningsforskriften § 7-12. Vedkommende er fremdeles personvernombud i kommunen og er til daglig seksjonsleder for juridisk seksjon. Personvernombudet peker på at personvernarbeidet har vært lavt eksponert etter denne gjennomgangen.

> Fra kommunens øverste ledelse har arbeid med personvern/informasjonssikkerhet vært lavt eksponert og prioritert. Med en rekke andre oppgaver knyttet til min stilling har arbeid med personvern ikke kunnet prioriteres og slik sett har jeg vært et personvernombud på papiret. Jeg har dog ved spørsmål fra sektorene bistått og gitt råd, samt påpekt overfor ledelsen at arbeidet bør settes på dagsorden og prioriteres.
>
> Personvernombudet i Lørenskog

Personvernombudet peker også på at sektorene har gjort mye arbeid med tanke på personvern og informasjonssikkerhet. Barnevernet pekes på som et godt eksempel. Barnevernet har fokusert på intern kontroll og utarbeidelse av rutiner med mer. Selv om arbeidet ikke har blitt kalt arbeid med personvern og informasjonssikkerhet, handler dette langt på vei om det samme: «utarbeid rutiner, prosedyrer, forta oppdateringer mm for å sikre at krav til konfidensialitet, integritet og tilgjengelighet overholdes» (ibid).

Personvernombudet opplyser at det i 2004-2006 ble utarbeidet en oversikt over opplysninger som nevnt i personopplysningsloven § 32, men denne oversikten over meldepliktige opplysninger er ikke

[6] Kvalitetssystemet RiskManager ble anskaffet på denne tiden, men systemet har ikke blitt holdt vedlike (opplyses av kommunaldirektør for oppvekst og utdanning og av personvernombudet).

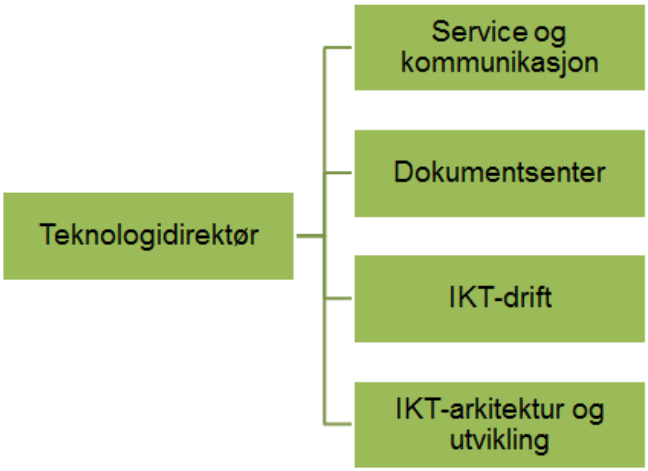
oppdatert etter dette. Per i dag finnes ingen totaloversikt over antall behandlinger av personopplysninger, og det har heller ikke gått meldinger til Datatilsynet så langt personvernombudet kjenner til. Etter personvernombudets mening er det viktigste at det finnes og faktisk benyttes rutiner og god praksis i organisasjonen som sikrer at det ikke skjer brudd på kravene til konfidensialitet, integritet og tilgjengelighet.

Det pågående internkontrollprosjektet i kommunen har ledelsesforankring opplyses videre. I denne forbindelse vil også rollen som personvernombud bli gjenstand for vurdering knyttet til hvem eller hvor i organisasjonen personvernombudet skal være (ibid).

4.4 Teknologiavdelingen

Teknologiavdelingen i kommunen ble opprettet 1.1.2015. Avdelingen ledes av teknologidirektør som tiltrådte 1.5.2015. Avdelingen er organisert slik:

Figur 3 Teknologiavdelingen



Kilde: Teknologidirektør, Lørenskog kommune

Teknologidirektøren informerer om at de fire seksjonene har ansvar for alle servicetjenester knyttet til informasjon, dataflyt, IKT, arkiv og saksgang. Ansvaret gjelder internt og mot kommunens innbyggere og næringsliv. Formålet med avdelingen er å bidra til effektivisering, standardisering og digitalisering av kommunale tjenester opplyses til revisjonen.

Dokumentsenterets hovedoppgave er å sørge for at kommunen foretar dokumenthåndtering og arkivering i henhold til lover og forskrifter.

> Seksjonen er kommunens hovedpostmottak og mottar daglig brev/e-post/elektroniske skjema og digitale henvendelser. Disse sorteres, kontrolleres og distribueres, enten via registrering i

> kommunens administrative sakssystem WebSak Fokus, eller via vårt internbud. Vi foretar kontroll av dokumenter produsert i WebSak Fokus.
>
> Dokumentsenteret[7]

Seksjon for IKT-drift har blant annet systemeieransvar for kommunens felleskomponenter og ansvar for brukerstøtte på interne tjenester og infrastruktur[8].

Seksjon for IKT-arkitektur og utvikling har blant annet ansvar for utvikling av IKT-målbilder og virksomhetsarktitektur (dataflyt og prosesser) i nært samarbeid med fagområdene og skal bistå sektorene i prosjekter og IKT-utvikling[9]. Det er utpekt kundeansvarlige for hver sektor og det etableres møteplasser for kundeansvarlige og sektorer (økonomiplan 2016-2019, 70). Avdelingen samarbeider med flere sektorer om anskaffelser, strategiarbeid og andre utviklingstiltak innenfor teknologi og digitaliseringskompetanse. Høsten 2015 ble det igangsatt et kartleggingsarbeid av IKT-porteføljen og det er igangsatt forprosjekter som skal bidra til økt standardisering og konsolidering (ibid). Nærmere om dette under punkt 4.4 nedenfor.

4.5 Overordnet ansvar for personopplysninger og informasjonssikkerhet

Kommunen som juridisk enhet er behandlingsansvarlig etter personopplysningsloven § 2 nr. 4. I en kommune vil eksempelvis rådmannen som kommunens øverste administrative leder ha ansvar for at personopplysningsloven og forskriften følges (Datatilsynet 2009). Dette ansvaret kommer til uttrykk i personopplysningsloven § 14:

> Behandlingsansvarlig er ansvarlig for etablering og vedlikehold av planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av personopplysningsloven, herunder sikre personopplysningenes kvalitet.

Behandlingsansvaret er i delegert[10] til kommunaldirektørnivå:

> Under henvisning til delegeringsbestemmelsene som framkommer i «Delegeringsreglement for Lørenskog kommune», vedtatt av Lørenskog kommunestyre i møte 08.02.2012, sak 001/12, samt gjeldende praksis, delegerer rådmannen sin myndighet i enkeltsaker og generelle saker av ikke-prinsipiell betydning til kommunalsjefer for hhv. helse, og omsorg, teknisk, kultur og idrett, og oppvekst og utdanning, samt avdelingssjefer i sentraladministrasjonen. [..].

[7] Hentet fra Lørenskog kommunes hjemmeside under nyheter/dokumentsenteret den 8.4.2016. Siden er sist endret 2.6.2015

[8] Hentet fra kommunens hjemmeside under nyheter/seksjon-for-ikt-basis-drift-og-support den 8.4.2016. Siden er sist endret 2.6.2015

[9] Hentet fra kommunens hjemmeside under nyheter/seksjon-for-ikt-arktitektur-og-utvikling den 8.4.2016. Siden er sist endret 11.12.2015

[10] Notat fra konstituert rådmann til kommunaldirektørene 8.12.2012 om videredelegering av rådmannens myndighet.

Dette ansvaret innebærer at lovgiver forventer at personopplysninger er sikret på en forsvarlig måte, og at øverste leder følger opp dette i praksis. Øverste leder skal sørge for at virksomheten har oversikt over hvilke plikter som gjelder, hvordan opplysningene blir behandlet og sikret samt at alle rutiner knyttet til dette er godkjent og blir fulgt opp av de ansatte (Datatilsynet 2009, 3).

4.6 Kommunens arbeid med internkontroll og informasjonssikkerhet

Rådmannen ga i oppstartmøtet uttrykk for at det har vært betydelige utfordringer på teknologiområdet i Lørenskog kommune og man startet derfor opp et stort arbeid innenfor dette området i 2014. Det redegjøres i korte trekk for dette under punkt 4.6.2 nedenfor.

4.6.1 Tilbakeblikk

Teknologidirektøren peker på at det jobbes godt i kommunen med informasjonssikkerhet nå, men ikke systematisk og ikke med god nok sporbarhet. Kommunaldirektøren for oppvekst og utdanning informerer om at kommunen hadde en gjennomgang av informasjonssikkerhet for noen år tilbake. Dette skjedde på den tiden kvalitetssystemet RiskManager ble innført. I dette systemet finnes et dokument om delegering av ansvaret for sikring av personopplysninger. I tillegg ble det utarbeidet kriterier for hva som er tilfredsstillende informasjonssikkerhet i Lørenskog. Kriteriene skulle legges til grunn ved gjennomføring av risikovurderinger etter personopplysningsloven § 13. Kvalitetssystemets brukerterskel viste seg imidlertid å være høy, og dokumentene i systemet er derfor i mindre grad kjent og brukt i organisasjonen i dag.

Teknologidirektøren opplyser at det på overordnet nivå ikke finnes skriftlige rutiner eller retningslinjer i kommunen for oppfølging og overvåking av tilgangsstyring, herunder tilgang til personopplysninger.

Kommunaldirektør for oppvekst og utdanning viser til at taushetserklæring, lederplattform og autorisasjonsskjema for nye IKT-brukere er i bruk i organisasjonen i dag.

4.6.2 Pågående prosjekter innen IKT og internkontroll i Lørenskog

I 2014 utarbeidet kommunen en IKT-forretningsplan. I forlengelsen av den ovennevnte gjennomgangen pågår to større prosjekter i kommunen:

- Et internkontrollprosjekt under ledelse av økonomidirektør og direktør for organisasjonsavdelingen.
- ROS – analyse (Risiko – og sårbarhetsanalyse) knyttet til IKT infrastruktur, med bistand fra et innleid konsulentfirma. ROS – analysen er i avslutningsfasen per februar 2016.

Det er ikke etablert noen IKT-strategi i Lørenskog kommune utover ovennevnte IKT-forretningsplan, men det er igangsatt arbeid med etablering av en digitaliseringsstrategi og det arbeides med etablering av IKT-strategier innenfor *helse og omsorg* og innen *oppvekst og utdanning* skriver teknologidirektør i et brev til revisjonen i september 2015.

Internkontrollprosjektet for hele kommunen er videreført i 2016. Teknologidirektør peker på at det blant annet skal innføres et verktøy for intern kontroll i tillegg til at det arbeides videre med å få på plass styrende dokumenter innen flere områder. Teknologidirektøren uttaler at «[i]nformasjonssikkerhet ligger som et av områdene internkontrollprosjektet skal gjennomføre aktiviteter innen» og at personvern inngår i dette arbeidet.

Videre pekes på at det innenfor personvern og informasjonssikkerhetsområdet blant annet er fokus på avklaring av roller og ansvar innen området og at styrende dokumenter skal revideres. Videre skal det gjennomføres innførings- og opplæringsaktiviteter for å sikre etterlevelse ut i organisasjonen. Det er ikke realistisk å være ferdig med dette før i 2017 opplyses videre.

5 INFORMASJONSSIKKERHET - BARNEVERNET

Det undersøkes om barnevernet i Lørenskog ivaretar sentrale krav til personvern og informasjonssikkerhet. Revisjonens funn gjennomgås i punktene 5.2-5.5. I punkt 5.6 følger revisjonens tips til barnevernet. Revisjonens vurderinger følger i kapittel 7.

5.1 Revisjonskriterier

Revisjonskriteriene er utledet foran i rapporten. De oppsummerte kriteriene gjentas nedenfor:

Problemstilling	Revisjonskriterier
Har barnevernet ivaretatt sentrale informasjons-sikkerhetskrav?	**Organisering av sikkerhetsarbeidet (personopplysningsforskriften § 2-7)** ➔ Organiseringen av sikkerhetsarbeidet skal beskrives ➔ Informasjonssikkerhetsarbeidet skal baseres på en klar fordeling av roller og ansvar ➔ Fordelingen av roller og ansvar skal være dokumentert. **Risikovurdering** (**personopplysningsforskriften § 2-4)** ➔ Det skal gjennomføres risikovurderinger med jevne mellomrom ➔ Risikovurderingene skal dokumenteres ➔ Resultatet av risikovurdering bør nedfelles i en aktivitetsplan eller lignende. ➔ Det skal foreligge en oversikt over personopplysningene som behandles. **Tilgangskontroll (personopplysningsforskriften § 2-5 og § 2-8)** ➔ Det skal være etablert rutiner og praksis for en tilfredsstillende tilgangskontroll i fagsystemet ➔ Det skal gjennomføres holdningsskapende arbeid ➔ Tilgang til informasjon i fagsystemet skal være i samsvar med tjenstlig behov

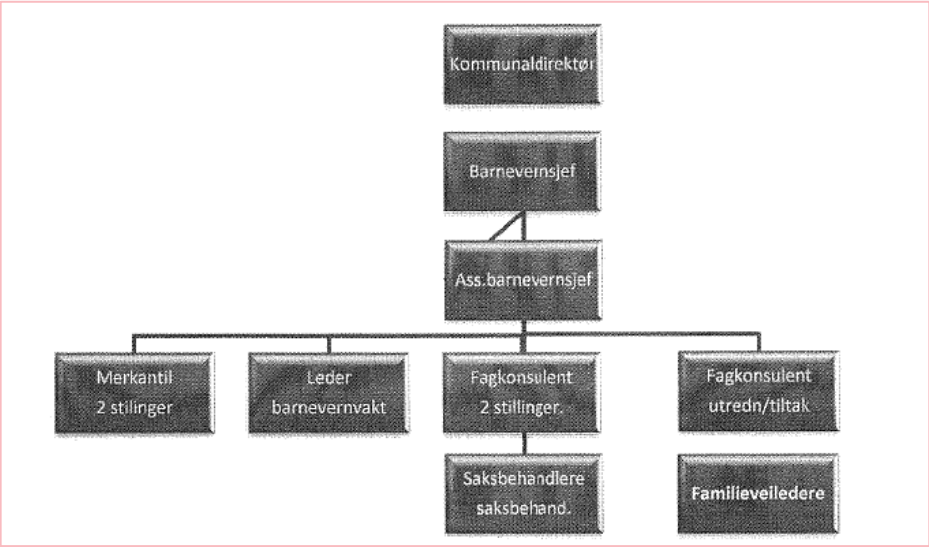
5.2 Introduksjon

Nærmere om organiseringen av barnevernet i kommunen

Barnevernsjef er leder av barnevernet i kommunen. Ledergruppen består av barnevernsjef, assisterende barnevernsjef og 3[11] fagkonsulenter i barnevernet. Barnevernadministrasjonen holder til i lokaler i NAV-bygget i Lørenskog, mens utrednings- og tiltaksteamet (UT-teamet) holder til i andre lokaler i Lørenskog.

[11] Antall fagkonsulenter har økt fra 2 til 3, se organisasjonskart på neste side.

Figur 4 Organisasjonskart barnevernet



Kilde: Barnevernet, Internkontroll 2015. Fra og med våren 2016
er det 3 fagkonsulenter i barnevernet opplyser barnevernet. I tillegg 1 fagkonsulent i UT-team.

I barnevernet er det i alt 32 stillinger (regnet i årsverk) hvorav 25 er knyttet til saksbehandling og administrasjon (KOSTRA 2016[12]).

Antall bekymringsmeldinger er økende. Barnevernet har avvik i forhold til tidsfrister for gjennomføring av barnevernundersøkelser og arbeider for å effektivisere dette arbeidet samtidig som rådmannen vil prioritere midler til ekstra kapasitet fra og med 2016 (økonomiplan 2016-2019, 89). Det var 315 barn med melding og 253 meldinger som gikk til undersøkelse i 2015 (KOSTRA 2016). Det er 198 barn med tiltak per 31.12.2015 (barnevernsjefen).

Generelt om behandling av personopplysninger i barnevernet
Barnevernet behandler personopplysninger om barn i barnevernet og deres familier. Behandling av personopplysninger i barnevernet er hjemlet i barnevernloven. Ansatte i barnevernet har tradisjonelt høyt fokus på taushetsplikten som følger av barnevernloven § 6-7 om taushetsplikt og forvaltningsloven §§ 13 til 13 e. Etter disse bestemmelsene har ansatte i barnevernet også taushetsplikt om noens personlige forhold, inkludert opplysninger om fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted.

Typiske opplysninger som er knyttet til noens personlige forhold er opplysninger om en persons slektskap, familie og hjemmeforhold, fysisk og psykisk helse, karakter og følelsesliv. Det samme gjelder opplysninger om en persons utdanning, arbeid, økonomiske situasjon, holdninger og innstillinger (Barne- og familiedepartementet 2005).

[12] KOSTRA 2016 er tall fra den foreløpige publiseringen for 2015 per 15. mars 2016

Generelt er det slik at barnevernet utfører mange oppgaver som involverer personopplysninger:

- Meldinger gjennomgås og vurderes.
- Undersøkelser gjennomføres.
- Iverksetter hjelpetiltak (tiltak i hjemmet, frivillige plasseringer i fosterhjem).
- Oppfølging av fosterhjem (omsorgsbesøk og tilsynsrapporter).
- Forberedelse og deltakelse i fylkesnemnda når det kreves (omsorgsovertakelse).

Taushetsbelagte opplysninger i barnevernet skal oppbevares nedlåst og barneverntjenesten skal ha et eget arkiv atskilt fra arkivene til andre kommunale tjenester. Opplysningene skal lagres og oppbevares i henhold til lov av 4. desember 1992 nr. 126 om arkiv. Opplysningene skal også behandles i henhold til lov av 14. april 2000 nr. 31 om personopplysninger (Barne- og familiedepartementet 2005).

Fagsystem
Barneverntjenesten benytter et fagsystem som skal tilfredsstille de nevnte lovkrav, være til hjelp i saksbehandling og tilfredsstille krav til rapportering. Barnevernet i Lørenskog bruker fagsystemet Visma Barnevern Familia (Familia).

I Lørenskog kommune er det som nevnt foran i punkt 4.4 slik at hver sektor har en kundekontakt på IKT-avdelingen (IKT arkitektur og utvikling). Kunde- eller sektorkontakten for Familia, som selv kommer fra det tidligere sosialkontoret, opplyser til revisjonen at han har god og jevnlig kontakt med barnevernsjefen som systemeier på Familia. Sektorkontakten opplyser videre at det er aktuelt å legge om tilgangene til fagsystemet fordi oppsettet for tilganger er gammelt, og det er ønskelig å få bedre kontroll med tilgangsstyringen knyttet til påloggingsbildet.

Fagsystemet i barnevernet ligger lokalt på server i Lørenskog kommune. Dataene i barnevernet ligger i sikker sone innenfor en brannmur, på lik linje med andre applikasjoner som kjører sensitive data i kommunen. Nettverksansvarlig på IKT-avdelingen opplyser at det kun er «én-faktor autentisering» uten kryptering fra brukere på intern sone i kommunen for fagsystemet i barnevernet. For de andre systemene i sikker sone krypteres trafikken på terminalserver før pålogging til selve fagsystemet. Det opplyses at det for tiden jobbes for å få løst dette problemet, slik man også kan kjøre trafikken kryptert gjennom terminalserver for fagsystemet i barnevernet.

Revisjonens vurdering
I avsnittet ovenfor framkommer at det er avdekket at fagsystemet og de opplysningene som lagres der bør sikres bedre. Påloggingen har så langt foregått uten tilstrekkelig kryptering («én-faktor autentisering») og dette er ikke en tilfredsstillende løsning.

5.3 Organisering av sikkerhetsarbeidet

Det er lagt til grunn i revisjonskriteriene at organiseringen av sikkerhetsarbeidet skal beskrives, baseres på en klar fordeling av roller og ansvar og fordelingen av roller og ansvar skal være dokumentert. Nærmere om dette i punktene under.

5.3.1 Beskrivelse av sikkerhetsarbeidet

Barnevernsjefen opplyser til revisjonen at det er tre styrende dokumenter i barnevernet som omhandler informasjonssikkerhetsarbeidet i barnevernet:

- Visma Barnevern Familia brukerveiledning
- barnevernets rutinehåndbok («Rutiner 2016»)
- barnevernets dokumenterte internkontroll («Internkontroll – 2015»).

Organisering av barneverntjenesten og dens oppgaver og formål framgår av internkontrollen under kapittel 2, punkt 2 a. I tråd med krav i barnevernloven er organisering og hovedoppgaver beskrevet. Revisjonens gjennomgang viser at dokumentene er utformet med utgangspunkt i barnevernloven, barnelova, offentlighetsloven, forvaltningsloven og arkivloven. Det er ikke gjort spesifikke henvisninger til personopplysningsloven. Rutinehåndboken inneholder en beskrivelse av fagprogrammet som barneverntjenesten bruker for elektronisk saksbehandling. I rutinene framgår de ulike tilgangene som de ansatte har i systemene, krav til passord, oversikt over brukere med utvidede rettigheter (superbrukere og administratorer) samt rutine for sletting av feilførte dokumenter (rutine nr. 15).

5.3.2 Fordeling av roller og ansvar

Behandlingsansvarlig

Det operative behandlingsansvaret / systemansvaret for fagsystemet som barnevernet bruker, er delegert til barnevernsjefen påpeker kommunaldirektør for oppvekst og utdanning. Barnevernsjefen er i samtale med revisjonen tydelig på at selv om ansvaret ikke er skriftlig delegert, er det han som er ansvarlig.

Av den mottatte dokumentasjonen framkommer:

- Organisasjonskart for barnevernet, illustrert under punkt 3 i «Internkontroll - 2015».
- Navn på ansatte med titler
- Oversikt over brukere og deres individuelle rettigheter i fagsystemet
- Oversikt over slettetilganger

Brukere med utvidede rettigheter

Rollen som superbruker innebærer for de ansatte i barnevernet:

- tilgang til å endre maler
- tilgang til å endre fagkoder i systemet
- tilgang til å legge inn nye brukere og endringer i tilganger for disse, og dette legges inn manuelt i systemet av superbruker
- administratorrettigheter.

5.3.3 Rutiner for av sikkerhetsarbeidet

Barnevernsjefen opplyser at det ikke er utarbeidet policydokument for informasjonssikkerhets-arbeidet, utover nevnte rutinehåndbok og internkontrollen i barnevernet. I intervjuer med fagkonsulent og saksbehandler vises til internkontroll og brukerhåndbok som styrende og

veiledende dokumenter. Dokumentene om internkontroll og brukerhåndboken gjennomgås og oppdateres årlig i ledergruppen. IKT og personvern blir ikke særskilt gjennomgått og oppdatert i denne sammenheng. Det er hovedsakelig daglig arbeid og mangler og svakheter i rutiner som diskuteres opplyses det i intervjuene. Endringer og oppdateringer formidles til alle ansatte som skriftlig bekrefter at de har lest internkontroll og rutinehåndbok. Det framkommer at dokumentene er utarbeidet etter kravene i barnevernloven, både i intervju og i dokumentasjonen.

Internkontroll
Barnevernet har dokumentert hvilke tiltak som er iverksatt for å hindre at dokumenter kan komme på avveie i internkontrollen. Dette kravet følger av forskrift av 14. desember 2005 nr. 1584 om internkontroll for kommunens oppgaver etter lov om barneverntjenester. Tiltakene angir regler for:

- fysisk oppbevaring av dokumenter
- låst dør ved lenger fravær fra kontoret
- oppbevaring av dokumenter utenfor arbeidstid og utenfor kontoret
- pc skal være sikret med passord
- elektroniske behandling av opplysninger (sensitive opplysninger sendes ikke på e-post, taushetsbelagte opplysninger som behandles i Websak Fokus[13] unndras offentlig innsyn)
- oppførsel på kontoret (unngå korridor-snakk og lukket dør under klientsamtaler).

I intervjuene ble det redegjort for fysisk og digital lagring av personopplysninger som etter revisjonens mening samsvarer godt med de tiltakene som er beskrevet ovenfor. I tillegg forteller de som revisjonen intervjuet, at originaldokumenter som hovedregel aldri tas med ut av kontoret[14].

Opplæring
Fagkonsulent og saksbehandler opplyser at det er utarbeidet en opplæringsplan for nyansatte i barnevernet og at alle ved ansettelse underskriver på skjema om taushetsplikt. Når det ansettes nye medarbeidere er det hovedfokus på e-post og datasikkerhet, herunder de administrative rutinene ved kontoret og rutiner for låsing og utskrift.

Risikovurdering
Fagkonsulent og saksbehandler opplyser at det ikke foretas periodisk risikovurdering knyttet til IKT og behandling av personopplysninger i fagsystemet eller i mappestruktur på eget område på server. Det gjennomføres periodiske vurderinger i ledergruppen rundt internkontroll, men det er ikke konkret fokus på IKT.

Etterlevelse av rutiner
Fagkonsulent og saksbehandler gir uttrykk for at det ikke er rutiner for regelmessig oppfølging av at rutiner etterleves. Imidlertid påminner man hverandre i det daglige, og man snakker om eventuelle avvik når de oppdages for å unngå gjentakelser.

[13] Kommunens administrative sakssystem. Se også punkt 4.5 om dokumentsenteret.
[14] Unntak for sak i retten. Her må originaler tas med.

Sikring av personopplysninger
Barnevernet mottar som nevnt innledningsvis henvendelser om barn fra ulike hold og kommuniserer med barn, foresatte og fosterforeldre i tillegg til tilsynspersoner, partene i en barnevernssak og fylkesnemnda. Det er derfor nødvendig å sikre personopplysninger ved lagring både i og utenfor fagsystemet.

Både barnevernsjefen og fagkonsulent opplyser til revisjonen at alle personopplysninger i barnevernet vurderes som sensitive. Unntaket er den generelle veiledningsplikten påpeker fagkonsulent.

I intervju opplyser fagkonsulent og saksbehandler at minnepinner ikke benyttes til overføring og eller lagring av data i forbindelse med arbeidet. Dette er det retningslinjer på. Saksbehandlerne legger som hovedregel igjen tjenestetelefonen sin på kontoret når arbeidsdagen er slutt og tar heller ikke bærbar pc med hjem[15]. Barnevernsjefen opplyser at samtlige ansatte bruker bærbare laptoper og hovedregelen er at disse ikke tas med hjem eller ut av kontoret. Saksbehandler opplyser at eventuelle opptak eller video av samtaler overføres til pc'en og at selve opptaket deretter slettes. Utskrifter kvalifiserer som sikker utskrift da det må benyttes kort og kode for å skrive de ut.

I intervjuene med fagkonsulent og saksbehandler stilte revisjonen spørsmål om sikring av personopplysninger ved lagring generelt og spesielt om fysisk og digital lagring. Svarene viser at de tiltakene som er iverksatt er kjent og følges i praksis. Når det gjelder digital lagring kom det fram at lagring av personopplysninger likevel kan skje på personlige arbeidsmapper på pc eller på fellesområdet som bare barnevernet har tilgang til (utenfor sikker sone).

Det opplyses også at barnevernet per dags dato har en blanding av elektronisk og fysisk arkiv. Det er planer om en overgang til helelektronisk arkiv i Familia, men dette avhenger av beslutning på overordnet nivå i kommunen sier fagkonsulent og saksbehandler.

Avvikshåndtering
Det er ikke opprettet rutiner for avvikshåndtering og klassifisering av alvorlighetsgrad dersom personopplysninger skulle komme på avveie. I intervjuene opplyser fagkonsulent og saksbehandler til revisjonen at personopplysninger i barnevernet for øvrig er klassifisert som sensitive personopplysninger. Fagleder vurderer det som veldig alvorlig om disse skulle komme på avveie.

5.4 Risikovurdering

Det er lagt til grunn i revisjonskriteriene at det skal gjennomføres risikovurderinger, arbeidet skal dokumenteres og resultatet skal synliggjøres i en plan eller lignende.

Kommunaldirektør for oppvekst og utdanning sier i intervju med revisjonen at det er barnevernsjefen som har ansvar for å gjennomføre risikovurderinger etter personopplysningslovens bestemmelser

[15] Unntak kan forekomme pga jobbrelaterte hendelser opplyser fagsjef (mobil, PC og arbeidspapirer)

innenfor barnevernet og deres fagsystem. Det opplyses videre at det ikke foreligger føringer på gjennomføring av dette fra sentralt hold i kommunen, men pekes samtidig på generelle føringer om risikovurderinger i tilknytning til HMS og prosjektrammeverket for investeringsprosjekter – samt dokumenter i RiskManager (kvalitetssystem)[16].

Det er krav om en dokumentert oversikt over hvilke personopplysninger som behandles. På revisjonens spørsmål om dette viser barnevernsjefen til internkontroll for barneverntjenesten (2015). Dette dokumentet dekker ikke kravene til risikovurdering i personopplysningsloven § 2-4. Barnevernsjefen opplyser at det likevel foretas risikovurderinger i forbindelse med gjennomgang av internkontroll i barnevernet etter barnevernlovens bestemmelser. Dokumentet revideres årlig.

Internkontrolldokumentet for barneverntjenesten inneholder et punkt om risikoanalyse. I dokumentet vises innledningsvis til forskrift om kommunens oppgaver etter lov om barneverntjenester. For å «skaffe oversikt over områder i barneverntjenesten hvor det er fare for svikt eller mangel på oppfyllelse av myndighetskrav» i eller i medhold av barnevernloven (punkt 1f), peker dokumentet på 21 områder som kan være sårbare. For hvert område pekes på et eller flere tiltak. Seks av områdene tar for seg tiltak om personopplysninger (taushetsplikt, dokumentflyt ved forsendelser, elektronisk behandling av opplysninger, uvedkommende i lokalene, dokumentoppbevaring og korridor-snakk).

Som opplyst i innledningen til dette kapitlet arbeider IKT-avdelingen for å sikre tilgangene til fagsystemet i barnevernet. Behovet ble avdekket i forbindelse med en ikke dokumentert risikovurdering gjennomført av IKT-avdelingen og barnevernet påpeker IKT-avdelingen.

5.5 Tilgangskontroll

Det er lagt til grunn i revisjonskriteriene at det skal etableres rutiner og praksis for tilgangskontroll i fagsystemet. I tillegg bør det gjennomføres holdningsskapende arbeid og tilgangene som gis skal være i samsvar med tjenstlig behov.

5.5.1 Etablerte rutiner og praksis for tilfredsstillende tilgangskontroll

Barnevernsjef opplyser at etablerte rutiner i forbindelse med tilgang til fagsystemet er redegjort for i rutine 15 i rutinehåndboken. De deler av rutinene som etter revisjonens syn er relevante for denne undersøkelsen oppsummerer revisjonen slik:

- Alle saksbehandlere og merkantil har tilgang til bruk av klientmodulen for saksbehandling.
- Det skilles mellom barneverntjenesten, utrednings- og tiltaksteamet (UT-team) og botiltakene.
- En ansatt ved IKT-avdelingen sentralt i kommunen har tilgang.
- Tilgang til systemadministrasjon er begrenset utvalgte personer.

[16] Se nærmere om dette i kapittel 4. Det framgår at systemet i liten grad er i bruk i dag.

- Det er etablerte rutiner med brukernavn og passord (krav til utforming og passordbytte).
- Fagkonsulentene tildeler rettigheter og oppretter brukere samt passiviserer brukertilganger når noen slutter i tillegg til at de kan låse opp passord ved behov.
- Det er åtte navngitte superbrukere ved kontoret, herunder assisterende barnevernsjef og barnevernsjef, samt IT-ansvarlig.
- Supergruppemøter avholdes to ganger i året – for implementering av nyheter.
- Beskrivelse av slettetilgang.

Barnevernsjefen forteller at superbrukerne har administratorrettigheter. Leverandøren gis tilgang til fagsystemet når det er behov. Denne tilgangen åpnes i det enkelte tilfelle av kundekontakten på IKT-avdelingen (systemendringer).

I dokumentet Internkontroll 2015[17] beskrives dessuten ansvarsfordeling, selve administrasjonen, saksbehandlingsrutiner, opplæringsrutiner, merkantile rutiner og arkivrutiner.

Fagkonsulent og saksbehandler opplyser at det er satt opp egne roller i fagsystemet (tilgangsgrupper). Rollene tar utgangspunkt i stilling, men tilpasses i forhold til den enkeltes arbeidsoppgaver, stilling og distriktstilhørighet (for eksempel barneverntjenesten).

Videre opplyses at alle brukere har slettetilgang innenfor de distriktene som den enkelte har tilgang til. Dette innebærer en mulighet til å opprette, endre og slette saker. I fagsystemet er det imidlertid slik at dokumenter i en sak ferdigstilles etter utløpet av en gitt angrefrist. Fristen gjelder for et kort tidsrom og muligheten til å foreta endringer faller bort når fristen har løpt ut.

Brukere med privilegerte rettigheter
Brukere med privilegerte rettigheter, såkalte superbrukere, tildeles på bakgrunn av erfaring og kjennskap til fagsystemet.

Fagkonsulent og saksbehandler påpeker at superbrukere har tilgang til tilgangsadministrasjon i «sysadm-modulen», kan godkjenne utbetalingsplaner[18] og vedtak, og kan endre maler i fagsystemet. Det er videre opprettet flere distrikter i fagsystemet, blant annet: barneverntjenesten (saksbehandlingen av barnevernsaker), utrednings- og tiltaksteamet (UT-teamet) og botiltakene.

Saksbehandlerne i barnevernet har tilgang til distrikt barneverntjenesten, dvs. hele klientmodulen. Saksbehandlere i UT-teamet har tilgang til distrikt UT-team, men ikke til distrikt barneverntjenesten opplyses til slutt.

[17] Revisjonen har mottatt kopi av dokumentene som er mest relevante, og som er nevnt her.
[18] Merkantilt ansatte har også denne tilgangen

Passordinnstillinger
I intervjuene opplyses at det er dobbel sign-on til fagsystemet ved at den ansatte først må logge seg på sin personlige bruker i kommunen for å få tilgang til nettverket og deretter må den ansatte logge seg på i fagsystemet Familia. Passordinnstillingene er de samme i begge systemene og tilfredsstiller dagens krav til passordinnstillinger med hensyn til antall tegn, kompleksitet og tvungent bytte av passord. Systemet inneholder imidlertid ingen passordhistorikk.

Superbrukere har anledning til å nullstille passord for andre brukere av fagsystemet Familia når det er behov for det.

Administrering av brukere og rettigheter
I intervjuene opplyses at nyansatte gis rettigheter i kommunen på grunnlag av en bestilling som sendes når det nye ansettelsesforholdet opprettes. Brukere i fagsystemet opprettes av ansatte med tilgang til brukeradministrasjonsmodulen. Det er likevel slik at det hovedsakelig er fagkonsulent superbruker som gjør dette, men saksbehandler superbruker kan opprette hvis fagkonsulent ikke har mulighet for å gjøre dette. Når ansatte slutter, deaktiveres tilgangen i kommunen på grunnlag av sluttmelding. I fagsystemet passiviseres bruker manuelt innenfor en rimelig tidsperiode.

Periodisk gjennomgang av brukere
Fagkonsulent superbruker foretar periodisk gjennomgang av brukere for å påse at det bare er nåværende ansatte som skal ha aktive brukere i fagsystemet. Fagkonsulent opplyser også at det ikke gjennomføres en periodisk gjennomgang av tilgangsnivå og rettigheter.

Loggføring i fagsystemet
I intervjuene opplyses at den eneste loggføringen i Familia er på slettede dokumenter. Det er mulighet for å se hvem som har slettet, men tekstinnholdet i dokumentet som er slettet kommer ikke fram. Slettelogger blir ikke gjennomgått opplyses til slutt.

5.5.2 Revisjonens test av tilganger

Det står i rutinen at det er 9 personer som er superbrukere i barnevernet med administratorrettigheter. Revisjonen har mottatt en utskrift fra fagsystemet over tilganger og undersøkt om rutinen stemmer med faktisk tilstand. Resultatet følger i tabellen under og viser at 11 personer har tilgang som superbrukere.

Tabell 1 Test av tilganger

Antall ansatte med tilgang som superbrukere i Familia

Stilling	Rutine 15	Oppgitt i intervju	Faktisk tilstand
Ledelse	2	2	2
Fagkonsulent i barnevernet	3	3	3
Saksbehandler i barnevernet	3	3	4*
Merkantil botiltak flyktninger	0	1	1**
IKT-ansvarlig på IKT-avd.	1***	1	1
Totalt antall	*9*	*10*	*11*

Kilder: Dokumenter og intervjuer, barnevernet i Lørenskog. Utskrift: *Tilgang – Saksbehandlere* den 16.3.2016 *En saksbehandler har permisjon, står oppført som aktiv bruker på liste. **Kun tilgang til beboere i botiltakene. ***Det framgår av rutinen at vedkommende har rollen, men vedkommende er ikke med i opplistingen over de personene dette gjelder.

Av tabellen ser vi at faktisk tilstand for personer med tilgang som superbruker stemmer ganske bra med det som er oppgitt i intervjuer og rutine.

5.5.3 Holdninger

Fagkonsulent opplyser at taushetsplikten blir gjennomgått med nyansatte som et ledd i opplæringen av nyansatte i tråd med plan ved ansettelse. Skjema om taushetsplikt underskrives. I tillegg til dette påminner de ansatte hverandre i det daglige arbeidet om taushetsplikten og kontorets regler for håndtering av informasjon og fysisk sikring av dokumenter og opplysninger. Medarbeiderne understreker også viktigheten av taushetsplikt i intervjuene.

5.5.4 Tilganger i samsvar med tjenstlig behov

Barnevernsjefen opplyser at han og assisterende barnevernsjef ikke har noen oppgaver knyttet til rollen som superbruker, og at rollen som superbruker derfor ikke praktiseres[19].

Fagkonsulent gir uttrykk for at antall superbrukere er satt ut fra hensyn til at det skal være mulig å gjøre de oppgavene som kommer inn så effektivt som mulig. Det er nødvendig at flere har denne tilgangen dersom fagkonsulent superbruker for eksempel er fraværende eller det kan være snakk om hastesaker som må løses på kveldstid.

Det framgår av utskriften fra fagsystemet over tilganger at det er tre fagkonsulent superbrukere og to ledere som har tilgang som superbrukere til UT-teamet.

[19] Barnevernsjef og assisterende barnevernsjef har tilgang som superbruker med administratorrettigheter. Dette er merket slik: *«kun rettigheter» i rutine 15 i barnevernets rutinehåndbok.

5.6 Råd og tips

Nedenfor følger enkelte råd og tips som barnevernet kan se nærmere på i forbindelse med oppfølgingen av denne rapporten. Rådene fra revisjonen er ment som faglig veiledning og er ikke uttømmende eller den eneste måten å løse utfordringer på.

Tilgangsgrupper i Familia
Gjennomgang av brukere med tilhørende roller med tilgang til Familia viser at det er et noe høyt antall brukere med privilegerte rettigheter (superbrukere) i fagsystemet i forhold til den totale brukermassen. Tilgangen til brukere av fagsystem burde styres ut fra prinsippet om at en medarbeider kun skal ha tilgang til de ressurser / systemer vedkommende trenger for å utføre sine ordinære arbeidsoppgaver. Dette prinsippet kalles minste privilegiums prinsipp. Dette prinsippet kan være nyttig å legge til grunn dersom barnevernet velger å gå igjennom sine tilganger på nytt.

Et annet viktig prinsipp er rendyrking av roller/arbeidsdeling. Barnevernet bør vurdere mulige løsninger for å segmentere/differensiere tilgangene mer enn hva som er situasjonen i dag. Dette for å støtte opp under en bedre arbeidsdeling i fagsystemet og begrense adgang til sensitive menyer / privilegerte rettigheter. Manglende arbeidsdeling kan føre til at brukere har roller som er i konflikt. Det øker også risikoen for utilsiktede/tilsiktede feil.

Det er også generelt viktig å vurdere hvor mange superbrukere som er nødvendig. Det er kun de med reelt behov for denne tilgangen som bør ha den. Ingen bør ha roller som tillater at man både kan autorisere brukere og legge til brukere i systemet. Et høyere antall brukere med privilegerte rettigheter enn nødvendig for daglig drift, vil øke tidligere nevnte risikoer.

Under presenteres et eksempel på hvordan tilgangsgruppene kan organiseres og hvilke tilganger de ulike tilgangsgruppene kan ha:

Figur 5 Eksempel på tilganger - barnevern

Tilgangsmatrise

Tilgangsgruppe	Modul	Tilgang for	Tilgang til å gjøre
Saksbehandler	Klient	Vanlig saksbehandler	Saksbehandleroppgaver
Merkantil botiltak	Klient	Merkantil botiltak	Godkjenne vedtak, utbetalingsplaner
Merkantil	Klient	Merkantil	Saksbehandleroppgaver, merkantile funksjoner, fullmakt til barnevernstjenesten.
Saksbehandler med vedtak	Klient	Saksbehandler (som i dag har superbrukertilgang).	Saksbehandleroppgaver, godkjenne vedtak
Leder (BV leder, BV ass. leder, fagkonsulent)	Klient	Leder med vedtaksfullmakt	Saksbehandleroppgaver, godkjenne vedtak og utbetalinger
Superbruker	SysAdm	Superbruker barnevern (2-3) utnevnte superbrukere	Tilgang til administrasjonsmodulen i Familia: Passord - legge til, endre, passivisere. Plassere brukere i tilgangsgruppe, passivisere bruker, vedlikeholde opplysninger om bruker, endre lokalt kodeverk
Superbruker	SysAdm	Superbruker botiltak	Kodeverk knyttet til botiltak

Kilde: Et eksempel, utarbeidet av Romerike revisjon

Loggføring i Familia

Et annet tiltak er å se på mulighetene for å aktivere utvidet loggføring i fagsystemet og om det eksisterer muligheter for loggføring ved opprettelse, endring og sletting av dokumenter. Loggføringen bør inneholde hvem som har utført handlingen (brukernavn) med dato og tidspunkt for opprettelse, endring og sletting. Tiltaket er ment for å øke sporbarhet, samt redusere risiko for tap av informasjon ved tilsiktede og utilsiktede endringer. Dersom en har mulighet for å se hvem som har opprettet, endret og slettet dokumenter, vil barnevernet lettere kunne spore seg tilbake til de endringer som er gjort og rette opp ved eventuelle feilendringer eller feilslettinger. Barnevernet kan forhøre seg med leverandøren om mulighetene for loggføring i fagsystemet, ut over det som er tilstede i dag.

Det kan også vurderes å aktivere logging over hvem som har sett på ulike journaler i fagsystemet for å oppdage «snoking». Dette kan også virke forebyggende i forhold å hindre at brukere leser saker de ikke er involvert i. Det gjør det også mulig å gjennomføre regelmessig gjennomgang av loggene for å se at alle endringer er berettiget.

6 INFORMASJONSSIKKERHET - GRUNNSKOLEN

Det undersøkes om skoleeier/skolene i Lørenskog ivaretar sentrale krav til personvern og informasjonssikkerhet. Revisjonens funn gjennomgås i punktene 6.2-6.5. I punkt 6.6 følger råd og tips. Revisjonens vurderinger følger i kapittel 7.

6.1 Revisjonskriterier

Revisjonskriteriene er utledet foran i rapporten. De oppsummerte kriteriene gjentas nedenfor:

Problemstilling	Revisjonskriterier
Har skolene ivaretatt sentrale informasjons-sikkerhetskrav?	**Organisering av sikkerhetsarbeidet (personopplysningsforskriften § 2-7)** ➔ Organiseringen av sikkerhetsarbeidet skal beskrives ➔ Informasjonssikkerhetsarbeidet skal baseres på en klar fordeling av roller og ansvar ➔ Fordelingen av roller og ansvar skal være dokumentert. **Risikovurdering** (**personopplysningsforskriften § 2-4)** ➔ Det skal gjennomføres risikovurderinger med jevne mellomrom ➔ Risikovurderingene skal dokumenteres ➔ Resultatet av risikovurdering bør nedfelles i en aktivitetsplan eller lignende ➔ Det skal foreligge en oversikt over personopplysningene som behandles. **Tilgangskontroll (personopplysningsforskriften § 2-5 og § 2-8)** ➔ Det skal være etablert rutiner og praksis for en tilfredsstillende tilgangskontroll i fagsystemet ➔ Det skal gjennomføres holdningsskapende arbeid ➔ Tilgang til informasjon i fagsystemet skal være i samsvar med tjenstlig behov

6.2 Introduksjon

Skoleavdelingen ledes som nevnt i punkt 4.2 av den kommunale skolesjefen. Skolesjefen har et overordnet ansvar for skolene og SFO. Kommunen har sju barneskoler og fire ungdomsskoler. Hver av de kommunale skolene ledes av et lederteam som består av rektor, assisterende rektor og inspektør(er) og ansvaret for klassene er organisert i lærerteam med egne teamledere (strategisk plan 2015-2026). Det er om lag 530 årsverk i grunnskolen i 2015/2016, et driftsbudsjett på 332 millioner kroner i 2015 og 4501 elever[20] i grunnskolen i 2015.

[20] Antall elever i kommunale grunnskoler, vektet (KOSTRA, foreløpige tall for 2015, per 15.3.2016).

Generelt om behandling av personopplysninger i skolen
Skolen behandler og håndterer personopplysninger om elevene og foresatte. Ansatte i skolen har taushetsplikt etter lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven) bestemmelser[21].

I dagens skole tas det gjerne i bruk mange forskjellige kanaler og systemer for å kommunisere med foresatte og elever. Opplysninger om elevene legges igjen flere steder, og med ulik grad av sikkerhet. Datatilsynet (2014) skriver i en samlerapport om personvern i skole og barnehage at tilsynet har sett eksempler på at skoleeier ikke har kjennskap til sikkerhetsaspektene forbundet med elevopplysninger og dermed heller ikke har utarbeidet retningslinjer for eller gitt opplæring i personvern.

Opplysninger om elevenes karakterer, fravær, anmerkninger, faglig progresjon, spesielle undervisningsbehov, atferdsmønstre og sosiale ferdigheter er personopplysninger. Videre betraktes opplysninger om innlevering av og innholdet i elevarbeider, besvarelse på prøver og eksamener, e-postkommunikasjon og andre former for elektroniske meldinger også som personopplysninger (Senter for IKT i utdanningen 2011, 8). Opplysninger om helseforhold og livssynsmessig oppfatning betraktes som sensitive opplysninger. Informasjon om sykdom og diagnoser, for eksempel for elever med lærevansker, betraktes som sensitive. Det samme gjelder informasjon om spesiell tilrettelegging, fravær og vanskelige familie- og hjemmeforhold (ibid, 8).

Fagsystem
Skolene håndterer mange og ulikeartede personopplysninger om elever og deres foresatte. I Lørenskog kommune håndteres noen opplysninger i kommunens sak-/arkivsystem (WebSak Fokus), for eksempel enkeltvedtak om skolestart, spesialundervisning og individuell opplæringsplan (IOP). Andre opplysninger håndteres i elevplattformen i systemet Fronter, for eksempel elevarbeider med tilbakemeldinger, ukeplaner og fravær[22]. Det er ulik bruk fra skole til skole og det er også forskjeller mellom barne- og ungdomsskoler i Lørenskog.

Sats er det skoleadministrative systemet som er under utskifting til fordel for *hypernet for Skole* og dette er en ny web-basert versjon av Sats. Dette nye systemet skal håndtere persondata om elever og foresatte, vitnemål, fravær[23] og klasseadministrasjon. I tillegg skal systemet håndtere fravær blant de ansatte i skolen og overføre lønnsopplysninger (variabel lønn) til kommunens lønns- og personalsystem. Det er i tillegg slik at den nye web-versjonen henter inn eller utveksler data med andre systemer, for eksempel timeplanadministrasjon (NovaSheme), nasjonale prøver (Vokal), prøveadministrasjonssystem (PAS – innregistreringssystem for nasjonale prøver og kartleggingsprøver) samt folkeregisteret.

[21] Forvaltningsloven §§ 13-13e med særregler i opplæringslova om opplysningsplikt til barnevernet og sosialtjenesten.
[22] Fravær i Fronter ut inneværende skoleår.
[23] Fravær i hypernet for Skole fra og med skoleåret 2016/2017.

De ansatte i skolen får tilgangsrettigheter med utgangspunkt i registrerte data om tiltredelse og slutt i personalsystemet, med pålogging via Feide. Feide betyr Felles Elektronisk IDEntitet og er Kunnskapsdepartementets valgte løsning for sikker identifisering i utdanningssektoren[24]. Det opprettes feidepålogging for elevene lokalt på den enkelte skole. Foreldrepålogging i Fronter løses via ID-porten/MinID/BankID.

Fagsystemet Sats har vært tilgjengelig for skolens ledelse og saksbehandler. Lærerne skal få tilganger i *hypernet for Skole* i tillegg til skolens ledelse og saksbehandler. Tilgangene styres fra personalsystemet og feidepåloggingen som administreres på den enkelte skole. Tilgangene skal differensieres ut fra den enkeltes behov.

WebSak Fokus ligger til forskjell fra fagsystemene på det kommunale nettet, på servere i kommunen. Tilgangene er begrenset til skolens ledelse og saksbehandlere.

Kunde- eller sektorkontakten ved IKT-avdelingen har jevnlige møter og samarbeider blant annet med systemeierne for Sats/*hypernet for Skole* og IKT-kontakt for alle fagsystemene i skolen. I tillegg opplyser sektorkontakten at han supporterer brukere av de ulike fagsystemene innenfor skolesektoren når det oppstår problemer om tilgang til systemer eller passord. Til forskjell fra fagsystemet som barnevernet bruker, ligger de ulike fagsystemene i skolen på servere hos leverandørene. IKT-avdelingen har ingen tilganger i fagsystemene, men involveres når tilganger til et fagsystem skal synkroniseres med systemer i kommunen og for å sikre nødvendige integrasjoner mellom ulike systemer i skolen.

Ansatte i skolen må i utgangspunktet registreres korrekt i personalsystemet for å få tilgang til de ulike datasystemene. Ansatt- og sluttdato i personalsystemet er styrende for tilgangene i Active Directory. Feidepåloggingen gir dessuten elev og lærer tilgang til ulike databaser som benyttes i undervisningen, for eksempel Kunnskap.no og ulike spill. Lærer gis dessuten tilgang til Office 365 og mulighet for å skrive og lagre dokumenter.

6.3 Organisering av sikkerhetsarbeidet

I revisjonskriteriene er det lagt til grunn at sikkerhetsarbeidet skal beskrives, baseres på en klar fordeling av roller og ansvar, og denne fordelingen skal være dokumentert. Nærmere om dette i punktene nedenfor.

6.3.1 Organiseringen av sikkerhetsarbeidet skal beskrives

Det er ikke gitt særskilte beskrivelser i stillingsinstruksene for rektor og assisterende rektor som beskriver ansvar eller rolle i forhold til informasjonssikkerhet og personvern. Det samme gjelder også rollene som saksbehandler og IKT-ansvarlig.

[24] Hentet fra www.feide.no/om-feide den 22.3.2016

Både kommunaldirektør for oppvekst og utdanning og skolesjef opplyser til revisjonen at organiseringen av sikkerhetsarbeidet ikke er skriftlig dokumentert fra overordnet hold i kommunen. For øvrig vises til det som fremgår om organiseringen av informasjonssikkerhetsarbeidet i Lørenskog i punkt 4.6. Skolesjefen peker også på at alle ansatte i skolene skal skrive under på taushetserklæring. Dette er nedfelt i skriftlige rutiner og gjelder både nyansatte og vikarer.

Ledelsen ved Løkenåsen skole opplyser at rektor på skolen har hovedansvaret for informasjonssikkerhet og håndtering av personopplysninger, og at ansvaret følger fullmaktshierarkiet på Løkenåsen skole. Det er ikke gitt noen egen beskrivelse av hva som ligger i dette ansvaret, men stillingsbeskrivelsene sier noe om hvilket ansvar man har i de ulike stillingene ved skolen.

Ledelsen ved Rasta barneskole opplyser at det ikke er utarbeidet egen formell policy og retningslinjer for informasjonssikkerhet og håndtering av personopplysninger for Rasta skole, men ledelsen er klare på at ansvaret ligger hos rektor.

6.3.2 Fordeling av roller og ansvar

Behandlingsansvarlig
Kommunen som juridisk enhet er behandlingsansvarlig etter personopplysningsloven, og det vises til tidligere omtale av dette i punkt 4.5 der det framkommer at behandlingsansvaret i praksis er delegert til kommunaldirektør for oppvekst og utdanning. For skolene er ansvaret videredelegert til skolesjefen i dokumentet[25] «Delegasjon av myndighet fra kommunaldirektør for oppvekst og utdanning til virksomhetsleder for skole». Delegeringen er generelt formulert og omfatter etter skolesjefens forståelse behandlingsansvaret for personopplysninger. Det operative behandlingsansvaret eller systemansvaret for de ulike fagsystemene som brukes i skolene, er i praksis delegert videre til den enkelte rektor.

Fordeling av ulike brukerrettigheter
Skolesjefen opplyser at utvalgte personer i dag har tilgang til det skoleadministrative systemet (Sats) og videre at det samme gjelder tilgang til WebSak Fokus. Lærerne har ikke tilgang til Sats eller WebSak Fokus, men de har tilgang til Fronter, spill og kunnskapsverktøy.

Skolesjefen opplyser også at det i forbindelse med overgangen fra Sats til *hypernet for Skole* vil bli laget en struktur på hvem som skal ha ulike tilganger. For eksempel skal følgende prinsipper legges til grunn i denne nye strukturen:

- lærer - tilgang til sin klasse
- elev - tilgang til sin mappe
- foresatte - tilgang til sitt barn.

[25] Skriftlig delegering datert 15. mars 2016

Hypernet for Skole
Oversikten «Hypernet skoleadministrasjon – systemansvarlige» viser at det er to systemansvarlige på kommunenivå for hypernet samt at skolens ledelse er gitt systemansvar på den enkelte skole.

Rektor, assisterende rektor samt undervisningsinspektør(er) og saksbehandler(e) er satt opp som systemansvarlige for hypernet på skolenivå. Antallet varierer fra 3 til 6 på den enkelte skole, alt etter skolenes størrelse. I tillegg er det to systemansvarlige på kommunenivå (25 % stilling på hver). De systemansvarlige på kommunenivå er ansatt som assisterende rektorer på hver sin skole i kommunen.

De systemansvarlige på den enkelte skolen har administratorrettigheter til sin skole. Videre er det slik at de systemansvarlige på kommunenivå er gitt administratorrettigheter for hypernet til alle skolene i kommunen opplyser de systemansvarlige på kommunenivå.

Fronter
IKT-ansvarlig i kommunen for Fronter er gitt administratorrettigheter. IKT-ansvarlig på den enkelte skole er gitt utvidede rettigheter for sin skole.

De systemansvarlige på kommunenivå opplyser at det ikke foreligger noen skriftlig delegering av ansvaret som er lagt til de systemansvarlige.

IKT-ansvarlig på Løkenåsen skole opplyser at hun har ansvar for Fronter på skolen og hun er også systemansvarlig på kommunenivå for dette systemet. Dette innebærer administrasjon av tilganger for ansatte (for eksempel team, kontaktlærere, nullstille passord i de tilfeller det blir glemt) og elevtilganger.

Assisterende rektor som samtidig er IKT-ansvarlig på Rasta skole, administrerer tilganger for ansatte og elever i Fronter. Alle lærere er gitt mulighet til å resette passord på denne barneskolen.

6.3.3 Beskrivelse av sikkerhetsarbeidet, herunder roller og ansvar

Generelt
Ledelsen ved Løkenåsen ungdomsskole opplyser at de har et dokument som omhandler informasjonssikkerhet og personvern: «Plan for informasjonssikkerhet og personvern – Løkenåsen skole». Dokumentet omhandler rutiner for låsing av dører/arkivskap/skap, oppbevaring av dokumenter med sensitive opplysninger, passordbeskyttelse på pc-skjermer og lagring av sensitive opplysninger i lærernettverket. Planen ble utarbeidet i 2005 og den er fremdeles gjeldende. Skolen forholder seg også til retningslinjer for behandling av elevarkiv fra sektorledelsen for oppvekst og utdanning. Dokumentet er fra 2011-2012 og omhandler behandling og lagring av elevmapper.

Det er utarbeidet rutiner og sjekklister for behandling av personopplysninger for den delen av skolen som gjelder «Rastabasen» ved Rasta skole. Dette fordi behovet for tilgang til personopplysninger er større ved denne delen av skolen opplyses i intervjuer med ansatte på skolen.

Ledelsen ved begge skolene opplyser imidlertid at det ikke er utarbeidet en oversikt ved skolen som dokumenterer hvilke systemer som behandler personopplysninger.

Opplæring
Ledelsen ved Løkenåsen ungdomsskole opplyser at alle ansatte undertegner taushetserklæringer og at det gis muntlig informasjon om informasjonssikkerhet og personvern i forbindelse med dette.

Løkenåsen ungdomsskole mangler en beskrivelse av informasjonssikkerhet og personvern som kunne vært gjennomgått ved skolestart hvert år. Likeledes mangler rutiner for å informere vikarer om informasjonssikkerhet og personvern på en ensartet måte. IKT-ansvarlig ved skolen mener videre at det hadde vært hensiktsmessig å innføre dette. Skolens ledelse opplyser på sin side at det informeres om rutiner i forbindelse med skolestart, for eksempel ønsker ledelsen bevissthet om låsing av dører. Videre påpekes at vikarer informeres gjennom taushetserklæringen som de leser og undertegner, og at det også blir gitt muntlig informasjon i forbindelse med dette.

Rasta skole opplyser at det ikke har vært regelmessig opplæring i informasjonssikkerhet og personvern, men den nye ledelsen på skolen ønsker å øke fokus på disse temaene fremover.

Det er også gjennomført opplæring i forbindelse med implementeringen av WebSak Fokus, og skolene opplever at veiledningen[26] de får på dette området er god.

IKT-ansvarlig for Fronter administrerer tilganger for lærere og elever. Hun snakker med alle nye elever i 8. klasse og gjennomgår dataavtale med elevene for å bevisstgjøre de i forhold til sine plikter ved bruk av skolenettet.

Hypernet for Skole
De systemansvarlige på kommunenivå informerer om at det er gjennomført to opplæringsrunder i forbindelse med overgangen til hypernet. I tillegg opplyses at det er gjennomført workshops for ungdomsskolene i forbindelse med enkelte tema. Det har ikke vært spesielt fokus på informasjonssikkerhet ut over at tilgang til personopplysninger bare skal gis til ansatte ut fra tjenstlig behov.

Etterlevelse av rutiner
Det er ikke etablert regelmessige rutiner eller kontroller for å påse at ansatte ved skolene etterlever god skikk i forhold til behandling av personopplysninger og informasjonssikkerhet. Hvis det avdekkes avvik i det daglige, påminner de hverandre om gjeldende regler. Eksempler på dette er å snakke med lukket dør, låse dør/skap og ikke la elevinformasjon ligge tilgjengelig. Både Løkenåsen og Rasta skoler opplyser at det har vært få kjente brudd på dette, og kjente brudd/tyverier ligger en stund tilbake i tid.

[26] Veiledning og tilbakemeldinger i WebSak Fokus gis av dokumentsenteret, en seksjon under teknologiavdelingen (se punkt 4.2.1).

Det er ikke et felles avviksregister i kommunen for registrering av sikkerhetsbrudd eller hendelser, og dette er heller ikke opprettet ved de to skolene.

Oppfølging
Skolesjefen opplyser at personvern kunne vært et tema i skolesjefens vurderingssamtaler med skolene eller i skoleledermøter. Informasjonssikkerhet og personvern har så langt ikke vært fast tema i møter som skolesjefen har med kommunaldirektøren. Videre opplyses at tema tidligere har blitt satt på dagsorden i forbindelse med konkrete hendelser for å minne om sikkerhetsrutiner. Ut over dette er det elektroniske elevarkivet jevnlig tema i skoleledermøter.

Sikring av personopplysninger
Overføring av informasjon mellom administrativt nett og skolenettet
På grunn av skolenes IT-infrastruktur hvor kun ledelse og administrativt personale har tilgang til det administrative nettet i kommunen, hvor blant annet WebSak Fokus ligger, og lærere har tilgang til skolenettet, så er det behov for rutiner for å gi tilgang til informasjon på tvers av nettene. Lærere må ha tilgang til elevinformasjon for å kunne utarbeide blant annet individuelle opplæringsplaner (IOPer) for sine elever. Deretter må IOPene overføres fra lærer til det administrative nettet for lagring i WebSak Fokus. Lærer kan dessuten ha behov for å lese en IOP på et senere tidspunkt for å følge opp eller endre en plan.

Informasjon på tvers av systemene overføres ved bruk av minnepinner. Skolesjefen opplyser at rutinene for bruk av minnepinner kan variere noe fra skole til skole. Skolesjef informerer om at det kan være en minnepinne per elev og at minnepinnene låses inn i skap på skolen og hentes ut ved behov. I tillegg kan det være en minnepinne per klasse.

Rutinene på skolene er slik at minnepinner skal låses ned. Det kan være en minnepinne per elev, eller generelle minnepinner. Det forutsettes at innholdet slettes etter hver gangs bruk når dokumentene (IOP) er overført til WebSak Fokus. Rutinene er ikke skriftlige. Skolene opplyser at det mangler skriftlig utsjekk/innsjekk av minnepinner. Minnepinnene ved skolene er ikke passordbelagt eller kryptert.

Skolenettet
Lærerne er tilknyttet skolenettet. Det varierer mellom skolene hvorvidt lærerne utarbeider IOPer eller andre dokumenter som kan inneholde personopplysninger på egen pc og hva som lagres på «fellesområdet» i Office 365 i skolenettet. Det er ingen kontroll med hva som lagres lokalt på lærernes maskiner på skolene. På «Rastabasen» følger imidlertid baseleder opp, sammen med de ansatte, at det ikke ligger personopplysninger på de ansattes datamaskiner. Passordbytte foretas hver uke for enkelte ansatte på «Rastabasen».

WebSak Fokus og fysisk arkiv
Rektor åpner tilgang i WebSak Fokus til elevmapper for assisterende rektor, undervisningsinspektør samt saksbehandler ved behov. Det fysiske arkivet speiler i dag det elektroniske arkivet i stor grad. Lærernes behov for å se dokumenter i den fysiske elevmappen løses i praksis på kontoret hos

saksbehandler. Hovedregelen er at elevmappen ikke skal tas med ut av kontoret, men det forekommer unntak fra dette. Ved Løkenåsen skole skal elevmapper som tas med ut av kontoret, registreres skriftlig i «lånekort» som ligger igjen i arkivet, og mappene skal tilbake til kontoret samme dag. Ved Rasta skole er det ingen skriftlig registrering i slike tilfeller.

Det opplyses også at mens Rasta skole selv skanner og legger inn dokumenter, er det andre skoler som fysisk oversender dokumenter til dokumentsenteret for skanning inn i WebSak Fokus. Det fysiske elevarkivet er avlåst og det er et begrenset antall som har tilgang til nøkkel.

6.4 Risikovurdering

Det er lagt til grunn i revisjonskriteriene at det skal gjennomføres risikovurderinger, arbeidet skal dokumenteres og resultatet skal synliggjøres i en plan eller lignende.

Kommunaldirektør for oppvekst og utdanning sier i intervju med revisjonen at det er skolesjefen som har ansvar for å gjennomføre risikovurderinger etter personopplysningslovens bestemmelser innenfor skole og deres fagsystem. Som nevnt i punkt 5.4 foreligger det ingen føringer på dette fra sentralt hold i kommunen.

Det skal også foreligge en oversikt over hvilke personopplysninger som behandles. Verken skolesjef eller de utvalgte skolene har utarbeidet en slik oversikt.

Løkenåsen skole har ingen prosess for å gjennomføre årlige risikovurderinger, og det foreligger heller ikke noe om dette fra sentralt hold i kommunen opplyser rektor og assisterende rektor.

Ledelsen ved Rasta skole opplyser at det ikke er dokumentert at det er gjennomført risikovurderinger av personvern og informasjonssikkerhet ved skolen og det er heller ikke gjennomført den siste tiden. Dette er imidlertid nylig tatt opp i interne møter ved skolen, og det er foretatt en foreløpig, kort vurdering som blant annet omfatter bruken av minnepinner og elevmapper.

Hypernet for Skole
De systemansvarlige for fagsystemet på skolenivå mener at det ikke er foretatt noen risikovurderinger innenfor skoleområdet i Lørenskog så langt de kjenner til.

Skolesjefen peker på at fagsystemet *hypernet for Skole* skulle vært tatt i bruk for skolene fra august 2015. Etter en utsettelse i 2015 skulle overgangen skje 1. februar 2016. Videre opplyses at det var usikkerhet rundt hva som forårsaket at fagsystemet ikke virket som forutsatt. Utfordringene som kom da man begynte å ta fagsystemet i bruk, var overraskende. Skolesjefens inntrykk er at IKT-avdelingen kom for sent inn i prosjektet og at oppgraderingen dessuten fant sted etter påtrykk fra leverandøren.

Teknologidirektøren opplyser at IKT ikke ble involvert i det første forsøket på oppgradering. Kompleksiteten med tanke på avhengigheter og integrasjoner ble ikke ivaretatt. Det var ikke dokumentert avhengigheter og løsningen ble ikke i tilstrekkelig grad testet før produksjonssetting.

Ansatte ved IKT-avdelingen mener at «[m]anglende planlegging og testing, samt dårlig koordinering, ga mange feilsituasjoner og forsinkelser underveis. Dette gjaldt både internt i kommunen og hos leverandørene».

6.5 Tilgangskontroll

Det er lagt til grunn i revisjonskriteriene at det skal etableres rutiner og praksis for tilgangskontroll i fagsystemet. I tillegg bør det gjennomføres holdningsskapende arbeid og tilgangene som gis skal være i samsvar med tjenstlig behov.

6.5.1 Etablerte rutiner og praksis for tilfredsstillende tilgangskontroll

Det er ikke utarbeidet skriftlige rutiner for administrering av brukere og rettigheter i forhold til fagsystemene.

Administrering av brukere og rettigheter
I intervjuene opplyses at alle nyansatte gis rettigheter i kommunen på grunnlag av en bestilling (tiltredelsesmelding) når det nye ansettelsesforholdet opprettes. Når ansatte slutter, deaktiveres tilgangen i kommunen på grunnlag av sluttmelding. Den samme rutinen følges ved endringer i arbeidsforhold.

Rektor er autorisert for å be om at det opprettes tilgang til WebSak Fokus for andre brukere enn skolens ledelse. Når ansatte slutter, stenges disse automatisk ute fra det kommunale nettet, mens tilganger som er gitt til mapper i WebSak Fokus fjernes av arkivet.

Både lærere, elever og foresatte må være korrekt registrert i *hypernet for Skole* i utgangspunktet for at de ulike tilgangene skal fungere. Saksbehandler ved skolen har ansvar for å legge inn korrekte data. Det gjennomføres for tiden tester i forbindelse med dette.

Periodisk gjennomgang av brukere
Det er ikke etablert rutiner for regelmessig gjennomgang av brukere og roller i systemene ved de utvalgte skolene. De får heller ikke tilsendt grunnlag fra sentral IKT-avdeling som viser hvilke brukere som har hvilke rettigheter i systemene. Skolene har ikke mulighet til å ta ut disse oversiktene selv.

Loggføring i systemene
Det er ingen rutiner for logging eller oppfølging av logger ved skolene.

6.5.2 Holdningsskapende arbeid

Ledelsen ved skolene informerer om at de ønsker å etablere rutiner for opplæring, informasjon og retningslinjer når det gjelder behandling av personopplysninger. Rektorene mener at bevisstheten om personopplysninger generelt er høy blant de ansatte på skolene.

I intervjuene adresseres flere problemstillinger til revisjonen. Flere etterlyser sentrale retningslinjer og rutiner om personvern og informasjonssikkerhet «slik at man har en ensartet måte å

informere/bevisstgjøre» vikarer og ansatte ved skolestart hvert år. Videre etterlyses økt bevissthet og rutiner når det gjelder e-postkorrespondanse mellom skole og hjem:

> Lærere er nok forholdsvis bevisste på dette i kommunikasjonen med foreldre, men foreldrene refererer jo gjerne til barnet i korrespondansen, slik at den totale korrespondansen kan inneholde sensitive opplysninger.
>
> IKT-ansvarlig ved en skole

Flere etterlyser og savner sentrale retningslinjer fra kommunen med hensyn til håndtering av overgangen fra fysisk til elektronisk arkiv; skal man fortsatt vedlikeholde det fysiske arkivet, og hvor lenge skal dokumenter lagres? Lærernes behov for tilgang til informasjon om elevene, for eksempel IOPer, er det ikke tilrettelagt for i dag. Rutinene er tungvinte og det antas at lærernes behov for innsyn vil øke etter hvert som det elektroniske arkivet tar over mener IKT-ansvarlig ved en skole.

Det kommer også fram at det er behov for å se på rutinene når det gjelder integrasjonen mellom det administrative nettet (WebSak Fokus) og lærer-pc for å sikre tilgjengelighet til data.

6.5.3 Tilganger i samsvar med tjenstlig behov

I intervjuene har revisjonen etterspurt dokumentasjon på gjennomførte tilgangskontroller og utskrift av brukere på sentrale systemer. Revisjonen har ikke mottatt slik dokumentasjon da den ikke foreligger.

Undersøkelsen viser at det er få brukere i skolen som har tilgang til WebSak Fokus, Sats eller *hypernet for Skole* i dag. Det er uttrykt behov for å definere ulike brukerrettigheter i *hypernet for Skole* både for å sikre at lærerne har de tilgangene de skal ha, men også for å ivareta tilstrekkelig informasjonssikkerhet.

6.6 Råd og tips

Nedenfor følger enkelte råd og tips som kommunen som skoleeier og skolene kan se nærmere på i forbindelse med oppfølgingen av denne rapporten. Rådene fra revisjonen er ment som faglig veiledning og er ikke uttømmende eller den eneste måten å løse utfordringer på.

Årshjul

Det bør gjennomføres jevnlige informasjonsmøter og gjøres risikovurderinger. Dette bør skje på sektornivå for å sikre at rutinene blir like på alle skolene. I intervjuene påpekes også viktigheten av å sikre likeartet opplæring og informasjon også til vikarene i skolene. Det kan for eksempel utarbeides et felles årshjul og felles dokumentasjon (malverk og retningslinjer) fra skoleeier som tidfester tidspunkter for gjennomføring av de ulike aktivitetene, for eksempel i form av sentrale informasjonspakker. På denne måten kan man sikre at den enkelte skole vet når det kan forventes at ulike tema tas opp fra skoleeiers side, når møter skal avholdes og skoleeier bør også få et bedre grunnlag for å følge opp arbeidet med personvern og informasjonssikkerhet i tråd med krav i lovgivningen.

E-postkorrespondanse hjem – skole
I intervjuene er det flere som peker på at selv om skolen besvarer en e-post fra en foresatt uten å oppgi elevens navn eller andre personalia, vil e-postkorrespondansen som helhet inneholde denne informasjonen fordi opplysningene står i e-posten fra foresatte. Skolene kan for eksempel løse dette ved å svare med en blank e-post tilbake, noe som er praksis i barnevernet. For øvrig kan det legges til rette for at kommunikasjonen kan foregå via portal for å ivareta tilstrekkelig informasjonssikkerhet. På denne måten kan e-post unngås i framtidig korrespondanse mellom hjem – skole. I tillegg kan det informeres godt om manglende informasjonssikkerhet ved bruk av e-post på foreldremøter og lignende.

Informasjon til foresatte og elever om innsynsrett og samtykke m.m.
Det er viktig at skoleeier og skolene informerer foresatte og elever om hvordan Lørenskog kommune håndterer opplysninger om elevene.

Integrasjon
Revisjonen har fått signaler fra IKT-avdelingen i kommunen om at det vil blir lagt til rette for en integrasjon mellom *hypernet for Skole* og WebSak Fokus slik at dokumenter kan overføres til saksarkivsystemet. Skoleeier må forsikre seg om at fagsystemet tilfredsstiller krav til informasjonssikkerhet og personvern dersom det er tenkt at sensitive personopplysninger vil kunne inngå i dokumenter som utarbeides og mellomlagres i *hypernet for Skole* (for eksempel IOPer).

Den fysiske elevmappen
Et mulig tiltak for økt kontroll med elevmappene er skriftlig inn- og utsjekk av mapper. Undersøkelsen viser at den ene av de to skolene har innført dette.

Utskrifter dokumenter med sensitiv informasjon
Benytte utskriftsordning med «sikker utskrift» slik at den som sender dokumentet til skriveren, selv må bruke kode eller kort for å hente utskriften på papir.

Lærer-pc
Mulige tiltak for økt kontroll kan være å fjerne lærers mulighet til å lagre lokalt på pc, alternativt kryptering av pc eller bruk av terminalserver. Et godt, alternativt internkontrolltiltak til å fjerne muligheten til å lagre lokalt kan være å skape gode holdninger gjennom informasjon for økt bevissthet omkring risikoene ved lagring av sensitive personopplysninger lokalt på pc.

Minnepinner
Minnepinner er i bruk på alle skolene. Rutiner og kontroll med minnepinnene varierer fra skole til skole. Gode tiltak kan være kryptering og passordbeskyttelse samt skriftlig inn- og utsjekk av minnepinnene, og sletterutine for innhold på tidligere brukte minnepinner.

Arkivering og kassasjon
I intervjuene er det også flere som påpeker usikkerhet med hensyn til arkiveringsregler og kassasjon i elevmappene i det fysiske elevarkivet. Det kan tas inn noe om dette i sentrale arkivbestemmelser i Lørenskog kommune, herunder:

- Hvilke dokumenter skal oppbevares for ettertiden i det historiske arkivet?
- Hvilke dokumenter kan slettes, og til hvilken tid?

- Ved overgang til helelektronisk arkiv – skal skolene i tillegg ha et fysisk arkiv som speiler det elektroniske arkivet?

Fødselsnummer
Fødselsnummer består av fødselsdato og personnummer. Skolene kan gjennomgå dagens rutiner og bruke begrepet «fødselsdato» når det er tilstrekkelig.

Databehandleravtaler
Det framgår av det innhentede datagrunnlaget til denne rapporten at det er inngått standard databehandleravtale mellom Lørenskog kommune som behandlingsansvarlig og IST (International Software Technology AS) som databehandler (datert 17.12.2014) og gjelder for *hypernet for Skole*. Selv om databehandleravtaler er holdt utenfor denne revisjonen, vil revisjonen minne om at skoleeier må vite hvem som behandler personopplysninger på deres vegne og etablere nødvendige databehandleravtaler.

Skoleeier må lage databehandleravtale når leverandørene av de ulike nettbaserte tjenestene har tilgang til opplysninger som kan knyttes til en person. «Gjennom personopplysningsloven er den behandlingsansvarlige (skoleeiere) pålagt å inngå databehandleravtaler med hver enkelt leverandør av nettbaserte Feide-tjenester» (Senter for IKT i utdanningen u.d.). Datatilsynet (2015) viser i personvernmeldingen for dette året til at det kan bli uklart hvem som eier elevopplysninger som samles inn av tredjeparter via digitale verktøy.

Skoleeier skal blant annet være kjent med sikkerhetsarbeidet hos de ulike leverandørene som behandler personopplysninger og de skal forsikre seg om at informasjonssikkerheten hos den enkelte leverandør er tilfredsstillende. Skoleeier bør vurdere å hente inn resultater fra ledelsesgjennomganger, sikkerhetsrevisjoner og avviksbehandlinger hos leverandørene for å oppnå dette og ta inn kravet i databehandleravtalene, eksempelvis etterspørre ISAE 3402 Uttalelse om internkontroll i serviceorganisasjoner.

Veiledninger og mer informasjon
Senter for IKT i utdanningen har en rekke veiledninger og informasjon tilgjengelig på sine hjemmesider. «Sikker håndtering av personopplysninger i skolen» er et eksempel på en veiledning fra senteret som tar for seg gjennomføring av risikovurderinger i skolen (Senter for IKT i utdanningen 2011).

Forsvarlig behandling av dokumentasjon er en FOU rapport som KS står bak, og som gir veiledning spesielt med tanke på oppbevaring av sensitiv dokumentasjon i grunnskolen, herunder IOPer (KS 2013). Vedlegg 5 i rapporten inneholder et eksempelskjema på en risikovurdering i den kommune.

7 VURDERINGER, KONKLUSJON OG ANBEFALINGER

7.1 Revisjonens vurderinger

Barnevernet

Revisjonen vurderer det slik at **organiseringen av sikkerhetsarbeidet** knyttet til barnevernet i Lørenskog kommune ikke er tilfredsstillende ivaretatt i henhold til personopplysningslovens bestemmelser. Det foreligger ingen overordnet beskrivelse av hvordan sikkerhetsarbeidet er organisert i kommunen sentralt, eller ved barnevernstjenesten. Revisjonen får inntrykk av at roller og ansvar er forstått både sentralt i kommunen og av barnevernsjefen, men det er ikke utarbeidet dokumentasjon som beskriver denne fordelingen av roller og ansvar.

Revisjonen viser at barnevernet foretar periodiske **risikovurderinger** med utgangspunkt i internkontrollkravene og taushetsplikten i barnevernloven. Risikovurderinger etter de kravene som følger av personopplysningsloven, ivaretas delvis som en følge av kravene i barnevernloven. Risikovurderingen er ikke dokumentert, men det følger av internkontrollen at den gjennomføres årlig og resultatet er nedfelt som tiltak i internkontrolldokumentet. Det er imidlertid begrenset fokus på IKT og informasjonssikkerhet i fagsystemet der personopplysninger lagres og behandles.

Gjennomgangen viser at det foreligger bevissthet til behandlingen av personopplysninger og at ansatte er oppmerksomme angående sikring av personopplysninger, både ved fysisk - og digital lagring. Det er strenge rutiner for fysisk sikring av alle dokumenter som inneholder personopplysninger og dokumentene skal låses inn når de ikke er i bruk av ansatte. I tillegg er det ikke lov til å bruke minnepinner eller eksterne harddisker for lagring av dokumenter digitalt. Tiltaket reduserer risikoen for at personopplysninger skal komme på avveie og at uautoriserte personer skal få tilgang til personopplysninger behandlet av barnevernet. Kravet om at alle ansatte underskriver taushetserklæringer etterleves og alle gjennomgår opplæring ved ansettelse, der også informasjonssikkerhet er et tema. Dette er positivt

Det er etablert rutiner og praksis for tilgangskontroll i fagsystemet Familia. Revisjonen vurderer imidlertid at oversikten over brukere og roller i liten grad er satt opp på en systematisk måte og tilgangene er etter revisjonens vurdering ikke tilfredsstillende med hensyn til god arbeidsdeling og IT-praksis på området. Undersøkelsen viser at flere ansatte er gitt roller som de ikke benytter, eller sjelden bruker. Dette gjelder blant annet flere av superbrukerne. Rollene er ikke fullt ut rendyrket og det er et stort antall superbrukere i fagsystemet. Tilgangen til ansatte bør styres ut fra prinsippet om at en medarbeider kun skal ha tilgang til de roller/funksjoner vedkommende trenger for å utføre sine ordinære arbeidsoppgaver. Muligheten til å administrere brukere og rettigheter i systemet bør også begrenses til et minimum, basert på autorisasjon fra barnevernsjefen.

Det er positivt at inaktive brukere passiviseres[27] og at dette følges opp av den ene fagkonsulenten to ganger i året. Barnevernet burde også inkludere gjennomgang av den enkeltes tilgangsnivå i denne periodiske kontrollen. Periodisk gjennomgang av brukermassen i fagsystemet reduserer risiko for at brukere beholder sine rettigheter etter at de har forlatt virksomheten samt at de gjeldende brukerne har tilganger som ikke er i samsvar med sine arbeidsoppgaver.

Det er det ingen rutiner for logging og oppfølging av logger. Revisjonen mener det er uheldig at dette ikke er innført da det er viktig å følge opp slettinger og forebygge «snoking» i mapper og lignende.

Skolene

Revisjonen vurderer det slik at organiseringen av sikkerhetsarbeidet knyttet til skolene i Lørenskog kommune ikke er tilfredsstillende ivaretatt i henhold til personopplysningslovens bestemmelser. Det foreligger ingen overordnet beskrivelse av hvordan sikkerhetsarbeidet er organisert i kommunen sentralt, eller ved de to utvalgte skolene. Revisjonen får inntrykk av at roller og ansvar er forstått både sentralt i kommunen og ved skolene, men det er ikke utarbeidet dokumentasjon som beskriver denne fordelingen av roller og ansvar.

Gjennom denne revisjonen er det avdekket at mangler rutiner for å gjennomføre regelmessige risikovurderinger, eller for å dokumentere risikovurderingene. Herav følger det at det heller ikke er utarbeidet planer for å definere hvilke risikoreduserende tiltak som bør iverksettes samt ansvar og frister for gjennomføring.

Ved den ene skolen vi besøkte har de nylig brakt risikoanalyser på dagsorden, men disse er ennå ikke dokumentert og satt i system. Etter revisjonens vurdering er det positivt at dette arbeidet er startet.

Verken Lørenskog kommune sentralt, eller skolene, har kunnet fremlegge en oversikt over de personopplysningene som behandles i grunnskolene i kommunen slik personopplysningsloven krever. Revisjonen er av den oppfatning at det generelt er høy kunnskap om hvor personopplysninger behandles og lagres, men dette er ikke dokumentert i henhold til personopplysningens bestemmelser. Ved «Rastabasen» er det imidlertid utarbeidet rutiner for behandling av personopplysninger, da avdelingen også behandler helseopplysninger i det daglige.

Det er et begrenset antall ansatte ved skolene som har tilgang til sensitive personopplysninger om elever og foresatte i det elektroniske arkivet, WebSak Fokus. Det er også etablert rutiner for å sikre urettmessig innsyn i de fysiske arkivene. På grunn av skillet mellom det administrative nettet i kommunen og skolenettet, er det etablert rutiner for å overføre dokumenter mellom lærer-pc og arkivet via minnepinner når det er behov for dette. Det er uttalte rutiner knyttet til minnepinnene, men i praksis har ikke skolene kontroll med hva lærere lagrer på egen pc, og på antallet minnepinner som er i omløp. I dag er det ikke kryptering av harddiskene på lærer-pc, og det er

[27] Passivisering betyr at en tilgang ikke lenger er tilgjengelig. Dette gjelder ansatte som slutter m.m.

heller ikke kryptering av minnepinnene. Dette øker risikoen for at uautoriserte kan få innsyn i personopplysninger dersom en lærer-pc eller minnepinne kommer på avveie. Revisjonen mener dette er en kritikkverdig praksis.

Innføringen av *hypernet for Skole* introduserer nye integrasjoner og dataflyt mellom systemene som benyttes i skolen. Det er ikke gjort noen formell risikovurdering i forbindelse med innføringen. Det er heller ikke utarbeidet rutiner som beskriver hvilke rettigheter lærerne skal ha i *hypernet for Skole*, og hvordan man skal sikre at personopplysninger blir forvaltet i henhold til lovverket.

Kommunen og skolene har ikke etablert rutiner for regelmessig gjennomgang av aktive brukere og deres rettigheter i systemer som behandler og lagrer personopplysninger. Skolene har heller ingen dokumentasjon fra systemene over ansatte med tilhørende tilganger. Dette må de i tilfelle motta fra sentral IKT-avdeling i kommunen.

Skolene holder informasjonsmøter for de ansatte ved skolestart, og har ellers av og til temaer på agendaen som vedrører informasjonssikkerhet og behandling av personopplysninger. Dette er imidlertid ikke satt i system, og blir ad hoc. Det mottas heller ikke veiledning, informasjonsmateriale eller jevnlige påminnelser fra kommunen sentralt på dette området.

Revisjonen vurderer, med unntak av det som er påpekt ovenfor, at holdninger og bevissthet knyttet til informasjonssikkerhet og behandling av personopplysninger ved skolene generelt er god. Revisjonen påpeker likevel at det mangler dokumentasjon og formelle rutiner i henhold til kravene i personopplysningsloven.

7.2 Samlet vurdering og konklusjon

Revisjonens samlede vurdering er at organisering av sikkerhetsarbeidet, risikovurderinger og tilgangskontroller knyttet til barnevern og skoler i Lørenskog kommune ikke er tilstrekkelig i henhold til de kravene som stilles i personopplysningsloven. Dette behøver ikke bety at personopplysninger behandles på en kritikkverdig måte, men det er behov for å styrke etterlevelsen i henhold til personopplysningslovens krav.

Revisjonen understreker at vi ikke har gjennomgått rutiner og praksis for hele kommunen, men gjort undersøkelser som har vært rettet mot barnevern og skole, både sentralt og ved utvalgte virksomheter. Revisjonens vurderinger og anbefalinger som knyttes til kommunens overordnede ansvar, vil imidlertid gjelde for Lørenskog kommune som skoleeier og for hele kommunen.

Revisjonen konkluderer på bakgrunn av den gjennomførte undersøkelsen slik på problemstillingen:

> *De undersøkte virksomhetene har i liten grad ivaretatt informasjonssikkerheten i tråd med kravene i personopplysningsloven.*

7.3 Anbefalinger

Revisjonen oppsummerer i alt 11 punkter som administrasjonen i kommunen bør følge opp. Disse punktene er deretter løftet opp og formulert som en anbefaling til kommunen. Det framkommer i

rapportens punkt 4.5 at det pågår et omfattende prosjekt for *internkontroll* i Lørenskog kommune som blant annet vil omfatte etablering av policyer, retningslinjer og rutiner for informasjonssikkerhet og personvern. Flere av punktene nedenfor må derfor forventes fulgt opp gjennom dette arbeidet.

Oppfølgingspunkter

1. Utarbeide en overordnet beskrivelse av sikkerhetsarbeidet i Lørenskog kommune som definerer organiseringen og fordelingen av roller og ansvar i henhold til personopplysningslovens bestemmelser.
2. Beskrive innholdet i roller og ansvar for informasjonssikkerhet og personvern for de ulike behandlingsansvarlige på alle nivåer, eksempelvis direktører, barnevernsjef og rektorer ved skolene.
3. Utarbeide retningslinjer for gjennomføring av årlige risikovurderinger i virksomheter som behandler personopplysninger.
4. Utarbeide malverk for utførelse av risikovurderinger, og gjennomføre opplæring i virksomhetene om hvordan dette skal gjennomføres, dokumenteres og følges opp.
5. Etablere rutiner for å identifisere hvilke personopplysninger som behandles i kommunen og dens virksomheter. Oversikten må til enhver tid holdes oppdatert. Koordineringen av dette arbeidet bør skje sentralt i kommunen, mens virksomhetene bevisstgjøres på å melde fra om endringer når disse skjer.
6. Utarbeide sentrale veiledninger og informasjonsmateriale som virksomhetene kan benytte for å sette informasjonssikkerhet og personvern på dagsorden i sine virksomheter.
7. Etablere rutiner for regelmessig distribusjon og gjennomgang av oversikter over brukere og deres rettigheter i systemer hvor det behandles personopplysninger i de ulike virksomhetene. Gjennomgangen bør minimum gjennomføres en gang per år, helst oftere.
8. Revidere rollene/rettighetene for brukere av fagsystemet Familia innenfor barnevernet.
9. Innføre kryptering av data og trafikk innenfor sikker sone for fagsystemet Familia.
10. Gjennomgå tilgangsstrukturene for ulike brukergrupper i skolene for å definere hvilke rettigheter ansatte skal ha til de forskjellige systemene. Dette er spesielt viktig i forbindelse med utrullingen av *hypernet for Skole*.
11. Etablere skriftlige rutiner og systemer for dokumenthåndtering uten bruk av lokal lagring på lærer-pc, herunder overføring av dokumenter mellom lærer-pc'er og det administrative nettet, slik at man kan unngå bruken av minnepinner og lagring på lærer-pc.

Revisjonens anbefaling sammenfatter revisjonsrapportens 11 oppfølgingspunkter og er:

Rådmannen må sørge for at kommunen etterlever lovens krav til informasjonssikkerhet ved behandling av personopplysninger, særlig gjelder dette å få på plass internkontroll i henhold til krav i forskriften til personopplysningsloven.

LITTERATUR- OG KILDEHENVISNINGER

Lov og forskrift

Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

Forskrift 15. desember nr. 1265 om behandling av personopplysninger (personopplysningsforskriften).

Andre kilder

Barne- og familiedepartementet. «Barnevernet og taushetsplikten, opplysningsretten og opplysningsplikten.» *Rundskriv Q-24.* Mars 2005.

Datatilsynet. *En veiledning om internkontroll og informasjonssikkerhet.* veileder, Oslo: Datatilsynet, 2009.

—. «Hva er personvern?» *Personvern på 1-2-3.* 2014. https://www.datatilsynet.no/personvern/Hva-er-personvern/ (funnet januar 18, 2016).

KS. «Forsvarlig behandling av dokumentasjon.» KS FOU 124020, 2013.

Normann, Rolf Sture, og Tommy Tranvik. *Personvern og informasjonssikkerhet i kommunen. En håndbok i risikovurdering.* Oslo: Kommuneforlaget , 2012.

Senter for IKT i utdanningen. *Databehandleravtale for Feide-tjenester.* Oslo, u.d.

Senter for IKT i utdanningen. «Sikker håndtering av personopplysninger i skolen.» Veiledning, 2011.

Wessel-Aas, Jon. «Personvern i Grunnloven.» 23 mai 2014. http://www.uhuru.biz/?p=1491&print=0 (funnet desember 9, 2015).

FIGURER OG TABELLER

Figur 1 Administrativ organisering 11
Figur 2 Sektor oppvekst og utdanning 12
Figur 3 Teknologiavdelingen 13
Figur 4 Organisasjonskart barnevernet 18
Figur 5 Eksempel på tilganger - barnevern 28

Tabell 1 Test av tilganger 26

VEDLEGG – RÅDMANNENS HØRINGSUTTALELSE

Romerike revisjon IKS
Ringveien 4
2050 JESSHEIM

Saksbehandler: Sidsel Nordhagen **Direkte telefon: 67934011**

Deres ref.:

Vår ref.: 15/10736 - 14/16/26969 **Klassering:** FE - 060, FA - X20 **Dato: 01.06.2016**

Høringsbrev foreleggelserapport etter forvaltningsrevisjon informasjonssikkerhet for barnevern og skole

Rådmannen i Lørenskog kommune viser til brev om foreleggelse av rapport etter forvaltningsrevisjon informasjonssikkerhet – personopplysninger i barnevern og skole. Rådmannen har lest rapporten og er inneforstått med rapportens innhold.

Rådmannen anser rapporten som svært nyttig i arbeidet med å forbedre informasjonssikkerheten i Lørenskog kommune, og er tilfreds med at den behandler komplekse forhold med et lettfattelig og forståelig språk.

Slik rådmannen leser rapporten, gir den et bilde av at Lørenskog kommunes ansatte innen skole og barnevern har et aktivt og godt forhold til informasjonssikkerhet, men at det mangler sentrale føringer og skriftlighet knyttet til dette. Dette er en beskrivelse som rådmannen kjenner seg igjen i. Rådmannen slutter seg til anbefalingene som revisjonen gir i rapporten og vil arbeide med å iverksette tiltak i tråd med disse.

Revisjonens anbefalinger vil bli lagt til grunn for videre arbeid med informasjonssikkerhet, og Lørenskog kommune vil følge opp arbeidet i det pågående prosjektet innen internkontroll. Gjennom dette prosjektet vil kommunen reetablere rutiner/prosedyrer innen informasjonssikkerhet og vil også beskrive roller og ansvar innen arbeidet med informasjonssikkerhet både sentralt i kommunen og i sektorene. Det vil også bli innført rutiner og verktøy for risikovurderinger samt avvikshåndtering. Et annet prosjekt, Lørenskogs digitale grunnmur, vil gå gjennom og etablere nye løsninger for tilgangsstyring og brukerhåndtering. Her vil blant annet revisjonens oppfølgingspunkter inngå som krav til løsningene.

Det pågår også arbeid med å definere roller og ansvar mellom den relativt nyetablerte teknologiavdelingen og sektorene innen arbeid med IKT. Dette arbeidet påvirkes også av revisjonens rapport, eksempelvis innen beskrivelsen av oppgraderingen av Hypernet. IKT-porteføljen i Lørenskog kommune er kompleks og med mange avhengigheter mellom ulike fag- og støttesystemer. Kartlegging av disse, samt avklaring av roller og ansvar, er under arbeid i samarbeid mellom teknologiavdelingen og sektorene.

Oppfølgingspunktene som revisjonen peker på er omfattende, og det må påregnes å vare ut 2017 for å lukke disse punktene.

Med hilsen

Ragnar Christoffersen
Rådmann

Sidsel Nordhagen
teknologidirektør

Dette dokumentet er elektronisk godkjent og sendes uten signatur.