Rapport

MOSS KOMMUNE

22.12.2021

Forvaltningsrevisjon
INFORMASJONSSIKKERHET - OG PERSONVERN I MOSS KOMMUNE

Innhold

1 SAMMENDRAG

Revisjonens fremgangsmåte

BDO har valgt å løse temaet som kontrollutvalget ønsket undersøkt ved å gjennomføre en forvaltningsrevisjon i tråd med «Standard for forvaltningsrevisjon» (RSK 001/god revisjonsskikk), samt å følge Østre Viken kommunerevisjons (ØVKR) egen mal for forvaltningsrevisjoner. Som et ledd i etterlevelse av RSK 001 har det vært en dedikert ressurs med ansvar for å kvalitetssikre at standarden følges av revisjonslaget. I tillegg har revisjonslaget hatt dialog med både ØVKR og Moss kommune om gjennomføringen av revisjonen.

Fremdriftsplanen har bestått av følgende faser med tilhørende aktiviteter:

- Planlegging
    - Oppstartsmøter (06.09.2021 & 21.09.2021).
    - Forankring av revisjonskriterier hos ØVKR.
    - Oppstartsbrev, informasjonsinnhenting og oversendelse av revisjonskriterier.
- Gjennomføring
    - Analyse av dokumenter og forespørsel om ytterlige dokumentasjon.
    - Gjennomføring av intervju og spørreundersøkelse.
    - Gjennomføring av penetrasjonstest.
    - Beskrivelse av datagrunnlag.
    - Analyse, vurdering og konklusjon.
- Sluttføring
    - Utarbeidelse av rapport.
    - Verifisering av faktagrunnlag fra Moss kommune.
    - Fullstendig rapportutkast er presentert for kommunen.
    - Kvalitetssikring hos ØVKR.
    - Endelig rapport, inkludert kommunedirektørens uttalelse, oversendes til ØVKR.

Revisjonskriterier

Revisjonskriterier er en samlebetegnelse for de krav eller forventninger som brukes som grunnlag for å vurdere kommunens virksomhet. Revisjonskriterier fastsettes normalt med basis i autoritative kilder. Kommunens egne retningslinjer kan også utgjøre revisjonskriterier. Fakta, omtalt som revisjonsbevis vurderes opp mot revisjonskriteriene, og disse vurderingene danner grunnlaget for de konklusjoner som trekkes.

Prosjektet har tatt utgangspunkt i følgende kilder for utledning av revisjonskriterier:

- Lov om kommuner og fylkeskommuner (Kommuneloven)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) - (FOR-2004-06-25-988)
- ISO/IEC 27001:2013 Ledelsessystemer for informasjonssikkerhet (heretter omtalt som ISO/IEC 27001)
- ISO/IEC 27701:2019 Utvidelse av ISO/IEC 27001 og ISO/IEC 27002 for håndtering av personverninformasjon (heretter omtalt som ISO/IEC 27701)
- Digitaliseringsdirektoratet (2020) *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner, Kunnskapsgrunnlag – En dokumentstudie*
- https://internkontroll-infosikkerhet.difi.no/

Revisjonens funn og konklusjoner

Problemstilling 1
Moss kommune har i noen grad etablert et tilfredsstillende styringssystem for personvern.

Moss kommune har etablert flere av elementene som et styringssystem typisk består av, men det bærer preg av at kommunen ikke er i mål ennå. Flere av dokumentene er ikke ferdigstilt og flere av tiltakene som er beskrevet er ikke gjennomført i praksis. Dette gjelder særlig kontrolltiltak. Kommunen har heller ikke utarbeidet en fullstendig protokoll over behandlingsaktiviteter som tilfredsstiller kravene i GDPR artikkel 30 eller gjennomført dokumenterte risikovurderinger av behandlingsaktivitetene. Dette medfører at kommunen ikke kan påvise at tiltakene som er planlagt og/eller iverksatt, er basert på behandlingenes art, omfang, formål og sammenhengen de utføres i, samt risikoene som kommunen står overfor, jf. GDPR artikkel 24. Det er også en gjennomgående utfordring at kommunens rutiner og retningslinjer beskriver hvilke oppgaver som skal gjøres, men ikke hvordan ansatte og ledere skal gå frem for å utføre disse oppgavene. Dette er særlig utfordrende når ansvaret i Moss kommune er delegert til linjeledere og det er gitt tilbakemeldinger om at linjelederne mangler kompetanse til å utøve dette ansvaret. I tillegg er det gitt tilbakemelding om at kommunen ikke sikrer god nok opplæring for linjeledere innen personvern.

Revisjonslaget vil bemerke at Moss kommune gir inntrykk av å være en kommune som er forholdsvis modne på personvernområdet. Kommunen har iverksatt flere gode tiltak og de har en god plan for hvordan de skal arbeide med å etterleve kravene i personvernlovgivningen fremover. Dersom kommunen lykkes med å gjennomføre de planlagte aktivitetene, vil kommunen ha sikret et godt styringssystem på personvern etter revisjonslagets vurdering.

Revisjonen har gjort følgende vurderinger opp mot revisjonskriteriene:

Nr.	Revisjonskriterier	Funn
1.1	Moss kommune har i noen grad etablert tiltak for å sikre at personvernprinsippene etterleves	
1.2	Moss kommune har i noen grad etablert tiltak for å sikre at alle behandlingsaktiviteter har et lovlig behandlingsgrunnlag	
1.3	Moss kommune har i stor grad etablert tiltak for å sikre at vilkårene for samtykke ivaretas	
1.4	Moss kommune har i liten grad etablert tiltak for å sikre at særlige kategorier av personopplysninger kun behandles når det er lov i henhold til GDPR artikkel 9	
1.5	Moss kommune har ikke etablert tiltak for å sikre at fødselsnummer og andre entydige identifikasjonsmidler kun behandles når det foreligger et saklig behov	
1.6	Moss kommune har i noen grad etablert tiltak for å ivareta informasjonsplikten overfor registrerte	
1.7	Moss kommune har i noen grad etablert tiltak for å sikre at den registrertes rett til innsyn ivaretas	
1.8	Moss kommune har i liten grad etablert tiltak for å sikre at den registrertes rett til retting ivaretas	
1.9	Moss kommune har i liten grad etablert tiltak for å sikre at den registrertes rett til sletting ivaretas	

1.10	Moss kommune har i noen grad etablert tiltak for å sikre at den registrertes rett til begrensing ivaretas	
1.11	Moss kommune har i noen grad etablert tiltak for å sikre at den registrertes rett til dataportabilitet ivaretas	
1.12	Moss kommune har i noen grad etablert tiltak for å sikre at den registrertes rett til protest ivaretas	
1.13	Moss kommune har i noen grad etablert tekniske og organisatoriske tiltak for å sikre og påvise at kommunens behandlinger utføres i samsvar med personvernforordningen	
1.14	Moss kommune har i noen grad etablert tiltak for å ivareta krav til innebygd personvern og personvern som standardinnstilling	
1.15	Moss kommune har ikke etablert tiltak som sikrer at de avdekker eller følger opp felles behandlingsansvar	
1.16	Moss kommune har i noen grad etablert tiltak for å sikre at databehandlere gir tilstrekkelige garantier for å ivareta krav til personvern	
1.17	Moss kommune har i svært stor grad etablert tilstrekkelige tiltak for å sikre at det inngås databehandleravtaler	
1.18	Moss kommune har i liten grad sørget for å utarbeide en fullstendig protokoll over behandlingsaktiviteter	
1.19	Moss kommune har i liten grad gjennomført risikovurderinger av kommunens behandlingsaktiviteter	
1.20	Moss kommune har i noen grad etablert tiltak for å oppnå egnet sikkerhetsnivå	
1.21	Moss kommune har i svært stor grad tiltak for å sørge for at avvik blir håndtert	
1.22	Kommunen har i noen grad etablert tiltak for å sikre at personvernkonsekvensvurderinger gjennomføres når det er påkrevd	
1.23	Kommunen har i noen grad etablert tiltak for å sikre at behovet for å gjennomføre personvernkonsekvensvurderinger dokumenteres	
1.24	Moss kommune har i svært stor grad utpekt et personvernombud	
1.25	Moss kommune har i stor grad sørget for at personvernombudet kan utføre sine lovpålagte oppgaver	
1.26	Moss kommune har i stor grad sørget for å sikre personvernombudets uavhengighet	
1.27	Moss kommune har i noen grad sørget for å sikre at personopplysninger overføres i tråd med kravene i GDPR artikkel 44-50	
1.28	Moss kommune har i noen grad sikret at mål og overordnede rammer for behandling av personopplysninger beskrives	
1.29	Moss kommune har i liten grad sikret at nødvendige rutiner og retningslinjer for behandling av personopplysninger utarbeides basert på en risikovurdering	
1.30	Moss kommune har i noen grad basert sitt styringssystem på personvern på anerkjente standarder	

Problemstilling 2
Moss kommune har i noen grad sikret at de ansatte etterlever rutinene til kommunen på personvernområdet.

Revisjonslaget ønsker å fremheve at Moss kommune har et høyt fokus på personvern, både på ledelsesnivå og nedover i organisasjonen. Revisjonslaget har imidlertid avdekket at Moss kommune ikke har lykkes helt med å sørge for at ansatte er kjent med rutiner og retningslinjer for personvern eller med opplæring av både ledere og ansatte. Kommunen er heller ikke helt i mål med å kontrollere at rutinene og retningslinjene faktisk etterleves i praksis. Revisjonslaget vil likevel bemerke at Moss kommune selv er klar over disse avvikene og at de arbeider med å utbedre dem.

Revisjonen har gjort følgende vurderinger opp mot revisjonskriteriene:

Nr.	Revisjonskriterier	Funn
2.1	Moss har i noen grad gjennomført tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen.	
2.2	Moss kommune har i noen grad sikret at styringssystemet for personvern integreres i kommunens prosesser og kommuniseres til kommunens ansatte.	
2.3	Moss kommune har i liten grad etablert tiltak for å sørge for opplæring av de ansatte for å sikre at de er i stand til å etterleve rutiner og retningslinjer.	
2.4	Moss kommune har i stor grad etablert et avvikssystem	

Problemstilling 3
Moss kommune har i noen grad etablert et tilfredsstillende styringssystem (internkontroll) for informasjonssikkerhet.

Moss kommune har et godt system for avvikshåndtering, mål for arbeidet med informasjonssikkerhet samt en detaljert og oversiktlig beredskapsplan.

Revisjonen har gjort følgende vurderinger opp mot revisjonskriteriene:

Nr.	Revisjonskriterier	Funn
3.1	Moss kommune har i noen grad etablert et styringssystem på anerkjente standarder	
3.2	Moss kommune har i stor grad etablert mål og sikkerhetsstrategi for informasjonssikkerhet	
3.3	Moss kommune har i noen grad definert roller og ansvar for informasjonssikkerhet	
3.4	Moss kommune har i liten grad gjennomført risikovurderinger knyttet til informasjonssikkerhet	
3.5	Moss kommune har i stor grad et etablert system for avvik	
3.5	Moss kommune gjennomfører ikke sikkerhetsrevisjoner, men har i noen grad andre kontroller knyttet til informasjonssikkerhet	
3.6	Moss kommune har i stor grad etablert en beredskapsplan og øvelser	

Problemstilling 4

Moss kommune har i liten grad sikret at styringssystemet for informasjonssikkerhet er blitt integrert i kommunenes prosesser og kommunisert til kommunenes ansatte. Kommunen har sørget for at de ansatte har signert taushetserklæring, samt at alle som er tiltenkt en rolle i krisehåndteringen i stor grad har tilstrekkelige kvalifikasjoner.

Revisjonen har gjort følgende vurderinger opp mot revisjonskriteriene:

Nr.	Revisjonskriterier	Funn
4.1	Moss kommune har i liten grad sikret at styringssystemet for informasjonssikkerhet integreres i kommunens prosesser og kommuniseres til kommunens ansatte	
4.2	Moss kommune har i stor grad et system for opplæring som sikrer at alle som er tiltenkt rolle i krisehåndteringen har til-strekkelige kvalifikasjoner	
4.3	Moss kommune har i svært stor grad sørget for at hver ansatt har signert taushetserklæring	

Revisjonens anbefalinger

Personvern	Informasjonssikkerhet
1. Har Moss kommune etablert et tilfredsstillende styringssystem (internkontroll) for personvern?	Basert på revisjonslagets vurderinger og konklusjon anbefaler vi at kommunen bør: • Prioritere arbeidet med å utarbeide en fullstendig protokoll over behandlingsaktiviteter. • Gjennomføre og dokumentere risikovurderinger av kommunens behandlingsaktiviteter. • Ferdigstille og utarbeide nødvendig dokumentasjon i styringssystemet. I Kommunen bør særlig ferdigstille styrende dokumentasjon for personvern, utarbeide tydelige rutiner for å håndtere anmodninger om håndheving av de registrertes rettigheter og utarbeide en rutine for hvilke krav linjeledere må ta hensyn til ved oppstart eller endring av behandlingsaktiviteter. • Gjennomføre kontrolltiltak, herunder ledelsens gjennomgang og internrevisjon. • Tydeliggjøre ansvarsfordelingen på personvern og hva dette ansvaret innebærer. • Gjennomføre målrettet og regelmessig opplæring av linjeledere.
2. Har kommunen sikret at de ansatte etterlever rutinene på området?	Basert på revisjonslagets vurderinger og konklusjon anbefaler vi at kommunen bør: • Fortsette arbeidet med å utarbeide et opplæringsprogram for nyansatte som inkluderer personvern. • Gjennomføre målrettet og regelmessig opplæring av både ledere og ansatte. • Sikre at alle kommunalområdene etablerer kvalitetsutvalg. • Gjennomføre kontrolltiltak, herunder ledelsens gjennomgang og internrevisjon.

Informasjonssikkerhet	
3. Har Moss kommune etablert et tilfredsstillende styringssystem (internkontroll) for informasjonssikkerhet?	Basert på revisjonslagets vurderinger og konklusjon anbefaler vi at kommunen bør: • Ha ytterligere kompetanseheving av nøkkelpersoner innen ISO/IEC 27001 for å kunne basere styringssystemet på standarden. • Godkjenne, implementere og kommunisere styrende dokumenter for styringssystemet. • Arbeide aktivt med kommunikasjon av kommunens retningslinjer på tvers og nedover i kommunen. • Gjennomføre ytterligere formelle kompetansehevende tiltak blant kommunens ansatte. • Ha en systematisk tilnærming til risikostyring knyttet til informasjonssikkerhet. • Gjennomføre og dokumentere kontrolltiltak, herunder sikkerhetsrevisjoner og ledelsens årlige gjennomgang (for øverste ledelse i kommunen).
4. I hvilken grad har de ansatte kjennskap til kommunens retningslinjer og rutiner for informasjonssikkerhet?	Basert på våre vurderinger og konklusjon anbefaler vi at kommunen bør: • Spesifisere roller og ansvar for informasjonssikkerhet i sine styrende dokumenter. • Gjennomføre regelmessig og omfattende program for opplæring innen informasjonssikkerhet. • Sørge for dokumenterte rutiner på kommunikasjon til sine ansatte. • Gjennomføre beredskapsøvelser på hendelser knyttet til informasjonssikkerhet.

2 PROSJEKTMANDAT

Revisjonen skal i henhold til kommuneloven § 24-2 (1) utføre forvaltningsrevisjon. Etter loven innebærer forvaltningsrevisjon å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Østre Viken kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med god kommunal revisjonsskikk. God kommunal revisjonsskikk er å følge RSK 001; Standard for forvaltningsrevisjon, utarbeidet av Norges kommunerevisorforbund (NKRF). Dette innebærer blant annet at rapporten skal skille klart mellom hva som er innsamlet data og hva som er revisjonens vurderinger. Det skal være en tydelig sammenheng mellom problemstillinger, faktaopplysninger[1], vurderinger, konklusjoner og eventuelle anbefalinger. Etter kommuneloven skal revisor rapportere resultatene av sin revisjon til kontrollutvalget.

Forvaltningsrevisjonen er gjennomført på bakgrunn av plan for forvaltningsrevisjon vedtatt i kommunestyret i Moss kommune i sak 20/20 (13.02.2020)

Plan for gjennomføring av forvaltningsrevisjonen ble vedtatt i kontrollutvalget 14.06.2021.
Planen ble vedtatt i tråd med revisjonens forslag. Kontrollutvalget ønsker at det også blir gjennomført en systemtest av kommunens systemer.

Forvaltningsrevisjonen er gjennomført etter vedtatt prosjektplan i tidsrommet juni til desember 2021. Vi har gjennomført oppstartsmøte med kommuneadministrasjonen slik at også administrasjonens innspill er tatt hensyn til.

Vi har kvalitetssikret faktagrunnlaget underveis, både gjennom verifisering av intervjuer og intern kvalitetssikring. I tillegg er rapportens faktaopplysninger i sin helhet verifisert av kommunen, slik at eventuelle feil eller misforståelser er rettet opp. Revisjonen avholdt avsluttende møte med administrasjonen 11.11.21 hvor revisjonens vurderinger, konklusjoner og anbefalinger ble gjennomgått. I etterkant av møtet er rapporten sendt på høring til kommunedirektøren. Kommunedirektørens uttalelse fremgår på side 62.

Forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Dagfinn Buset, Arnt Olav Laueng Aardal og Inger-Johanne Weidel. Casper Støten er oppdragsansvarlig revisor. Revisorenes habilitet og uavhengighet er vurdert opp mot kommunen og den undersøkte virksomheten, og revisjonen finner de habile til å utføre forvaltningsrevisjonen.

Revisor vil takke kontaktpersonen og andre som har deltatt i forvaltningsrevisjonen, for godt samarbeid i forbindelse med gjennomføringen.

Østre Viken kommunerevisjon IKS
Rolvsøy, 22. desember 2021

Casper Støten (sign.)
oppdragsansvarlig revisor

Dagfinn Buset (sign.)
utførende forvaltningsrevisor

Arnt Olav Laueng Aardal (sign.)
utførende forvaltningsrevisor

Inger-Johanne Weidel (sign.)
utførende forvaltningsrevisor

[1] Fakta er en gjengivelse av informasjonen vi har fått tilgang til gjennom datainnsamlingen.

3 FREMGANGSMÅTE

3.1 Problemstillinger og avgrensninger

Revisjonslaget har tatt for seg følgende problemstillinger:

Personvern	Informasjonssikkerhet
1. Har Moss kommune etablert et tilfredsstillende styringssystem (internkontroll) for personvern?	3. Har Moss kommune etablert et tilfredsstillende styringssystem (internkontroll) for informasjons-sikkerhet?
2. Har kommunen sikret at de ansatte etterlever rutinene på området?	4. I hvilken grad har de ansatte kjennskap til kom-munens retningslinjer og rutiner for informasjons-sikkerhet?

For å besvare de fire revisjonskriteriene har revisjonslaget utledet revisjonskriterier for å besvare disse.

3.2 Om revisjonskriterier

I henhold til forskrift om kontrollutvalg og revisjon § 15 skal revisor fastsette revisjonskriterier for den enkelte forvaltningsrevisjon. Revisjonskriterier er en samlebetegnelse for de krav eller forventninger som brukes som grunnlag for å vurdere kommunens virksomhet. Revisjonskriteriene etablerer den norm som de innsamlede dataene skal vurderes opp mot. I tillegg til dette skal revisjonskriteriene også gjøre det tydelig for den reviderte enhet hva de måles opp mot. Revisjonskriteriene klargjør også overfor folkevalgte, media og andre lesere av forvaltningsrevisjonen hva revisors vurderinger bygger på. Dette vil gjøre det enklere å etterprøve revisors vurderinger. Revisjonskriteriene skal være relevante, konkrete og i samsvar med de kravene som gjelder for revidert enhet.

Revisjonskriterier fastsettes normalt med basis i autoritative kilder. Fakta, omtalt som revisjonsbevis vurderes opp mot revisjonskriteriene, og disse vurderingene danner grunnlaget for konklusjoner som trekkes.

Prosjektet har tatt utgangspunkt i følgende kilder for utleding av revisjonskriterier:

- Lov om kommuner og fylkeskommuner (Kommuneloven)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) - (FOR-2004-06-25-988)
- ISO/IEC 27001:2013 Ledelsessystemer for informasjonssikkerhet (heretter omtalt som ISO/IEC 27001)
- ISO/IEC 27701:2019 Utvidelse av ISO/IEC 27001 og ISO/IEC 27002 for håndtering av person-verninformasjon (heretter omtalt som ISO/IEC 27701)
- Digitaliseringsdirektoratet (2020) *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner, Kunnskapsgrunnlag – En dokumentstudie*
- https://internkontroll-infosikkerhet.difi.no/

3.3 Revisjonsmetoder

I henhold til god revisjonsskikk skal praksis eller tilstand innen det reviderte området beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner. Revisjonslaget har benyttet ulike revisjonsmetoder for å besvare revisjonskriteriene samt for å sikre høyest mulig grad av gyldighet og pålitelighet.

Utfordringer og begrensninger i rapportens faktagrunnlag beskrives nedenfor sammen med beskrivelsen av de ulike metodene som er benyttet. Vi tar også hensyn til metodens begrensninger i vurderingene.

I denne forvaltningsrevisjonen er informasjonen hentet inn gjennom bruk av følgende metoder:

- Dokumentanalyse.
- Intervjuer.
- Spørreundersøkelse.
- Penetrasjonstest.

Dokumentanalyse

Vi har gjennomgått sentrale dokumenter på området. Dokumentene er oversendt fra kommunen/hentet ut fra kommunens kvalitetssystem. Fullstendig oversikt over dokumentene fremgår av kildehenvisningene i kapittel 8.

Intervjuer

Det er totalt gjennomført 23 intervjuer av 21 intervjuobjekter for å sikre at nøkkelpersoner knyttet til personvern og informasjonssikkerhet har blitt inkludert i prosessen.

Alle intervjuer er verifisert. Det betyr at alle intervjuobjekter har hatt anledning til å lese gjennom referatet i etterkant av intervju for å bekrefte at referatet er i overenstemmelse med det som ble sagt under intervjuet. Videre har dette bidratt til å rette opp eventuelle misforståelser.

Spørreundersøkelse

Det ble sendt ut en spørreundersøkelse til alle ansatte i Moss kommune i henhold til e-postliste som ble oversendt revisjonslaget av Moss kommune. Undersøkelsen er gjennomført ved hjelp av det nettbaserte spørreundersøkelsesverktøyet Feedback.

Feedback er et verktøy for spørreundersøkelser som er utarbeidet av BDO. Spørreundersøkelsen besto av ni spørsmål, med et ekstra spørsmål betinget på hva brukeren svarte på ett av spørsmålene. Formålet med spørreundersøkelsen var å kartlegge de ansatte i Moss kommune sine oppfattelser og inntrykk av rutinene for internkontroll innen personvern og informasjonssikkerhet.

Det var to hovedutfordringer som oppsto etter utsendelse av spørreundersøkelsen: 1) en teknisk feil førte til at en spesifikk svarkombinasjon resulterte i at brukeren ikke fikk muligheten til å levere inn sin besvarelse. Denne feilen ble fanget opp av det tekniske teamet bak Feedback i BDO, og rettelse av feilen ble gjort umiddelbart. BDO ble også informert om feilen av ledelsen i Moss kommune som hadde fått flere henvendelser av brukere. Feilen kan ha medført at enkelte ikke fikk levert besvarelse, som kan ha medført noe lavere svarprosent på undersøkelsen. Imidlertid vil ikke feilen ha medført noen ytterligere påvirkning på faktagrunnlaget annet enn noe lavere svarprosent totalt sett. Den andre feilen innebar to upresise formuleringer i spørreskjema vedrørende ansiennitet i kommunen. Feilen medførte at enkelte brukere ble usikre på hva de skulle svare samt at alternativene knyttet til opplæring ikke var tilstrekkelig dekkende. Førstnevnte har ikke hatt betydning for faktagrunnlaget og påfølgende analyser

som revisjonen bygger sine vurderinger på, da svar fra de andre spørsmålene ikke ble koblet opp mot ansiennitet som det opprinnelig var planlagt for. Spørsmålet knyttet til opplæring kan ha hatt innvirkning på faktagrunnlaget. Basert på tilbakemelding var det enkelte ansatte som ville besvart «Ja, men ikke med faste intervaller» (heretter omtalt som alternativ fire), dersom det hadde vært et svaralternativ. Revisjonslaget har valgt å benytte funn fra spørsmål om opplæring som et supplement til andre revisjonskilder (intervju og dokumentgjennomgang). Revisjonslaget vil påpeke at svarfordelingen trolig ville vært påvirket dersom alternativ fire var inkludert. Imidlertid, ville alternativ fire ikke gitt et bedre grunnlag for å vurdere hvorvidt Moss kommune arbeider systematisk med opplæring da det er andre revisjonskilder som har vært benyttet for å vurdere nettopp dette.

Spørreundersøkelsen ble sendt ut til 5286, hvorav 1188 fullførte undersøkelsen. Det var 25,98% av de 5286 respondentene som åpnet spørreundersøkelsen uten å fullføre. Det er uvisst hvor i spørreundersøkelsen respondentene har valgt å avbryte. Noen mulige årsaker knyttet til at enkelte respondenter ikke fullførte kan være den tekniske feilen med innsendelse av undersøkelsen som nevnt ovenfor. Til tross for at undersøkelsen kun er på én side kan respondentene ha opplevd den som for lang. En annen årsak kan være at respondentene ikke har ansett undersøkelsen som viktig eller obligatorisk.

Penetrasjonstest

Revisjonslaget gjennomførte en penetrasjonstest som et tillegg til denne revisjonsrapporten. Hensikten med penetrasjonstesten var å undersøke hvor sikre kommunens IT-systemer er mot uautorisert inntrengning. Helhetlig rapport fra penetrasjonstesten vil presenteres i eget vedlegg.

3.4 Forhold som kan ha påvirket Moss kommunes arbeid med informasjonssikkerhet og personvern

Revisjonslaget er innforstått med at Moss kommunes aktiviteter knyttet til informasjonssikkerhet og personvern har vært påvirket av håndteringen av covid-19 pandemien, og har derfor forståelse for eventuelle utsettelser dette har forårsaket.

3.5 Skala og symbolbruk for vurdering av funn

I tilknytning til evalueringen av revisjonsbevisene opp imot hvert enkelt revisjonskriterium benyttes symboler som uttrykk for vår oppfatning av resultatet av gjennomgangen (funn). Symbolbruken og beskrivelsen av disse illustreres i figur 1 nedenfor.

	Avdekkede forhold oppfyller ikke revisjonskriteriet. Det er avdekket vesentlige forbedringspotensial som bør gis høy prioritet.
	Avdekkede forhold oppfyller i liten grad revisjonskriteriet. Det er avdekket vesentlige forbedringspotensial.
	Avdekkede forhold oppfyller i noen grad revisjonskriteriet. Det er avdekket forbedringspotensial.
	Avdekkede forhold oppfyller i stor grad revisjonskriteriet. Det er imidlertid avdekket mindre forbedringspotensial.
	Avdekkede forhold oppfyller fullt ut revisjonskriteriet.

Figur 1 – Visualisering av subjektiv oppfatning av kvalitet.

4 PROBLEMSTILLING 1: HAR MOSS KOMMUNE ETABLERT ET TILFREDSSTILLENDE STYRINGSSYSTEM (INTERNKONTROLL) FOR PERSONVERN?

4.1 Utledning av revisjonskriterier

Kravet om å utarbeide et styringssystem (internkontroll) for personvern følger av GDPR artikkel 24 nr. 1. Det følger av ordlyden i artikkel 24 nr. 1 at internkontrollen skal sikre at alle aktuelle plikter etter GDPR etterleves, og at etterlevelsen kan dokumenteres. Personvernforordningen stiller ikke eksplisitte krav om hvordan interkontrollen skal utformes utover at den skal være tilpasset behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene som virksomheten står overfor.

Datatilsynet har utformet en veileder for å etablere internkontroll hvor det er presisert at internkontroll:

«[…] skal være ledelsens verktøy for å ivareta sitt ansvar og demonstrere etterlevelse etter personvernregelverket, og de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte»[2].

Ansvaret for å sikre etterlevelse av personvernlovgivningen i den enkelte virksomhet ligger hos virksomhetens ledelse. Ledelsen må implementere personvern i virksomhetsstyringen, og sikre at det er tilstrekkelig med ressurser, verktøy og kompetanse for å sikre etterlevelse.

Videre beskriver Datatilsynet at internkontroll bør bestå av styrende elementer, gjennomførende elementer og kontrollerende elementer som er proporsjonale med behandlingen virksomheten utfører.[3] Virksomheten må ta utgangspunkt i behandlingsaktivitetene den er behandlingsansvarlig for. Videre må virksomheten identifisere hvilke plikter den er underlagt, og hvilke risikoer som foreligger for de registrerte, og tilpasse internkontrollen deretter. Det bør være en sammenheng mellom omfanget av gjennomførende og kontrollerende elementer, og risikoen for de registrertes rettigheter og friheter ved behandlingen. Det er altså ikke risikoer knyttet til virksomhetens verdier som er avgjørende.[4]

Ledelsen må sikre at internkontrollen gir et korrekt bilde av eksisterende organisering og utførelse av behandlinger i virksomheten. Dette innebærer at internkontrollen må gjennomgås og oppdateres jevnlig. Internkontrollens styrende elementer skal gi en overordnet og systematisk beskrivelse av hvilke krav og plikter virksomheten må oppfylle, virksomhetens strategi og målsetninger, samt fordeling av roller og ansvar. Dette er vanligvis beskrevet i dokumenter som danner grunnlag for- og gir en oversikt over gjennomførende tiltak, samt dokumentasjon av disse. De gjennomførende elementene består vanligvis av rutiner og instrukser for tiltak, systemer og prosesser som innebærer behandling av personopplysninger. Internkontrollens kontrollerende elementer består normalt av kontrollrutiner som dokumenterer at rutiner og arbeidsinstrukser følges, og som fanger opp eventuelle avvik. De kontrollerende elementene må også sikre ledelsens systematiske gjennomgang og forbedring av internkontrollen.

I tillegg til at GDPR artikkel 24 stiller krav om å etablere en internkontroll for personvern, stiller også kommuneloven § 25-1 krav om at kommunen skal ha internkontroll for å sikre at lover og forskrifter følges. Internkontrollen skal være tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold.

[2] Datatilsynet veileder "Etablere internkontroll" punkt 1
[3] Datatilsynet veileder "Etablere internkontroll" punkt 1
[4] Datatilsynet veileder "Etablere internkontroll" punkt 2

Bestemmelsen fastsetter at kommunedirektøren er ansvarlig for internkontrollen, og at kommunedirektøren må sikre at det blant annet utarbeides en beskrivelse av virksomhetens hovedoppgaver, mål og organisering, at kommunen har nødvendige rutiner og prosedyrer og at internkontrollen er dokumentert i den formen og det omfanget som er nødvendig.

Revisjonslaget er informert om at Moss kommune baserer sitt styringssystem for informasjonssikkerhet på ISO/IEC 27001. Revisjonslaget mener derfor at det også vil være hensiktsmessig å basere sitt styringssystem for personvern på anerkjente standarder som ISO/IEC 27701 som er en forlengelse av ISO/IEC 27001.

4.2 Revisjonskriterier

Basert på utledningen ovenfor har revisjonslaget utarbeidet følgende revisjonskriterier:

Moss kommunen skal:

- Sørge for at personvernforordningens prinsipper ivaretas ved behandling av personopplysninger (GDPR artikkel 5).
- Sørge for at alle behandlingsaktiviteter har et lovlig behandlingsgrunnlag (GDPR artikkel 6 og personopplysningsloven § 8).
- Kunne påvise at den registrerte har avgitt gyldig samtykke når dette benyttes som behandlingsgrunnlag (GDPR artikkel 7 og personopplysningsloven § 5).
- Sørge for at særlige kategorier av personopplysninger kun behandles når det er lovlig i henhold til personvernforordningen (GDPR artikkel 9 og personopplysningsloven §§ 6, 7 og 9).
- Sikre at fødselsnummer og andre entydige identifikasjonsmidler kun behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering (personopplysningsloven § 12)
- Oppfylle plikten til å gi informasjon til de registrerte (GDPR artikkel 12-14).
- Sikre at de registrertes rett til innsyn ivaretas (GDPR artikkel 15).
- Sikre at den registrertes rett til retting ivaretas (GDPR artikkel 16).
- Sikre at den registrertes rett til sletting ivaretas (GDPR artikkel 17).
- Sikre at den registrertes rett til begrensning av behandling ivaretas (GDPR artikkel 18).
- Sikre at den registrertes rett til dataportabilitet ivaretas (GDPR artikkel 20).
- Sikre at den registrertes rett til å protestere ivaretas (GDPR artikkel 21).
- Gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen (GDPR artikkel 24).
- Sørge for innebygd personvern og personvern som standardinnstilling i systemer som kommunen utvikler og anskaffer (GDPR artikkel 25).
- Sikre at databehandlere gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller personvernforordningens bestemmelser (GDPR artikkel 28).
- Sørge for at kommunen på en åpen måte fastsetter sitt ansvar for å overholde forpliktelsene i personvernforordningen dersom kommunen er felles behandlingsansvarlig med en annen virksomhet (GDPR artikkel 26).
- Inngå databehandleravtaler med alle databehandlere (GDPR artikkel 28).
- Føre skriftlig protokoll over behandlingsaktiviteter som kommunen er behandlingsansvarlig for (GDPR artikkel 30).
- Gjennomføre risikovurderinger for å fastsette et egnet sikkerhetsnivå (GDPR artikkel 32).
- Gjennomføre tekniske og organisatoriske tiltak for å oppnå det sikkerhetsnivået som er egnet med hensyn til risikoen forbundet med behandlingen av personopplysninger (GDPR artikkel 32).

- Håndtere og dokumentere alle brudd på personopplysningssikkerheten, herunder underrette Datatilsynet og de registrerte når dette er nødvendig (GDPR artikkel 33-34).
- Gjennomføre og dokumentere personvernkonsekvensvurderinger når det er sannsynlig at en behandling vil medføre en høy risiko for fysiske personers rettigheter og friheter (GDPR artikkel 35).
- Dokumentere vurderinger av om kommunen er pålagt å gjennomføre personvernkonsekvensvurderinger (GDPR artikkel 35 nr. 1, jf. artikkel 5 nr. 2)
- Utpeke et personvernombud (GDPR artikkel 37).
- Sørge for at personvernombudet kan utføre sine lovpålagte oppgaver (GDPR artikkel 38 og 39).
- Sikre at personvernombudet ikke mottar instrukser om utførelsen av sine lovpålagte oppgaver (GDPR artikkel 38 nr. 3 og nr. 6).
- Sørge for at kravene til overføring av personopplysninger til tredjestat er ivaretatt dersom slik overføring skjer (GDPR artikkel 44-50).
- Beskrive mål og overordnede rammer for behandling av personopplysninger i kommunen (Kommuneloven § 25-1 og Datatilsynets veileder – Etablere internkontroll).
- Utarbeide nødvendige rutiner og retningslinjer for behandling av personopplysninger basert på en risikovurdering (Kommuneloven § 25-1 og Datatilsynets veileder – Etablere internkontroll).

Moss kommune bør:

- Basere sitt styringssystem for personvern på anerkjente standarder.

4.3 Datagrunnlag

4.3.1 Ivaretakelse av personvernprinsippene

Personvernprinsippene er nevnt i flere dokumenter som Moss kommune har fremlagt, herunder i *«MK Hvordan skal jeg som ansatt forholde meg til GDPR»*, i *«MK Internkontroll og kvalitet i Moss kommune», «MK Personvernveileder»* og i *«MK - Rutine for automatiserte individuelle avgjørelser».* Det fremgår imidlertid ikke av dokumentasjonen hva prinsippene innebærer eller hvordan kommunen skal arbeide for å ivareta prinsippene. Dokumentene *«MK Internkontroll og kvalitet i Moss kommune»* og *«MK - Rutine for automatiserte individuelle avgjørelser»* er ikke godkjent på tidspunktet for revisjonen. Etter kommunens gjennomgang av datagrunnlaget ble det informert om at dokumentet *«MK Internkontroll og kvalitet i Moss kommune»* etterleves til tross for at det ikke er formelt godkjent. Det ble videre kommentert i kommunens gjennomgang av datagrunnlaget at «prinsippene ligger i lovverket».

Det er opplyst i intervju at kommunen har fokus på dataminimering ved å begrense innsamlingen av informasjon til det som er kun nødvendig. I tillegg fremkom det av både intervju og dokumentasjon at kommunen har iverksatt flere tiltak for å ivareta personopplysningenes integritet og konfidensialitet, for eksempel ved å ha fokus på å lagre personopplysninger i riktige fagsystemer og ved å sørge for tilgangskontroll. Videre arbeider kommunen med å utarbeide personvernerklæringer for å ivareta prinsippet om åpenhet. Kommunen har ikke fremlagt dokumentasjon på at alle behandlingsaktiviteter har et lovlig behandlingsgrunnlag, at alle behandlingsaktiviteter har et definert formål eller at det er fastsatt slettefrister. Det er heller ikke fremlagt dokumentasjon som beskriver hvordan kommunen arbeider med å sikre personopplysningenes riktighet, utenom å sørge for at de registrerte har en rett til å få rettet personopplysninger.

4.3.2 Behandlingens lovlighet

Revisjonslaget har fått fremlagt dokumentet *«MK Personvernveileder».* Det fremgår blant annet av veilederen at kommunen må vurdere og dokumentere behandlingsgrunnlag for hver enkelt behandling. Videre gis det også en beskrivelse av de ulike behandlingsgrunnlagene og når disse kan benyttes.

Det fremgår av rutinen *«MK - Rutine for automatiserte individuelle avgjørelser»* at behandlingsgrunnlag skal vurderes og dokumenteres ved bruk av automatiserte individuelle avgjørelser. Rutinen er ikke godkjent og implementert på tidspunktet for revisjon. Revisjonslaget har ikke fått fremlagt andre rutiner som skal sikre at ansatte vurderer og dokumenterer behandlingsgrunnlag ved oppstart eller endring av behandlingsaktiviteter. Etter kommunens gjennomgang av datagrunnlaget ble revisjonslaget informert om at dette skal gjøres når det gjennomføres en DPIA. Revisjonslaget har heller ikke fått fremlagt dokumentasjon på at alle behandlingsaktiviteter har et lovlig behandlingsgrunnlag.

4.3.3 Vilkår for samtykke

Det fremgår både av dokumentet *«MK Hvordan skal jeg som ansatt forholde meg til GDPR»* og dokumentet *«MK Personvernveileder»* at samtykker skal være frivillige, lett forståelige, tydelige og entydige, dokumenterte og at samtykker kan trekkes tilbake. Det fremgår av *«MK Personvernveileder»* at dokumentasjonen skal inneholde hva den registrerte har samtykket til, hva de har fått opplyst, når og hvordan den registrerte har samtykket. Videre fremgår det av *«MK Hvordan skal jeg som ansatt forholde meg til GDPR»* at kommunen må bruke samtykke som behandlingsgrunnlag dersom kommunen ikke har hjemmel i lov for å behandle personopplysninger.

Det er opplyst at kommunen ønsker å anskaffe et helhetlig system for samtykkeerklæringer, men at kommunen ikke har lykkes med dette da det finnes få leverandører som kan levere et tilfredsstillende system. Det er opplyst om at vilkårene for samtykke ivaretas av virksomhetene i linjen. Eksempelvis benytter skolene Visma for å innhente og dokumentere samtykker.

4.3.4 Behandling av særlige kategorier av personopplysninger

Det fremgår av dokumentet *«MK Personvernveileder»* hva sensitive personopplysninger er og at det gjelder særlig strenge krav til behandling av slike opplysninger. Videre fremgår det av *«MK - Rutine for automatiserte individuelle avgjørelser»* at behandling av særlige kategorier av personopplysninger skal ha grunnlag i GDPR artikkel 9. Det fremgår av det sistnevnte dokumentet at rutinen ikke er vedtatt og implementert på tidspunktet for revisjonen. Det er ikke fremlagt annen dokumentasjon som beskriver hvordan kommunen sikrer at særlige kategorier av personopplysninger kun behandles når det er lovlig etter GDPR artikkel 9. Etter kommunens gjennomgang av datagrunnlaget ble det informert om at dette ivaretas når det gjennomføres en DPIA. Revisjonslaget har heller ikke fått fremlagt dokumentasjon på at behandling av særlige kategorier av personopplysninger i kommunen er basert på et rettslig grunnlag i henhold til GDPR artikkel 9.

4.3.5 Behandling av fødselsnummer og andre entydige identifikasjonsmidler

Det er ikke fremlagt dokumentasjon som beskriver hvordan kommunen sikrer at fødselsnummer og andre entydige identifikasjonsmidler kun behandles når det foreligger et saklig behov for sikker identifisering.

Etter kommunens gjennomgang av datagrunnlaget ble det kommentert at kommunen tolker regelverket til at det ikke er et dokumentasjonskrav som beskriver hvordan kommunen sikrer at fødselsnummer og andre identifikasjonsmidler kun behandles når det foreligger et saklig behov for sikker identifisering. Kommunen informerte videre at det ble «fremlagt eksempler» på det overstående.

4.3.6 Oppfyllelse av informasjonsplikten

Moss kommune har fremlagt en personvernerklæring som ligger tilgjengelig på kommunens nettsider. Personvernerklæringen gjelder for hele kommunen og gir en overordnet beskrivelse av hvordan kommunen behandler både innbyggeres og ansattes personopplysninger. Det er fastsatt i *«MK Retningslinje*

informasjonssikkerhet og personvern» at personvernerklæringen til enhver tid skal være oppdatert og ifølge kommunens personvernerklæring skal denne revideres av personvernombudet.

Det fremgår av dokumentet *«MK Internkontroll og kvalitet i Moss kommune»* at de ulike kommunalområdene skal ha egne spesifikke personvernerklæringer som gjenspeiler behandlingen av personopplysninger relevant for hvert område. Revisjonslaget har ikke fått fremlagt andre personvernerklæringer enn den som gjelder for kommunen generelt. Revisor er informert gjennom intervju at dette er noe kommunen arbeider med å få utarbeidet.

Dokumentene *«MK Retningslinje informasjonssikkerhet og personvern»* og *«MK Internkontroll og kvalitet i Moss kommune»* er ikke godkjent og implementert på tidspunktet for revisjonen.

4.3.7 Retten til innsyn

Det fremgår av kommunens personvernerklæring, som er tilgjengelig på nettsiden, at enhver kan sende anmodning om innsyn til hvilken som helst ansatt i kommunen eller til kommunens personvernombud. At den registrerte har rett til innsyn er beskrevet i dokumentet *«MK Personvernveileder»* og i dokumentet *«MK Hvordan skal jeg som ansatt forholde meg til GDPR»*. Det fremgår av veilederen at retten til innsyn innebærer en rett til informasjon om behandlingen av personopplysninger og innsyn i selve opplysningene. Det fremgår av de sistnevnte retningslinjene at ansatte skal gi innsyn etter kommunens rutine for innsyn og gi innsyn i personopplysninger etter regelverk som offentleglova, forvaltningsloven, pasientjournalloven mv.

Revisjonslaget har fått fremlagt dokumentet *«DOK Innsynsbegjæringer (generelle og spesielle)»* hvor det er beskrevet hvordan retten til innsyn etter offentleglova § 3 skal håndteres. Dokumentet inneholder også rutiner for å gi ansatte innsyn i egen personalmappe med henvisning til den opphevede personopplysningsloven § 18. I tillegg har revisjonslaget fått fremlagt rutiner for innsyn som gjelder kommunalområdet helse og mestring. Disse rutinene viser til forvaltningsloven § 13a og innsynsbestemmelser som fremgår av særlovgivning for helsesektoren.

Det fremgår ikke av de fremlagte rutinene hvordan ansatte skal håndtere anmodninger om innsyn etter kravene i GDPR, herunder hvem som er ansvarlig for å håndtere slike anmodninger eller hvilke frister som gjelder. Etter kommunens gjennomgang av datagrunnlaget ble det fra kommunens side kommentert «forvaltningsloven». Det er videre ikke beskrevet hvordan reglene i GDPR er ulike fra andre innsynsbestemmelser i særlovgivningen. Det er opplyst i intervju at anmodninger om innsyn etter GDPR skal sendes til personvernombudet, men dette gjenspeiles ikke i dokumentasjonen. Etter kommunens gjennomgang av datagrunnlaget ble det informert om at anmodninger om innsyn ikke automatisk skal oversendes til personvernombudet, men at personvernombudet kan bistå med råd.

4.3.8 Retten til retting

Anmodninger om å få rettet personopplysninger i Moss kommune kan sendes til hvilken som helst ansatt i kommunen eller til personvernombudet. Dette fremgår av kommunens personvernerklæring. Ifølge dokumentene *«MK Personvernveileder»* og dokumentet *«MK Hvordan skal jeg som ansatt forholde meg til GDPR»* kan den registrerte ha rett til å få rettet sine personopplysninger dersom de er ufullstendige eller uriktige, men det fremgår ikke av dokumentene hva en ansatt skal gjøre dersom de mottar anmodninger om retting, hvordan retting kan gjennomføres eller hvem som er ansvarlig for å vurdere og følge opp slike anmodninger. Det er ikke fremlagt andre rutiner for å håndtere anmodninger om retting. Etter kommunens gjennomgang av datagrunnlaget ble revisjonslaget informert om at ansattes mulighet til å rette opplysninger i stor grad styres av tilganger og systemer.

4.3.9 Retten til sletting

Det fremgår av Moss kommunes personvernerklæring at anmodninger om sletting kan sendes til hvilken som helst ansatt i kommunen eller til personvernombudet. I dokumentet *«MK Personvernveileder»* er det beskrevet at den registrerte kan ha rett til sletting og hva retten til sletting innebærer. I *«MK Hvordan skal jeg som ansatt forholde meg til GDPR»* er det beskrevet at registrerte kan ha en rett til å bli glemt dersom personopplysninger er innhentet gjennom samtykke og i noen andre tilfeller. Den sistnevnte rutinen spesifiserer ikke hvilke tilfeller dette gjelder. Det fremgår heller ikke av dokumentene hva ansatte skal gjøre dersom de mottar anmodninger om sletting eller hvem som er ansvarlig for å følge opp slike anmodninger. Det er ikke fremlagt andre rutiner for å håndtere anmodninger om sletting.

Revisjonslaget er informert om at kommunen i mange tilfeller ikke vil ha anledning til å slette personopplysninger grunnet dokumentasjonsplikter i andre regelverk. Det er også opplyst om at noen fagsystemer kan begrense ansattes mulighet til å gjennomføre sletting.

4.3.10 Retten til begrensning

Det fremgår av dokumentet *«MK Personvernveileder»* at den registrerte kan ha rett til begrensning av behandling og hva retten til begrensning innebærer. Moss kommune har ikke fremlagt dokumentasjon på hvordan de sikrer at retten til begrensning av behandling ivaretas. Etter kommunens gjennomgang av datagrunnlaget ble revisjonslaget informert om at retten til begrensning er nevnt i dokumentet «*MK – Rutine for automatiserte individuelle avgjørelser*» under trinn 5. Dokumentet er på tidspunktet for revisjonen i utkast form og ikke godkjent.

4.3.11 Retten til dataportabilitet

Det fremgår av dokumentet *«MK Personvernveileder»* at den registrerte kan ha rett til dataportabilitet og hva retten til dataportabilitet innebærer. Moss kommune har ikke fremlagt dokumentasjon på hvordan de sikrer at retten til dataportabilitet ivaretas.

4.3.12 Retten til å protestere

Det fremgår av dokumentet *«MK Personvernveileder»* at den registrerte kan ha rett til å protestere og hva retten til å protestere innebærer. Moss kommune har ikke fremlagt dokumentasjon på hvordan de sikrer at retten til å protestere ivaretas.

4.3.13 Den behandlingsansvarliges ansvar

Moss kommune har fremlagt dokumentet *«MK Internkontroll og kvalitet i Moss kommune»* som omhandler kommunens arbeid med internkontroll og kvalitet i kommunen generelt. Dokumentet er ikke godkjent på tidspunktet for revisjon. Det fremgår av ovennevnte dokumentet at det er etablert et kvalitetssystem som er tilgjengelig for alle i kommunen og at systemet skal være et oppslagsverk innen dokumentasjon, et verktøy for å melde avvik og et verktøy for å gjennomføre risikovurderinger. Videre er det fastsatt at hvert kommunal- og stabsområde har ansvar for egenkontroll og leveranser innen kvalitet og forbedring, og at hvert område skal ha egne kvalitetsutvalg. Team internkontroll og kvalitet i kommunens stabsfunksjon skal understøtte kommunalområdene og bidra til enhetlig praksis, utvikling og samhandling. Det fremgår av ovennevnte dokument at internkontrollen inkluderer personvern.

Moss kommune har også fremlagt dokumentasjon som inneholder styrende, gjennomførende og kontrollerende elementer for personvern spesifikt.

Styrende elementer
I *«MK Retningslinje informasjonssikkerhet og personvern»* har kommunen beskrevet hvordan de arbeider med informasjonssikkerhet og personvern. Det fremgår av dokumentet at retningslinjene dekker

styrende og kontrollerende tiltak og at retningslinjene referer til utførende dokumenter. Retningslinjene er gjeldende for alle medarbeidere i kommunene, i foretakene, folkevalgte og for leverandører og tilsynsmyndigheter som skal ha tilgang til Moss kommunes systemer. Dokumentet *«MK Retningslinje informasjonssikkerhet og personvern»* er ikke godkjent og implementert på tidspunktet for revisjonen.

De ovennevnte retningslinjene inneholder blant annet en beskrivelse av myndighet og ansvar for informasjonssikkerhet og personvern i kommunen. I tillegg har Moss kommune fremlagt dokumentet *«MK Personvern oversikt oppgaver og ansvar»* hvor det er listet opp oppgaver innen personvern. Det fremgår av disse dokumentene at det operative ansvaret for personvern er lagt til kommunal- og stabssjefer og linjeledere. Dette inkluderer et ansvar for å avdekke behov for retningslinjer og prosedyrer for eget tjenesteområde, registrere behandlinger og systemer som blir brukt, gjennomføre risikovurderinger og personvernkonsekvensvurderinger, inngå databehandleravtaler, sikre internkontroll, opplæring mv. Som beskrevet i punkt 4.3.7 - 4.3.12 er det ikke fremlagt dokumentasjon på hvem som er ansvarlig for å håndtere anmodninger om håndheving av de registrertes rettigheter. Etter kommunens gjennomgang av datagrunnlaget ble revisjonslaget informert om at dette faller innenfor det operative ansvaret for personvern.

At ledere i kommunen er delegert det operative ansvaret for personvern samsvarer med det som er opplyst gjennom intervjuer. Det er imidlertid gitt tilbakemelding om at ansvarsfordelingen for personvern oppleves som uklar og at det er uklart hva ansvaret innebærer. Flere av intervjuobjektene har også uttrykt at det mangler kompetanse innen personvern som gjør det mulig å utøve ansvaret. Det er videre opplyst at kommunen ikke gjennomfører systematisk og regelmessig opplæring innen personvern. Etter kommunens gjennomgang av datagrunnlaget ble revisjonslaget informert om at det ble gjennomført opplæring frem til desember 2020.

I tillegg til at linjeledere er tildelt et ansvar for personvern, er det opprettet et sikkerhet- og personvernutvalg som skal ha ansvar for å bidra til å utvikle, etablere og implementere overordnede retningslinjer og prosedyrer, samt å følge opp avvik. Det er bekreftet i intervju at utvalget er etablert. Utvalget ledes av personvernombudet og alle kommunalområdene skal være representert. Det fremkom i intervju at kommuneadvokaten ikke er representert i utvalget og at det ennå ikke er helt avklart hvorvidt kommuneadvokaten skal delta i utvalget eller ikke.

Gjennomførende elementer

Det er opplyst at kommunen ikke har gjennomført en kartlegging av behandlingsaktiviteter og det er heller ikke gjennomført dokumenterte risikovurderinger basert på disse. Det er opplyst i intervju at kommunen arbeider med å implementere et system for å kartlegge behandlingsaktiviteter.

Moss kommune har utarbeidet og fremlagt skriftlige prosedyrer, retningslinjer, sjekklister og veiledere på personvernområdet som er utarbeidet av kommunen sentralt. Dokumentene er tilgjengelig for de ansatte gjennom kvalitetssystemet «Risk Manager». Kommunen har blant annet fremlagt flere rutiner og retningslinjer for databehandleravtaler og avvikshåndtering. Enkelte av de fremlagte dokumentene er fortsatt i utkastform og inneholder kommentarer. Dette gjelder for eksempel *«MK - Rutine for automatiserte individuelle avgjørelser».* I *«MK Personvernveileder»* er det henvist til en rutine for å håndtere anmodninger om håndheving av de registrertes rettigheter som revisjonslaget ikke har fått fremlagt. Det er opplyst i intervju at disse rutinene ikke finnes. Det fremkom i intervju at personvernombudet arbeider med å få på plass manglende dokumentasjon innen personvern, men at det mangler ressurser som kan bistå ham med dette. Revisjonslaget er informert om at personvernombudet vil trenge rundt seks måneder å ferdigstille dokumentasjonen som må være å plass, og at det vil ta rundt to år å ferdigstille alt som bør være på plass.

I tillegg til de generelle rutinene som kommunen har utarbeidet sentralt, er det opplyst at de ulike kommunalområdene og enhetene har utarbeidet egne rutiner for sitt daglige arbeid hvor også krav til personvern blir ivaretatt. Dette gjelder for eksempel i kommunalområdet for helse og mestring, kommunalområdet for kultur, oppvekst og aktivitet og avdeling for dokumentforvaltning. Revisjonslaget har ikke gjennomgått alle disse rutinene.

Kontrollerende elementer
Det fremgår av dokumentet *«MK Internkontroll og kvalitet i Moss kommune»* og *«MK Retningslinje informasjonssikkerhet og personvern»* at det årlig skal gjennomføres ledelsens gjennomgang. I tillegg til at det skal gjennomføres en ledelsens gjennomgang sentralt, fremgår det av dokumentet *«MK Internkontroll og kvalitet i Moss kommune»* at de enkelte kvalitetsutvalgene gjennomføre ledelsens gjennomgang innen sitt kommunalområde

Ledelsens gjennomgang omfatter kommunes arbeid med interkontroll generelt, hvor personvern er en del av dette. I dokumentet *"MK retningslinje informasjonssikkerhet og personvern"* står det at kommunedirektøren, kommunal- og stabssjefene og sikkerhetsansvarlig har et ansvar for ledelsens gjennomgang. I tillegg fremgår det av det samme dokumentet at personvernombudet er ansvarlig for å gjennomføre ledelsens gjennomgang.

Moss kommune har fremlagt dokumentet *«MK Ledelsens gjennomgang av informasjonssikkerhet og personvern».* Det fremgår av dette dokumentet at ledelsens gjennomgang skal gjennomføres tre ganger i året og at det er kommunedirektøren og kommunedirektørens ledergruppe som har ansvar for gjennomføringen av «ledelsens gjennomgang».

Det er opplyst i intervju at ledelsens gjennomgang ikke er gjennomført sentralt på tidspunktet for revisjon, men at enkelte kvalitetsutvalg har gjennomført ledelsens gjennomgang. Andre kvalitetsutvalg er imidlertid ikke etablert og har derfor ikke gjennomført ledelsens gjennomgang.

Kommunen har videre utarbeidet *«MK Sjekkliste for egenkontroll av informasjonssikkerhet og GDPR»* som inneholder en rekke spørsmål om informasjonssikkerhet og personvern som er rettet til virksomhetene/enhetene i linjen, herunder innen kategoriene ansvar og organisering, opplæring, tilganger, avviks-håndtering, risikovurderinger og de registrertes rettigheter. I intervju er det opplyst at dette skjemaet ble sendt ut til alle ledere som er systemeiere for første gang ved utgangen av 2020 fra kommunen sentralt. Svarene skulle benyttes for å sammenligne bevisstheten rundt personvern i kommunen før og etter opplæring, men dette ble ikke fulgt opp idet kommunen ikke hadde kapasitet til å gjennomføre den planlagte opplæringen.

Ifølge *«MK Interkontroll og kvalitet i Moss kommune» og «MK Retningslinje for informasjonssikkerhet og personvern*» skal det gjennomføres internrevisjoner. Det fremgår av dokumentet *«Internrevisjon Moss kommune 26082021»* at det skal gjennomføres en internrevisjon av personvern i Q2 hvert år. Det er opplyst i intervju at det arbeides med å få på plass en systematisk internrevisjon.

Det er fremlagt dokumentasjon på at status på personvernområdet har vært tema i kommunegruppens ledergruppe (KLG), men det er opplyst om at kommunen ikke har en systematisk overordnet kontroll av at kravene til personvern etterleves i linjen og at det hittil har blitt gjennomført kontrollaktiviteter ad hoc.

4.3.14 Innebygd personvern og personvern som standardinnstilling

Kommunen har fremlagt en mal for databehandleravtale hvor det er fastsatt et krav om at databehandlere skal påse at systemene er designet i overenstemmelse med kravene til innebygd personvern. I tillegg er det fastsatt et punkt om å vurdere innebygd personvern i malen for personvernkonsekvensvurderinger. Det er ikke fremlagt annen dokumentasjon som beskriver hvordan kommunen ivaretar kravet til innebygd personvern og personvern som standardinnstilling, men det er opplyst i intervju at kravet til innebygd personvern ivaretas i anskaffelsesprosesser ved at personvernombudet blir involvert. Dette sørger kommunen for ved at ansatte som ønsker å anskaffe systemer må melde inn et ønske gjennom et skjema på kommunens intranettside. Dersom ansatte besvarer at systemet skal behandle personopplysninger, vil personvernombudet bli koblet på prosessen.

Det er opplyst i intervju at det er planlagt å gjennomføre et kurs om innebygd personvern for kommunikasjonsavdelingen i kommunen.

4.3.15 Felles behandlingsansvar

Moss kommune har ikke fremlagt dokumentasjon på hvordan de sikrer at kommunen avdekker felles behandlingsansvar og at felles behandlingsansvar følges opp.

4.3.16 Databehandlere

Det er opplyst om at kommunen har en anskaffelsesprosedyre og at det er planlagt å legge inn krav knyttet til personvern i denne. For å sikre at personvern ivaretas i anskaffelsesprosesser i dag, sørger kommunen for å inkludere personvernombudet. Dette gjøres ved at ledere som ønsker seg et nytt system må melde inn dette via et skjema på kommunens intranett hvor de må oppgi informasjon knyttet til behandlingen av personopplysninger. Dersom ledere fyller inn slik informasjon vil personvernombudet involveres.

Moss kommunen har fremlagt dokumentet *«MK Oversikt over fagsystem personopplysningsloven (Behandlingsprotokoll)»* som gir en oversikt over leverandører og databehandlerrelasjoner. Det er opplyst i intervju at oversikten er fra gamle Moss og Rygge og at kommunen ikke har en oppdatert oversikt over alle databehandlerrelasjoner som Moss kommune har i dag. Det er planlagt å anskaffe et nytt verktøy for å holde oversikt over databehandlerrelasjoner.

Moss kommune stiller krav til databehandlere i databehandleravtalen om at de skal levere en årlig revisjonsrapport. Det er ikke fremlagt rutiner som skal sikre at det gjennomføres revisjoner/kontroller av databehandlere og det er opplyst i intervju at kommunen ikke gjennomfører regelmessige revisjoner/kontroller av databehandlere, men at dette er noe de har planlagt å begynne med. Gjennom intervju har det blitt avdekket ansvarsfordelingen knyttet til oppfølging av databehandlere er uklar.

4.3.17 Databehandleravtaler

Det fremgår av retningslinjer og prosedyrer til Moss kommune at det skal inngås databehandleravtaler med alle leverandører av applikasjoner og datautstyr hvor personopplysninger behandles. Det fremgår videre av retningslinjene at databehandleravtaler som hovedregel skal inngås på kommunens egen mal og at personvernombudet alltid skal involveres. Dersom leverandøren ønsker å benytte egen databehandleravtale, så skal man gjennomgå en sjekkliste for databehandleravtale. Rutinene er beskrevet i dokumentene *«MK Retningslinje informasjonssikkerhet og personvern», «MK Retningslinje for databehandleravtale», «MK Sikring av databehandleravtale»* og *«MK hvordan skal jeg som ansatt forholde meg til GDPR».*

Kommunen har fremlagt en mal for databehandleravtale både på norsk og engelsk. Kommunen har også fremlagt sjekklisten som skal gjennomgås dersom malen ikke benyttes. Sjekklisten oppstiller obligatoriske og ikke obligatoriske krav til databehandleravtaler.

4.3.18 Protokoll over behandlingsaktiviteter

Det fremgår av dokumentet *«MK Personvern oversikt oppgaver og ansvar»* at ledere skal registrere alle behandlinger i «Forms skjema». I tillegg har Moss kommune fremlagt en presentasjon som ble benyttet ifm. opplæring innen behandlingsoversikt og protokoll. Det fremgår av presentasjonen hva en protokoll skal inneholde og at kommunen benytter et regneark og et skjema for å føre protokoll. Det fremkom i intervju at presentasjonen ble gitt som en del av et større opplæringsprogram for ledere i 2018.

Det ble i intervju opplyst om at kommunen tidligere kartla sine behandlingsaktiviteter gjennom et verktøy for protokoll av behandlingsaktiviteter levert av RISMA, men at kommunen ikke lenger har tilgang til dette. I intervju fremkom det videre at kommunen ikke har en protokoll for sine behandlingsaktiviteter og at de heller ikke systematisk kartlegger dette i dag. Det er både fremlagt dokumentasjon på og opplyst i intervju at kommunen nylig har anskaffet et verktøy kalt Fiks DigiOrden som blant annet skal benyttes til å føre protokoll over behandlingsaktiviteter. Arbeidet med implementering av verktøyet skal starte høsten 2021.

Moss kommune har fremlagt dokumentet *«MK Oversikt over fagsystem personopplysningsloven (Behandlingsprotokoll)»* som gir en oversikt over fagsystemer hvor det behandles personopplysninger. Av oversikten fremgår det blant annet hva systemene benyttes til, hvilken lov kommunen benytter som grunnlag for behandlingen, formål og hvordan sletting ivaretas. Det er opplyst i intervju at oversikten er fra gamle Moss og Rygge kommune.

4.3.19 Risikovurderinger for å fastsette egnet sikkerhetsnivå

Ifølge *«MK Retningslinje for informasjonssikkerhet og personvern»* skal det gjennomføres en årlig risikovurdering som skal identifisere risikoene forbundet med tap av konfidensialitet, integritet og tilgjengelighet. Det fremgår av den overnevnte retningslinjen at risikovurderingen skal gjennomføres i henhold til «gjeldende retningslinje». Revisjonslaget har ikke fått oversendt en slik retningslinje, og kan dermed heller ikke vurdere hvordan risikovurderingene skal gjennomføres. Etter kommunens gjennomgang av datagrunnlaget kommenterte kommunen at den nevnte retningslinjen var i dokumentet «*MK Internkontroll og kvalitet i Moss kommune*». I tillegg skal det gjennomføres fortløpende risikovurderinger basert på behov og endringer. De ovennevnte dokumentene er i utkastform og ikke godkjent på tidspunktet for revisjonen.

Moss kommune har gjennomført en helhetlig risiko- og sårbarhetsanalyse (ROS) i 2019. ROS-analysen tar ikke for seg risikoer knyttet til personvern. Det fremkom i intervju at det ikke er gjennomført risikovurderinger knyttet til personvern sentralt i kommunen. Det har blitt opplyst at det er gjort enkelte risikovurderinger av virksomhetene i linjen og knyttet til anskaffelse av systemer i ny kommune. Det er fremlagt en oversikt over gjennomførte risikovurderinger i kommunen. Av oversikten fremgår det at det blant annet er gjort en risikovurdering av informasjonssikkerhet og ivaretakelse av personvern i henhold til GDPR og bruk av NAV fagsystemer, arkivsystemet og SMS funksjonalitet i Gerica. Revisjonslaget har ikke gjennomgått disse risikovurderingene. Etter kommunens gjennomgang av datagrunnlaget ble revisjonslaget informert om at risikovurderinger også er en del av kommunens DPIA.

I intervju ble det uttrykt at kompetansen til å gjennomføre risikovurderinger er varierende nedover i organisasjonen. Det ble trukket frem at det mangler en strukturert og systematisert måte å gjennomføre

risikovurderinger på og at det per i dag i større grad gjennomføres ad-hoc. Enkelte opplyste i intervju at det trolig gjøres risikovurderinger, men at disse ikke alltid dokumenteres.

4.3.20 Tiltak for å oppnå egnet sikkerhetsnivå

Det fremgår av dokumentet *«MK Retningslinje informasjonssikkerhet og personvern»* at:

«Kommunen skal ha et sikkerhetsnivå på fysisk og digital informasjon som samsvarer med normative krav satt i de internasjonale standardene for ledelsessystem for informasjonssikkerhet, helselovgivning, personopplysningsloven (GDPR), nasjonale retningslinjer og føringer fra myndigheter som NSM og Datatilsynet.»

Det ovennevnte dokumentet er i utkastform og ikke godkjent eller implementert på tidspunktet for revisjonen.

Moss kommune har iverksatt flere tiltak for å ivareta personopplysningenes sikkerhetsnivå. Det er blant annet opplyst i intervju at kommunalområdene har et særlig fokus på å lagre personopplysninger i riktige fagsystemer og å sørge for at det kun er ansatte med et tjenstlig behov som har tilgang til personopplysningene. Dette er også beskrevet flere steder i mottatt dokumentasjon.

Moss kommune har også iverksatt tiltak for å sikre personopplysningene mot angrep fra utsiden. Ved anvendelse av penetrasjonstest (utside) og passordgjetting over flere dager, lykkes ikke revisjonslaget med å gjette noen passord. Videre ble TLS konfigurasjonen til de ulike tjenestene testet med Qualys SSL server test. Resultatet fra testen avdekket at https://politiker.moss.kommune.no og https://wap.moss.kommune.no har støtte for TLS 1.0 og TLS 1.1. Ved bruk av ulike fritt tilgjengelige åpne kilder på internett ble informasjon og data knyttet til Moss kommune samlet inn og kartlagt. Oppsummert ble det funnet 30 domener og subdomener og 248 e-postadresser. Videre ble e-postadressene brukt til å gjøre passordgjetting mot Moss kommunes Microsoft 365 tenant. Mot domenene ble det gjort sårbarhetsskanning for ytterligere kartlegging av tjenestene som kjører på disse domenene.

Moss kommune har ikke fremlagt dokumentasjon som viser at sikkerhetsnivået eller tiltakene er basert på behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene som kommunen står overfor.

4.3.21 Håndtering av brudd på personopplysningssikkerheten

Det ble informert i intervju at Moss kommune benytter et enhetlig system for innmelding av avvik, både knyttet til personvern og informasjonssikkerhet. Avvikssystemet er tilgjengelig gjennom kommunens kvalitetssystem. Alle kommunens ansatte får kommunal e-postadresse og derav tilgang til kvalitetssystemet. Vikarer på SFO, tilkallingsvikarer i barnehage og midlertidige knyttet til vaksineringen av COVID-19 får imidlertid ikke en kommunal e-postadresse og derfor heller ikke tilgang til kvalitetssystemet. Etter kommunens gjennomgang av datagrunnlaget er revisjonslaget informert om at de overnevnte stillingene får tilgang til å melde avvik, men ikke til kvalitetsdokumentasjonen.

Moss kommune har definert hva som anses som avvik og uønskede hendelser i dokumentet *«MK definisjoner for avvik og uønskede hendelser, skader og varslinger»*. Dokumentet gjelder alle typer avvik, men det er spesifisert at «personvernbrudd» og «personopplysninger på avveie» regnes som avvik. Prosessen for avvikshåndtering fremgår av dokumentet *«MK Retningslinjer for avvikshåndtering og årsaksanalyse»*.

Det fremgår videre av dokumentet «*MK Håndtering av brudd på personopplysningsloven*» hvordan avvik som involverer personopplysninger skal håndteres. Ifølge dette dokumentet skal ansatte melde brudd på personopplysningsloven i avvikssystemet. Avvik som involverer personopplysninger, vil automatisk sendes direkte til personvernombudet. Det fremgår videre at ved alvorlige brudd skal man også kontakte personvernombudet per telefon. Personvernombudet er deretter ansvarlig for å vurdere avviket og rapportere avviket til Datatilsynet innen fristen på 72 timer ved behov. Dette er også kommunisert gjennom dokumentet *«MK hvordan skal jeg som ansatt forholde meg til GDPR»*

Videre har Moss kommune dokumenterte retningslinjer og rutiner for hele avvikshåndteringsprosessen, herunder følgende dokumenter:

- «*Slettede avvik og skader*».
- «*Oversikt over avviksområder og avvikskategorier*».
- «*Melde avvik i web-applikasjonen for avvik*».
- «*Hvordan melde avvik på sikkerhets – og personvernbrudd*».
- «*Hvordan håndtere avvik og uønskede hendelser*».
- «*Retningslinjer for avvikshåndtering og årsaksanalyser*».

Hvorvidt ansatte er kjent med hvordan de skal melde avvik er nærmere beskrevet under problemstilling 2.

4.3.22 Gjennomføring av personvernkonsekvensvurderinger

Ansvar for å gjennomføre personvernkonsekvensvurderinger i Moss kommune ligger hos virksomhetene i linjen. Moss kommune har opplyst at de benytter malen til Foreningen Kommunal Informasjonssikkerhet (KiNS) for å gjennomføre personvernkonsekvensvurderinger. Malen legger opp til at ansatte først må gjøre en vurdering av behovet for å gjennomføre fullstendige personvernkonsekvensvurderinger.

Ved behov for å gjennomføre fullstendige personvernkonsekvensvurderinger skal følgende deltakere involveres:

- Behandlingsansvarlig eller representant for denne.
- Personvernombud.
- Representanter for de registrerte.
- Eventuelle andre, herunder prosjektleder, IT-sikkerhet og databehandlere.

Malen legger videre opp til at det skal gis en systematisk beskrivelse av behandlingen, gjennomføres en vurdering av nødvendighet og proporsjonalitet, og en konsekvensutredning. Malen inneholder til slutt punkter for å innhente de ulike deltakernes synspunkter og for ledelsens validering av vurderingen. Her kan ledelsen blant annet velge et alternativ for å anmode Datatilsynet om forhåndsdrøfting.

I dokumentet *«MK Personvern oversikt oppgaver og ansvar»* fremgår det at det er ledere som er ansvarlig for å gjennomføre personvernkonsekvensvurderinger, men Moss kommune har ikke fremlagt dokumenterte rutiner som beskriver når malen for personvernkonsekvensvurderinger skal tas i bruk. Revisjonslaget har fått opplyst at dersom ledere for eksempel ønsker å ta i bruk et nytt verktøy, så må de fylle ut et skjema som er tilgjengelig på kommunens intranett hvor de må oppgi informasjon om lagring av data og om det skal behandles sensitive personopplysninger. Ved behov vil skjemaet gå videre til personvernombudet. Personvernombudet vil deretter sørge for at de ansvarlige gjennomfører nødvendige vurderinger knyttet til etterlevelsen av GDPR, herunder at det gjennomføres personvernkonsekvensvurderinger ved behov. Revisjonslaget er videre forelagt en presentasjon som ble benyttet ifm. opplæring i personvernkonsekvensvurderinger. Det fremgår av presentasjonen at det skal vurderes

om det er behov for å gjennomføre en personvernkonsekvensvurdering ved ny behandling eller ved innføring av nytt system, og at malen skal benyttes. Det fremkom i intervju at denne presentasjonen ble gitt som en del av et større opplæringsprogram for ledere i 2018. Etter kommunens gjennomgang av datagrunnlaget ble revisjonslaget informert om at presentasjonen også var gitt i 2019 og 2020.

Det er opplyst at det ikke finnes en oversikt over gjennomførte personvernkonsekvensvurderinger i kommunen og at personvernombudet kun har vært involvert i én personvernkonsekvensvurdering siden mai 2021. Det er videre uttrykt gjennom intervju at det er begrenset kompetanse nedover i linjen for å kunne gjennomføre personvernkonsekvensvurderinger.

Moss kommune har fremlagt en gjennomført personvernkonsekvensvurdering. Revisjonslaget har ikke vurdert innholdet i den.

4.3.23 Dokumentere behovet for å gjennomføre personvernkonsekvensvurderinger

Moss kommune har fremlagt en mal for personvernkonsekvensvurdering som inneholder en mal for å vurdere og dokumentere behovet for å gjennomføre personvernkonsekvensvurderinger. Det er ikke fremlagt rutiner som beskriver når malen skal benyttes, men det er opplyst om en prosess som ansatte må gjennom dersom de eksempelvis ønsker å anskaffe et nytt verktøy. Denne prosessen er beskrevet nærmere under punkt 4.3.22.

4.3.24 Utpeke et personvernombud

Moss kommune har utpekt et personvernombud. At kommunen har et personvernombud kommuniseres gjennom flere dokumenter, herunder i *«MK Hvordan skal jeg som ansatt forholde meg til GDPR».* Det er også opplyst i intervju at dette kommuniseres gjennom Moss kommunes intranett.

Intervjuobjektene formidlet at de hadde inntrykk av at de ansatte er kjent med at kommunen har et personvernombud og at vedkommende kan kontaktes dersom de har spørsmål knyttet til personvern. Det er også gitt tilbakemelding fra intervjuobjektene at de ansatte opplever personvernombudet som en god sparringspartner dersom de har behov for bistand innen personvern.

4.3.25 Sørge for at personvernombudet kan utføre sine lovpålagte oppgaver

Det er opplyst at rollen som personvernombud i gamle Moss kommune lå til informasjonssikkerhetsansvarlig, men at det ble etablert en 100%-stilling til personvernombudet etter sammenslåingen. Denne beslutningen var basert på kommunens nye størrelse kombinert med at det var uheldig at beslutningstaker for informasjonssikkerhet var samme person som var rådgiver for personvern. Det fremgår av dokumentet «*HR Rolle- og oppgavebeskrivelse personvernombud*» hvilke oppgaver personvernombudet har i Moss kommune etter GDPR artikkel 37 og 39. Det er opplyst om at personvernombudet har mulighet til å ta videreutdanning og kurs for å styrke faglig kompetanse.

I intervju har det blitt gitt tilbakemeldinger på at det gjenstår mye arbeid knyttet til personvern i kommunen, herunder knyttet til utarbeidelse av protokoll og nye rutiner og dokumenter. Det er videre opplyst at personvernombudet i stor grad driver dette arbeidet fremover.

4.3.26 Personvernombudets uavhengighet

I dokumentet *«HR Rolle- og oppgavebeskrivelse personvernombud»* er det blant annet fastsatt at kommunen skal sikre at personvernombudet ikke mottar instrukser om utførelsen av oppgavene i stillingsinstruksen, og at kommunen skal sikre at personvernombudets oppgaver og plikter ikke medfører en interessekonflikt. I intervju er det gitt tilbakemelding på at personvernombudet ikke mottar instrukser om utførelsen av oppgavene sine. Det er imidlertid opplyst om at personvernombudet i stor grad utarbeider

rutiner og retningslinjer i kommunen. Det er videre opplyst om at dette skyldes ressurs- og kompetansesituasjonen i kommunen.

4.3.27 Overføring av personopplysninger til tredjestat

Det er fastsatt krav i malen for databehandleravtale om at enhver overføring til tredjestat krever skriftlig godkjenning fra behandlingsansvarlig. Det er ikke fremlagt rutiner som skal sikre at kravene til overføring av personopplysninger til tredjestat etterleves.

Etter kommunens gjennomgang av datagrunnlaget ble det informert om at «det ligger i lovverket og at databehandleravtaler ligger til grunn for alle avtaler».

Det er opplyst i intervju at kommunen ikke har oversikt over om kommunen overfører personopplysninger til tredjestat, selv om de vet at kommunen benytter noen leverandører som innebærer overføring, herunder Microsoft. Det er også opplyst at kommunen aktivt velger å ikke benyttes enkelte leverandører som følge av problematikken med overføringer til tredjestat, herunder Google.

4.3.28 Beskrive mål og overordnede rammer for behandling av personopplysninger i kommunen

Det fremgår av dokumentet «MK Internkontroll og kvalitet i Moss kommune» at all behandling av personopplysninger skal skje i samsvar med personvernprinsippene. I tillegg fremgår det av dokumentet «*MK Retningslinje for informasjonssikkerhet og personvern*» hvordan kommunen skal arbeide med informasjonssikkerhet og personvern i kommunen. Retningslinjene fokuserer i stor grad på mål og overordnede rammer for informasjonssikkerhet. Det er for eksempel flere steder kun referert til informasjonssikkerhet og ikke personvern. Øvrige krav til personvern er i begrenset grad beskrevet, herunder hvordan kommunen skal arbeide for å ivareta personvernprinsipper som formålsbegrensning og lovlighet, samt hvordan kommunen skal arbeide for å ivareta plikter knyttet til innebygd personvern og de registrertes rettigheter.

Det fremgår av de ovennevnte dokumentene at disse ikke godkjent og implementert på tidspunktet for revisjonen.

4.3.29 Utarbeide nødvendige rutiner og retningslinjer for behandling av personopplysninger basert på en risikovurdering

Moss kommune har fremlagt flere rutiner og retningslinjer for behandling av personopplysninger som beskrevet under punkt 4.3.13. Det er ikke opplyst hva som ligger til grunn for rutinene og retningslinjene som kommunen har utarbeidet.

Kommunen har i dokumentet «MK Oversikt over fagsystem for personopplysningsloven (Behandlingsprotokoll)» kartlagt de ulike fagsystemene kommunen bruker, med tilhørende databehandleravtaler, juridisk grunnlag og formål. Revisjonslaget er informert om at dette er en ufullstendig og utdatert oversikt for gamle Moss og Rygge kommune. Moss kommune har derimot ikke kartlagt sine behandlingsaktiviteter og det er ikke gjennomført risikovurderinger av disse.

4.3.30 Basere sitt styringssystem for personvern på anerkjente standarder

Det fremgår av dokumentet *«MK Retningslinje informasjonssikkerhet og personvern»* at retningslinjene er *«utarbeidet ihht NS-EN ISO/IEC 27001:2017; NS-EN ISO/IEC 27002:2017; NS-EN ISO/IEC 27004:2016 og NS-EN ISO/IEC 27005:2018, samt anbefalinger fra Datatilsynet og NSM.»*

Som beskrevet under punkt 4.3.13 har Moss kommune utarbeidet en internkontrollstruktur med styrende, utførende og kontrollerende elementer for informasjonssikkerhet og personvern. Slik revisjonslaget forstår det, består den styrende dokumentasjonen for personvern av *«MK Internkontroll og kvalitet i Moss kommune», «MK Retningslinje for informasjonssikkerhet»* og *«MK Personvern oversikt oppgaver og ansvar».* I disse dokumentene er blant annet målsetninger og ansvarfordelingen knyttet til informasjonssikkerhet og personvern i kommunen beskrevet. Dokumentene *«MK Internkontroll og kvalitet i Moss kommune»* og *«MK Retningslinje for informasjonssikkerhet»* er imidlertid ikke godkjent på tidspunktet for revisjonen.

Videre har Moss kommune utarbeidet gjennomførende dokumenter i form av generelle rutiner som gjelder for hele kommunen og noen mer spesifikke rutiner nedover i linjen. Det er også fremlagt dokumentasjon på flere sikkerhetstiltak, slik som tilgangskontroll. Det er imidlertid ikke fremlagt dokumentasjon på at tiltakene er valgt på bakgrunn av kartlagte behandlingsaktiviteter eller gjennomførte risikovurderinger. Etter kommunens gjennomgang av datagrunnlaget fikk revisjonslaget opplyst at tiltakene ikke eksplisitt er valgt på bakgrunn av gjennomførte risikovurderinger og kartlagte behandlingsaktiviteter, men at de er et resultat av prosesser og risikovurderinger.

I dokumentene *«MK Internkontroll og kvalitet i Moss kommune»* og *«MK Retningslinje for informasjonssikkerhet»* har Moss kommune har også beskrevet en rekke kontrolltiltak som skal gjennomføres, herunder ledelsens gjennomgang både sentralt og i linjen, samt internrevisjoner.

4.4 Vurderinger

Moss kommune har i noen grad etablert tiltak for å sikre at personvernprinsippene etterleves	

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene knyttet til personvernprinsippene, jf. § GDPR artikkel 5.

Revisjonslaget har sett flere eksempler på at Moss kommune aktivt arbeider med å ivareta prinsipper som dataminimering og integritet og konfidensialitet, både i dokumentasjon og i intervju. Revisjonslaget ser positivt på dette. Det er imidlertid avdekket forbedringspotensial knyttet hvordan kommunen sikrer at prinsipper som formålsbegrensning, lovlighet, riktighet og lagringstid etterleves. Kommunen informerte i sin gjennomgang av datagrunnlaget at «prinsippene ligger i lovverket». Revisjonslaget bemerker at kommunen også må kunne fremlegge dokumentasjon som viser hvordan disse prinsippene skal etterleves. Dokumentasjon på dette er ikke fremlagt for revisjonslaget. Uten dokumentasjon kan ikke kommunen påvise at de etterlever disse prinsippene i tråd med prinsippet om ansvar, jf. GDPR artikkel 5 nr. 2.

Revisjonslaget vurderer at svakhetene i stor grad kan utbedres ved å etablere en tilfredsstillende og fullstendig protokoll over behandlingsaktiviteter og dokumentasjon av hvilke behandlingsgrunnlag kommunen benytter seg av.

Moss kommune har i noen grad etablert tiltak for å sikre at alle behandlingsaktiviteter har et lovlig behandlingsgrunnlag	

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene for å sikre lovlig behandlingsgrunnlag, jf. GDPR artikkel 6 og personopplysningsloven § 8.

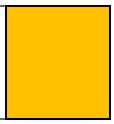
Det er positivt at kommunen har veiledning som beskriver at kommunen må vurdere og dokumentere behandlingsgrunnlag for hver enkelt behandling og at det gis en beskrivelse over når de ulike behandlingsgrunnlagene kan benyttes. Kommunen informerte i sin gjennomgang av datagrunnlaget at de vurderer behandlingens lovlighet når det gjennomføres en personvernkonsekvensvurdering. Revisjonslaget bemerker i den anledning at dette tiltaket i seg selv ikke er tilstrekkelig for å sikre at alle behandlingsaktiviteter har et lovlig behandlingsgrunnlag. Det vises til at personvernkonsekvensvurderinger ikke vil bli gjennomført for alle behandlingsaktiviteter. Revisjonslaget kommer tilbake til vurderingen av personvernkonsekvensvurderinger i en senere vurdering. Det er avdekket forbedringspotensial knyttet til hvordan kommunen sikrer at alle behandlingsaktiviteter har et lovlig behandlingsgrunnlag. Det er ikke fremlagt dokumentasjon som viser hvilke behandlingsgrunnlag kommunen baserer seg på. Uten dokumentasjon kan ikke kommunen påvise at alle behandlinger har et lovlig behandlingsgrunnlag etter GDPR artikkel 6 i tråd med prinsippet om ansvar, jf. GDPR artikkel 5 nr. 2. Det vil også være vanskelig å gjennomføre kontrollaktiviteter for å sikre at kravene etterleves. Kommunen må derfor sørge for at behandlingsgrunnlag blir dokumentert.

Moss kommune har i stor grad etablert tiltak for å sikre at vilkårene for samtykke ivaretas

Revisjonslaget vurderer at Moss kommune i stor grad oppfyller kravene knyttet til gyldig samtykke jf. GDPR artikkel 7 og personopplysningsloven § 5.

Etter revisjonslagets vurdering har kommunen etablert tilfredsstillende veiledning og retningslinjer som skal sikre at vilkårene for samtykke ivaretas. Det er imidlertid avdekket mindre forbedringspotensial knyttet til beskrivelsen i dokumentet *«MK Hvordan skal jeg som ansatt forholde meg til GDPR»* om at samtykker skal benyttes der kommunen ikke har hjemmel i lov. Etter revisjonens vurdering kan denne setningen være misvisende. Beskrivelsen kan forstås dithen at kommunen ikke kan benytte seg av behandlingsgrunnlag som avtale eller berettiget interesse. Dette kan medføre at kommunen benytter samtykke som behandlingsgrunnlag i tilfeller hvor kommunen burde benyttet seg av et annet behandlingsgrunnlag. Dette kan igjen påvirke samtykkets gyldighet. I visse tilfeller vil det ikke være anledning til å benytte samtykke av hensyn til at det ikke er mulig å oppfylle vilkåret om frivillighet. Behandling av personopplysninger om ansatte kan være et eksempel på slik behandling. Kommunen bør derfor vurdere å tydeliggjøre formuleringen om når samtykke skal benyttes.

Moss kommune har i liten grad etablert tiltak for å sikre at særlige kategorier av personopplysninger kun behandles når det er lov i henhold til GDPR artikkel 9



Revisjonslaget vurderer at Moss kommune i liten grad oppfyller kravene knyttet til å sikre at særlig kategorier av personopplysninger kun behandles når det er lov, jf. GDPR artikkel 9 og personopplysningsloven §§ 6, 7 og 9.

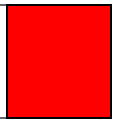
Moss kommune har utarbeidet veilederen «*MK Personvernveileder*» som beskriver hva særlige kategorier av personopplysninger er og at det «gjelder særlig strenge krav til lovlig behandling» av slike opplysninger. Kommunen informerte i sin gjennomgang av datagrunnlaget at de gjennom personvernkonsekvensvurderingene sikrer at særlige kategorier av personopplysninger kun behandles når det er lovlig. Revisjonslaget bemerker i den anledning at dette tiltaket i seg selv ikke er tilstrekkelig for å sikre at særlige kategorier av personopplysninger kun behandles når det er lovlig. Det vises til at en person-

vernkonsekvensvurdering ikke vil bli gjennomført for alle behandlingsaktiviteter, selv ved særlige kategorier av personopplysninger. Revisjonslaget kommer tilbake til vurderingen av personvernkonsekvensvurderinger i en senere vurdering.

Det er avdekket vesentlig forbedringspotensial knyttet til hvordan kommunen sikrer at all behandling av særlige kategorier av personopplysninger er basert på et av unntakene i GDPR artikkel 9. Det er ikke fremlagt dokumentasjon som viser hvilke grunnlag kommunen baserer seg på ved behandling av særlige kategorier av personopplysninger. Uten dokumentasjon kan ikke kommunen påvise at all behandling av særlige kategorier av personopplysninger er lovlig i henhold til GDPR artikkel 9 i tråd med prinsippet om ansvar, jf. GDPR artikkel 5 nr. 2. Det vil også være vanskelig å gjennomføre kontrollaktiviteter for å sikre at kravene etterleves. Kommunen må derfor sørge for at grunnlaget for behandling av særlige kategorier av personopplysninger blir dokumentert. Kommunen bør blant annet fastsette i rutine at resultatet av vurderinger knyttet til hvilket unntak som kommer til anvendelse, skal dokumenteres.

Revisjonslaget bemerker at avviket anses som alvorlig ettersom en kommune vil behandle et stort antall særlige kategorier av personopplysninger.

Moss kommune har ikke etablert tiltak for å sikre at fødselsnummer og andre entydige identifikasjonsmidler kun behandles når det foreligger et saklig behov



Revisjonslaget vurderer at Moss kommune ikke oppfyller kravene knyttet til å sikre at entydige identifikasjonsmidler kun behandles når det foreligger et saklig behov, jf. personopplysningsloven § 12.

Det er avdekket vesentlig forbedringspotensial knyttet til hvordan Moss kommune sikrer at det gjøres vurderinger av om det foreligger et saklig behov for sikker identifisering ved innsamling av fødselsnummer og andre entydige identifikasjonsmidler. Kommunen har ikke fremlagt dokumentasjon som viser hvordan de arbeider med å sikre at disse kravene etterleves. Revisjonslaget legger dermed til grunn at kommunen ikke gjør noe særskilt for å sikre at fødselsnummer og andre entydige identifikasjonsmidler kun behandles når det foreligger et saklig behov for sikker identifisering.

Kommunen informerte i sin gjennomgang av datagrunnlaget at de tolker lovverket til at det ikke er et dokumentasjonskrav. Revisjonslaget vurderer at for å overholde Personopplysningsloven § 12 og kommunelovens bestemmelser om internkontroll må det foreligge dokumentasjon som viser til at fødselsnummer og andre entydige identifikasjonsmidler kun skal behandles når det foreligger et saklig behov. Kommunen informerte videre at det ble «oversendt eksempler», revisjonslaget har ikke observert dette i dokumentasjonen som er oversendt av Moss kommune.

Moss kommune har i noen grad etablert tiltak for å ivareta informasjonsplikten overfor registrerte

Revisjonslaget vurderer at Moss kommune i noen grad har etablert tiltak for å ivareta informasjonsplikten overfor registrerte, jf. GDPR artikkel 12-14.

Moss kommune har utarbeidet en personvernerklæring som gjelder kommunens behandling av personopplysninger for innbyggere og ansatte. Det er imidlertid avdekket forbedringspotensial ved at det ikke er utarbeidet mer spesifikke personvernerklæringer for kommunalområdene slik kommunen har beskre-

vet at de skal. Revisjonslaget vil også bemerke at informasjonen i personvernerklæringen er svært generell. Dette kan medføre at kommunens ansatte ikke får den informasjonen de har krav på i henhold til GDPR artikkel 12-14.

Moss kommune har i noen grad etablert tiltak for å sikre at den registrertes rett til innsyn ivaretas

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene knyttet til de registrertes rett til innsyn, jf. GDPR artikkel 15.

Moss kommune har utarbeidet veiledning om hva retten til innsyn etter GDPR innebærer. Det er imidlertid avdekket forbedringspotensial knyttet til at det ikke er spesifisert hva ansatte skal gjøre dersom de mottar anmodninger om innsyn etter GDPR. Revisjonslaget bemerker at Moss kommune har rutiner for innsyn, men at disse rutinene omhandler innsyn etter andre regelverk, herunder offentleglova og forvaltningsloven. Etter revisjonslagets vurdering er ikke rutinene egnet for å ivareta alle kravene til innsyn etter GDPR artikkel 15 da de ikke er tydelige på forskjellene mellom innsynsreglene i GDPR og innsynsreglene etter andre særlover. Det er viktig at kommunen har tydelige rutiner for hvilke krav som gjelder ved innsyn etter GDPR for å unngå misforståelser ved håndteringen av slike anmodninger, herunder registrertes rett til informasjon og krav om kopi av alle personopplysninger.

Revisjonslaget vil også bemerke at det er gitt varierende informasjon om hvem som er ansvarlig for å håndtere anmodninger om innsyn etter GDPR. Noen mener slike anmodninger skal håndteres i linjen, mens andre mener at slike anmodninger skal sendes til personvernombudet. Når Moss kommunes personvernerklæring åpner for at anmodninger om innsyn kan sendes til enhver ansatt i kommunen, er det svært viktig at kommunen utarbeider tydelige rutiner for hvordan slike anmodninger skal håndteres og at disse kommuniseres til de ansatte. Dette er viktig for å sikre at anmodningene håndteres på riktig måte og innen de fristene som kommunen er underlagt.

Moss kommune har i liten grad etablert tiltak for å sikre at den registrertes rett til retting ivaretas

Revisjonslaget vurderer at Moss kommune i liten grad oppfyller revisjonskriteriet.

Moss kommune har utarbeidet veiledning om hva retten til retting innebærer, men det er avdekket et vesentlig forbedringspotensial knyttet til at det ikke er spesifisert hva ansatte skal gjøre dersom de mottar anmodninger om retting. Når Moss kommunes personvernerklæring åpner for at anmodninger om retting kan sendes til enhver ansatt i kommunen, er det svært viktig at kommunen utarbeider tydelige rutiner for hvordan slike anmodninger skal håndteres og at disse kommuniseres til de ansatte. Dette er viktig for å sikre at anmodningene håndteres på riktig måte og innen de fristene som kommunen er underlagt.

Moss kommune har i liten grad etablert tiltak for å sikre at den registrertes rett til sletting ivaretas

Revisjonslaget vurderer at Moss kommune i liten grad oppfyller revisjonskriteriet.

Moss kommune har utarbeidet veiledning om hva retten til sletting innebærer, men det er avdekket et vesentlig forbedringspotensial knyttet til at det ikke er spesifisert hva ansatte skal gjøre dersom de mottar anmodninger om sletting av personopplysninger. Når Moss kommunes personvernerklæring åpner for at anmodninger om sletting kan sendes til enhver ansatt i kommunen, er det svært viktig at kommunen utarbeider tydelige rutiner for hvordan slike anmodninger skal håndteres og at disse kommuniseres til de ansatte. Dette er viktig for å sikre at anmodningene håndteres på riktig måte og innen de fristene som kommunen er underlagt.

Moss kommune har i noen grad etablert tiltak for å sikre at den registrertes rett til begrensing ivaretas

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller revisjonskriteriet.

Moss kommune har utarbeidet veiledning om hva retten til begrensning innebærer. Kommunen informerte i sin gjennomgang av datagrunnlaget at retten til begrensning er nevnt i rutinen for automatiserte individuelle avgjørelser. Revisjonslaget vurderer dokumentet til å omhandle en begrenset mengde behandlinger, da det kun omtaler automatiserte individuelle avgjørelser. Det er avdekket forbedringspotensial knyttet til at det ikke er spesifisert hva ansatte skal gjøre dersom de mottar anmodninger om begrensning av behandling. Revisjonslaget vurderer ikke dette like alvorlig som at kommunen ikke har dokumenterte rutiner for innsyn, retting og sletting, da retten til begrensning trolig ikke vil være like aktuell for kommunen som disse øvrige rettighetene for de registrerte.

Moss kommune har i noen grad etablert tiltak for å sikre at at den registrertes rett til dataportabilitet ivaretas

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene knyttet til de registrertes rett til dataportabilitet, jf. GDPR artikkel 20..

Moss kommune har utarbeidet veiledning om hva retten til dataportabilitet innebærer, men det er avdekket forbedringspotensial knyttet til at det ikke er spesifisert hva ansatte skal gjøre dersom de mottar anmodninger om dataportabilitet. Revisjonslaget vurderer ikke dette like alvorlig som at kommunen ikke har dokumenterte rutiner for innsyn, retting og sletting, da retten til dataportabilitet trolig ikke vil være like aktuell for kommunen som disse rettighetene for de registrerte.

Moss kommune har i noen grad etablert tiltak for å sikre at at den registrertes rett til å protestere ivaretas

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene knyttet til de registrertes rett til å protestere, jf. GDPR artikkel 21.

Moss kommune har utarbeidet veiledning om hva den registrertes rett til å protestere innebærer, men det er avdekket forbedringspotensial knyttet til at det ikke er spesifisert hva ansatte skal gjøre dersom de mottar henvendelser fra registrerte som ønsker å protestere på den aktuelle behandlingen. Revisjonslaget vurderer ikke dette like alvorlig som at kommunen ikke har dokumenterte rutiner for innsyn, retting og sletting, da retten til protest trolig ikke vil være like aktuell for kommunen som disse øvrige rettighetene for de registrerte.

Moss kommune har i noen grad etablert tekniske og organisatoriske tiltak for å sikre og påvise at kommunens behandlinger utføres i samsvar med personvernforordningen	

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene knyttet til tekniske og organisatoriske tiltak, jf. GDPR artikkel 24.

Moss kommune har utarbeidet et styringssystem for personvern som inneholder styrende, gjennomførende og kontrollerende elementer. Revisjonslaget mener at flere av tiltakene som Moss kommune har planlagt, og til en viss grad iverksatt, er godt egnet for å sikre at kommunen etterlever kravene i GDPR. Revisjonslaget vil særlig trekke frem etableringen av kvalitetsutvalgene som en hensiktsmessig måte å drive internkontroll på i en kommune. Videre vil revisjonslaget også trekke frem etableringen av kommunens sikkerhet- og personvernutvalg som et positivt tiltak.

Det er imidlertid avdekket forbedringspotensial knyttet til at kommunen ikke er helt i mål med å etablere styringssystemet på personvernområdet. Det er avdekket forbedringspotensial knyttet til utarbeidelse av dokumentasjon, fordeling av ansvar og kommunikasjon av hva dette ansvaret innebærer, samt gjennomføringen av planlagte kontrollaktiviteter. Revisjonslaget vurderer også at opplæringen av linjeledere ikke har vært tilstrekkelig.

Dokumentasjonen som Moss kommune har fremlagt bærer preg av at kommunen ikke er helt i mål med å etablere et styringssystem for personvern i ny kommune. Flere av dokumentene som Moss kommune har fremlagt er i utkastform og/eller er ikke godkjent på tidspunktet for revisjon. Revisjonslaget vil også bemerke at kommunen har dokumentasjon som viser til rutiner som ikke finnes. Dette gjelder for eksempel *«MK Personvernveileder»*. Dette kan medføre forvirring og misforståelser knyttet til hva som er gjeldende praksis i Moss kommune. Videre har ikke Moss kommune utarbeidet en fullstendig protokoll over behandlingsaktiviteter. Moss kommune har heller ikke gjennomført dokumenterte risikovurderinger av sine behandlingsaktiviteter. Det at kommunen ikke har utarbeidet en fullstendig protokoll over behandlingsaktiviteter eller gjennomført dokumenterte risikovurderinger knyttet til behandlingsaktivitetene, medfører at Moss kommune ikke kan dokumentere at styringssystemet er basert på behandlingenes art, omfang, formål og sammenhengen de utføres i, samt risikoene som kommunen står overfor. Disse aktivitetene skal sikre at kommunen etablerer de tiltakene som er nødvendig og at styringssystemet blir effektivt for virksomheten. Revisjonslaget mener derfor at kommunen bør prioritere å utarbeide en fullstendig protokoll og å gjennomføre risikovurderinger av behandlingsaktivitetene for å sikre at det videre arbeidet med styringssystemet blir hensiktsmessig.

I Moss kommune er det operative ansvaret for personvern delegert til linjeledere. Revisjonslaget mener at slik delegering av ansvaret er hensiktsmessig i en kommune på størrelse med Moss. Når ansvaret er delegert slik, er det svært viktig at kommunen sikrer at linjelederne er klar over sitt ansvar og at de vet hvordan de skal utøve dette ansvaret. Det er imidlertid gitt tilbakemeldinger om at ansvarsfordelingen er uklar og at det mangler kompetanse på personvernområdet nedover i organisasjonen. Videre er det gitt tilbakemelding om at opplæringen knyttet til personvern er noe mangelfull. Dette kan medføre at de delegerte oppgavene på personvernområdet ikke blir gjennomført på en tilfredsstillende måte. At det ikke gis tilstrekkelig opplæring på personvernområdet slik at linjeledere er i stand til å forstå hva ansvaret innebærer, kan også medføre at de ikke vet når de har behov for å involvere personer med særskilt kompetanse innen personvern. Dette kan igjen medføre at viktige vurderinger knyttet til personvern ikke blir gjennomført.

Revisjonslaget ser positivt på at Moss kommune har planlagt å gjennomføre flere systematiske kontrolltiltak på personvernområdet, herunder ledelsens gjennomgang både sentralt og i linjen, egenkontroll og internrevisjon. Flere av de planlagte aktivitetene fra kommunen sentralt er imidlertid ikke gjennomført ennå. Revisjonslaget vil trekke frem viktigheten av å gjennomføre kontrolltiltak på personvernområdet for å sikre at kravene etterleves, særlig når det operative ansvaret er delegert til linjeledere.

Moss kommune har i noen grad etablert tiltak for å ivareta krav til innebygd personvern og personvern som standardinnstilling

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene til innebygd personvern og personvern som standardinnstilling, jf. GDPR artikkel 25.

Moss kommune har fremlagt dokumentasjon hvor det er innarbeidet elementer av krav knyttet til innebygd personvern, herunder i malen for databehandleravtaler og i malen for personvernkonsekvensvurderinger.

Det er imidlertid avdekket forbedringspotensial knyttet til at Moss kommune ikke har en mer strukturert tilnærming til hvordan kommunen skal arbeide for å sikre kravet til innebygd personvern i sine rutiner, særlig i anskaffelsesprosesser. Revisjonslaget mener likevel at risikoen for at kravet ikke etterleves reduseres ved at kommunen sørger for å involvere personvernombudet i anskaffelsesprosesser. Revisjonslaget ser også positivt på at kommunen skal gjennomføre et eget kurs om temaet for kommunikasjonsavdelingen.

Moss kommune har ikke etablert tiltak som sikrer at de avdekker eller følger opp felles behandlingsansvar

Revisjonslaget vurderer at Moss kommune ikke oppfyller kravene til å avdekke og følge opp felles behandlingsansvar, jf. GDPR artikkel 26.

Det er avdekket vesentlig forbedringspotensial knyttet til hvordan Moss kommune vurderer og eventuelt følger opp felles behandlingsansvar. Moss kommune har ikke fremlagt dokumentasjon på hvordan de arbeider med å sikre at kravene til felles behandlingsansvar etterleves. Revisjonslaget legger dermed til grunn at kommunen ikke gjør noe særskilt for å sikre at kravene til felles behandlingsansvar etterleves.

Moss kommune har i noen grad etablert tiltak for å sikre at databehandlere gir tilstrekkelige garantier for å ivareta krav til personvern

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene knyttet til å sikre at databehandlere gir tilstrekkelig garantier, jf. GDPR artikkel 28.

Revisjonen har avdekket at Moss kommune ikke har oversikt over sine databehandlerrelasjoner og at kommunen ikke gjennomfører revisjoner/kontroller av databehandlere. Revisjonslaget ser positivt på at kommunen har planlagt å anskaffe et nytt verktøy for å holde oversikt over databehandlerrelasjoner og at kommunen har planlagt å begynne med revisjoner/kontroller. Kommunen bør sørge for at revisjonene/kontrollene er basert på en risikobasert tilnærming. Kommunen bør også sørge for å kommunisere tydelig hvem som er ansvarlig for gjennomføringen av slike revisjoner/kontroller for å sikre at dette etterleves.

Moss kommune har i svært stor grad etablert tilstrekkelige tiltak for å sikre at det inngås databehandleravtaler

Revisjonslaget vurderer at Moss kommune oppfyller kravene knyttet til at det inngås databehandleravtaler med alle databehandlere, jf. GDPR artikkel 28, fullt ut.

Revisjonslaget vil for øvrig bemerke at det er utarbeidet svært mange dokumenter som beskriver det samme. Dette kan være egnet til forvirring blant ansatte og kommunen kan derfor vurdere å forenkle rutinene.

Moss kommune har i liten grad sørget for å utarbeide en fullstendig protokoll over behandlingsaktiviteter

Revisjonslaget vurderer at Moss kommune i liten grad oppfyller kravet om å føre skriftlig protokoll over behandlingsaktiviteter, jf. GDPR artikkel 30.

Det er avdekket vesentlig forbedringspotensial knyttet til at Moss kommune ikke har utarbeidet en fullstendig protokoll over behandlingsaktiviteter som tilfredsstiller kravene i GDPR artikkel 30. Oversikten som Moss kommune har fremlagt gir informasjon om hvilke fagsystemer kommunen behandler personopplysninger i, men ikke hvilke behandlingsaktiviteter som gjennomføres. Dokumentet mangler derfor vesentlige punkter som skal beskrives etter GDPR artikkel 30, herunder hvilke personopplysninger som behandles og hvilke registrerte som er omfattet av behandlingene. Dette medfører også at formål ikke blir beskrevet på en tilstrekkelig måte. Revisjonslaget mener at dette er et alvorlig avvik som påvirker hvorvidt kommunen kan etterleve flere sentrale bestemmelser i GDPR. At det ikke foreligger en tilfredsstillende protokoll over behandlingsaktiviteter, medfører blant annet at Moss kommune ikke får gjennomført risikovurderinger av alle behandlingsaktivitetene. Kommunen får derfor ikke dannet et tilstrekkelig grunnlag for å vurdere hvilke tiltak som skal iverksettes for å etablere en tilfredsstillende internkontroll. En tilfredsstillende protokoll over behandlingsaktiviteter vil også bidra til at Moss kommune kan forbedre sin etterlevelse av andre krav i GDPR, herunder krav til å avdekke felles behandlingsansvar og definere slettefrister. Avviket bør derfor gis høy prioritet.

Revisjonslaget vil bemerke at dette er et avvik kommunen selv er klar over og som de har fokus på å forbedre. Revisjonslaget vil i den anledning trekke frem at det er positivt at kommunen har anskaffet et digitalt verktøy for å gjennomføre dette arbeidet.

Moss kommune har i liten grad gjennomført risikovurderinger av kommunens behandlingsaktiviteter

Revisjonslaget vurderer at Moss kommune i liten grad oppfyller kravet om å gjennomføre risikovurderinger for å fastsette et egnet sikkerhetsnivå, jf. GDPR artikkel 32.

Revisjonslaget ser positivt på at Moss kommune har dokumenterte krav om at det skal gjennomføres årlige risikovurderinger og at det skal gjennomføres fortløpende risikoer basert på behov og endringer. Revisjonslaget ser også positivt på at det er gjennomført enkelte risikovurderinger knyttet til spesifikke behandlinger.

Det er imidlertid avdekket vesentlig forbedringspotensial knyttet at Moss kommune ikke har gjennomført helhetlige og dokumenterte risikovurderinger av kommunens behandlingsaktiviteter. At det ikke er gjennomført risikovurderinger medfører blant annet at kommunen ikke kan dokumentere at tekniske og organisatoriske tiltak er egnede for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen som Moss kommune står overfor. Dette bør derfor gis høy prioritet.

Kommunen informerte, etter sin gjennomgang av datagrunnlaget, om dokumentasjon hvor det stod beskrevet retningslinjer for hvordan de skal gjennomføre risikovurderinger i Moss kommune. Revisjonslagets vurdering er at det nevnte dokumentet ikke er retningslinjer for hvordan gjennomføre en risikovurdering, men heller en overordnet tilnærming til risiko i Moss kommune.

Det er også avdekket et mindre forbedringspotensial knyttet til kompetansen for å gjennomføre risikovurderinger nedover i organisasjonen. Manglende kompetanse på risikovurderinger nedover i organisasjonen kan medføre at risikovurderinger ikke blir gjennomført eller at de ikke blir gjennomført på en tilstrekkelig måte. Dette kan igjen medføre at kommunen ikke oppdager risikoer som burde vært hensyntatt.

Moss kommune har i noen grad etablert tiltak for å oppnå egnet sikkerhetsnivå

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene om å etablere tiltak for å oppnå egnet sikkerhetsnivå, jf. GDPR artikkel 32.

Moss kommune har etablert flere tiltak for å ivareta personopplysningssikkerheten. Revisjonslaget ser særlig positivt på at kommunen har etablert tekniske tiltak for å beskytte personopplysninger fra trusselaktører på utsiden av kommunen. Penetrasjonstesten som ble gjennomført i forbindelse med revisjonen viser at Moss kommune sine systemer er godt nok sikret til at det ikke lyktes å oppnå full tilgang under testperioden gitt tiden som var tilgjengelig. Det ble funnet noen svakheter, men den helhetlige vurderingen er at et vellykket datainnbrudd mest sannsynlig vil inkludere sosial manipulasjon av ledere eller medarbeidere gjennom falske e-poster. Moss kommune har konfigurert SPF og DMARC og er derfor godt beskyttet mot at trusselaktører sender forfalsket e-post fra Moss kommunes domene.

Det er imidlertid avdekket forbedringspotensial knyttet til at Moss kommune ikke kan dokumentere at de har fastsatt et *egnet* sikkerhetsnivå. Moss kommune har definert sikkerhetsmål og en sikkerhetsstrategi i *«MK retningslinje informasjonssikkerhet og personvern»*, som gir føringer for ønsket sikkerhetsnivå. Moss kommune ikke fremlagt en protokoll over behandlingsaktiviteter eller dokumenterte risikovurderinger som viser at sikkerhetsnivået er basert på behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene som kommunen står overfor. I tillegg foreligger dokumentet *«MK retningslinje informasjonssikkerhet og personvern»* kun i utkastform og er ikke godkjent på tidspunktet for revisjon.

Moss kommune har i svært stor grad tiltak for å sørge for at avvik blir håndtert

Revisjonslaget vurderer at Moss kommune oppfyller kravene knyttet til håndtering og dokumentering av alle brudd på personopplysningssikkerhet, jf. GDRP artikkel 33-34, fullt ut.

Hvorvidt ansatte er kjent med hvordan de skal melde avvik er nærmere beskrevet under problemstilling 2.

Kommunen har i noen grad etablert tiltak for å sikre at personvernkonsekvensvurderinger gjennomføres når det er påkrevd

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravene knyttet til gjennomføring og dokumentering av personvernkonsekvensvurderinger når det er påkrevd, jf. GDPR artikkel 35.

Etter revisjonens vurdering er malen for personvernkonsekvensutredninger som kommunen benytter egnet til å sikre at det gjøres gode og utdypende vurderinger som tilfredsstiller kravene i GDPR artikkel 35. Det er imidlertid avdekket forbedringspotensial knyttet til at Moss kommune ikke har tydelige rutiner for når malen skal benyttes. Dette kan medføre at personvernkonsekvensvurderinger ikke blir gjennomført når det er påkrevd, og at kommunen dermed ikke oppdager risikoer som burde vært dempet. Risikoen for at personvernkonsekvensvurderinger ikke gjennomføres reduseres noe ved at personvernombudet blir involvert i anskaffelsesprosesser. Det kan imidlertid også oppstå behov for å gjennomføre personvernkonsekvensvurderinger utenom anskaffelsesprosesser, for eksempel dersom man skal begynne å behandle personopplysninger på en ny måte enn man har gjort før. Det er gitt noe opplæring til ledere om at personvernkonsekvensvurderinger skal gjennomføres i slike tilfeller, men revisjonslaget vil bemerke at det er gitt tilbakemeldinger om at det er for lite kompetanse på personvern nedover i organisasjonen til å gjennomføre personvernkonsekvensvurderinger. Revisjonslaget mener derfor at kommunens tiltak ikke er tilstrekkelige for å sikre at personvernkonsekvensvurderinger gjennomføres.

Kommunen har i noen grad etablert tiltak for å sikre at behovet for å gjennomføre personvernkonsekvensvurderinger dokumenteres

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravet knyttet til å dokumentere vurderinger av om kommunen er pålagt å gjennomføre personvernkonsekvensvurderinger jf. GDPR artikkel 35 nr. 1, jf. GDPR artikkel 5. nr. 2.

Det er positivt at kommunen benytter en mal som inneholder en forhåndsvurdering. Det er avdekket mindre forbedringspotensial knyttet til at Moss kommune ikke har definert når malen skal benyttes. Om dette ikke defineres, kan det medføre at behovet for personvernkonsekvensvurderinger ikke blir dokumentert.

Moss kommune har utpekt et personvernombud

Revisjonslaget vurderer at Moss kommune oppfyller kravet om å utpeke et personvernombud, jf. GDPR artikkel 37, fullt ut.

Moss kommune har i stor grad sørget for at personvernombudet kan utføre sine lovpålagte oppgaver

Revisjonslaget vurderer at Moss kommune i stor grad oppfyller kravet knyttet til å sørge for at personvernombudet kan utføre sine lovpålagte oppgaver, jf. GDPR artikkel 38 og 39.

Revisjonslaget vurderer det som positivt at kommunen har satt av en 100%-stilling til personvernombudet. Det er imidlertid avdekket et forbedringspotensial knyttet til at kommunen har et etterslep på det

utførende arbeidet knyttet til personvern. Revisjonslaget er informert om at det er personvernombudet som i stor grad driver dette arbeidet fremover. Revisjonslaget vurderer at om Moss kommune ikke setter av tilstrekkelig med ressurser som kan ta igjen etterslepet på det utførende arbeidet, kan dette medføre at personvernombudet ikke får utført sine lovpålagte oppgaver.

Moss kommune har i stor grad sørget for å sikre personvernombudets uavhengighet

Revisjonslaget vurderer at Moss kommune i stor grad oppfyller kravet knyttet til å sikre at personvernombudets uavhengighet, jf. GDPR artikkel 38 nr. 3 og nr. 6.

Moss kommune har sikret at personvernombudet ikke mottar instrukser i sin stilling. Det er imidlertid avdekket forbedringspotensial knyttet til andre aspekter ved personvernombudets uavhengighet. Grunnet ressursmangel utarbeider i dag personvernombudet enkelte rutiner og retningslinjer. At personvernombudet gjennomfører disse oppgavene, kan medføre en interessekonflikt og sette personvernombudet i en situasjon hvor vedkommende ikke er uavhengig ved utførelsen av sine kontrolloppgaver. Av denne grunn bør kommunen være varsom med å sette personvernombudet til å utøve operativt arbeid som å utarbeide rutiner og retningslinjer. Det er derfor viktig at kommunen sørger for å sette av ressurser til å utføre det planlagte arbeidet på personvernområdet.

Moss kommune har i noen grad sørget for å sikre at personopplysninger overføres i tråd med kravene i GDPR artikkel 44-50

Revisjonslaget vurder at Moss kommune i noen grad oppfyller kravene knyttet til overføring av personopplysninger til tredjestat er ivaretatt, jf. GDPR artikkel 44-50.

Det er positivt at kommunen har et bevisst forhold til at de ikke ønsker å overføre personopplysninger til tredjestater og at kommunen derfor unngår enkelte leverandører. Det er imidlertid avdekket forbedringspotensial knyttet til at kommunen ikke har en mer strukturert tilnærming til hvordan kommunen skal arbeide for å sikre at overføringer ikke skjer, eventuelt at overføringer skjer i tråd med de kravene som er fastsatt i GPDR artikkel 44-50. Kommunen bør utarbeide en oversikt over hvilke overføringer som gjennomføres i dag og utarbeide en plan for å håndtere eventuelle overføringer som kommunen er ansvarlig for. Revisjonslaget bemerker for øvrig at det ikke bare er i databehandlerrelasjoner at det kan forekomme at personopplysninger overføres til tredjestater.

Moss kommune har i noen grad sikret at mål og overordnede rammer for behandling av personopplysninger beskrives

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller kravet om å beskrive mål og overordnede rammer for behandling av personopplysninger i kommunen, jf. Kommuneloven § 25-1 og Datatilsynets veileder – Informasjonssikkerhet og internkontroll.

Det er avdekket forbedringspotensial knyttet til beskrivelse av mål og overordnede rammer for behandling av personopplysninger. Revisjonslaget bemerker at Moss kommune ikke har oversendt ferdigstilt dokumentasjon som beskriver mål og overordnede rammer for behandling av personopplysninger. Revisjonslaget vurderer at utkastene som er oversendt i noen grad beskriver disse, men vil bemerke at

dokumentasjonen i stor grad fokuserer på informasjonssikkerhet. Moss kommune bør sikre at dokumentasjonen ferdigstilles og implementeres og vurdere hvorvidt mål for personvern kan få en mer fremtredende plass i kommunens styrende dokumenter.

Moss kommune har i liten grad sikret at nødvendige rutiner og retningslinjer for behandling av personopplysninger utarbeides basert på en risikovurdering	

Revisjonslaget vurderer at Moss kommune i liten grad oppfyller kravet knyttet til å utarbeide rutiner og retningslinjer for behandling av personopplysninger basert på en risikovurdering, jf. Kommuneloven § 25-1 og Datatilsynets veileder – Informasjonssikkerhet og internkontroll.

Moss kommune har utarbeidet flere rutiner og retningslinjer for behandling av personopplysninger, men det er avdekket vesentlig forbedringspotensial knyttet til at disse ikke er basert på en risikovurdering. Revisjonslaget bemerker at den oversendte dokumentasjonen kan ha vært utarbeidet på bakgrunn av risikovurderinger, men at det ikke er oversendt dokumentasjon som kan bekrefte dette. Kommunen kan derfor ikke dokumentere at de fastsatte rutinene og retningslinjene er utarbeidet på bakgrunn av risikoene som kommunen står overfor. Kommunen kan dermed heller ikke dokumentere at rutinene/retningslinjene således er tilstrekkelige for å redusere disse risikoene slik som påkrevd i kommuneloven § 25-1 annet ledd, og slik som fastsatt i Datatilsynets veileder for å etablere internkontroll punkt 2.

Moss kommune har i noen grad basert sitt styringssystem for personvern på anerkjente standarder	

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller revisjonskriteriet knyttet til at kommunen bør basere sitt styringssystem for personvern på anerkjente standarder.

Kommunen har opplyst at de følger anerkjente standarder for sitt styringssystem på informasjonssikkerhet og at de følger Datatilsynet sine anbefalinger. Dette vises til en viss grad gjennom dokumentasjonen som revisjonslaget har fått fremlagt.

Det er avdekket forbedringspotensial knyttet til oppbyggingen av styringssystemet da det er noe utfordrende å få oversikt over dokumentene i styringssystemet som er knyttet til personvern. Det er også utfordrende å se sammenhengen mellom dokumentene og den hierarkiske oppbyggingen av dem. *«MK Retningslinje informasjonssikkerhet og personvern»* inneholder blant annet en blanding av styrende og kontrollerende elementer. Overordnede strategiske mål og føringer for personvern burde vært fastsatt i en overordnet policy for personvern. Videre er *«MK Retningslinje informasjonssikkerhet og personvern»* fortsatt i utkastform og ikke formelt godkjent i kommunen.

Videre er det avdekket forbedringspotensial knyttet til at kommunens gjennomførende tiltak ikke er basert på en dokumentert risikovurdering. Revisjonslaget bemerker at den tiltakene kan ha vært utarbeidet på bakgrunn av risikovurderinger, men at det ikke er oversendt dokumentasjon som kan bekrefte dette. Kommunen bør sørge for å dokumentere hva som ligger til grunn for valg av de tiltakene som er iverksatt.

4.5 Konklusjon og anbefalinger

Moss kommune har i noen grad etablert et tilfredsstillende styringssystem for personvern.

Kommunen har etablert flere av elementene som et styringssystem typisk består av, men det bærer preg av at kommunen ikke er i mål ennå. Flere av dokumentene er ikke ferdigstilt og flere av tiltakene som er beskrevet er ikke gjennomført i praksis. Dette gjelder særlig kontrolltiltak. Kommunen har heller ikke utarbeidet en fullstendig protokoll over behandlingsaktiviteter som tilfredsstiller kravene i GDPR artikkel 30 eller gjennomført dokumenterte risikovurderinger av behandlingsaktivitetene. Dette medfører at kommunen ikke kan påvise at tiltakene som er planlagt og/eller iverksatt, er basert på behandlingenes art, omfang, formål og sammenhengen de utføres i, samt risikoene som kommunen står overfor, jf. GDPR artikkel 24. Det er også en gjennomgående utfordring at kommunens rutiner og retningslinjer beskriver hvilke oppgaver som skal gjøres, men ikke hvordan ansatte og ledere skal gå frem for å utføre disse oppgavene. Dette er særlig utfordrende når ansvaret i Moss kommune er delegert til linjeledere og det er gitt tilbakemeldinger om at linjelederne mangler kompetanse til å utøve dette ansvaret. I tillegg er det gitt tilbakemelding om at kommunen ikke sikrer god nok opplæring for linjeledere innen personvern.

Revisjonslaget vil avslutningsvis bemerke at Moss kommune gir inntrykk av å være en kommune som er forholdsvis modne på personvernområdet. Kommunen har iverksatt flere gode tiltak og de har en god plan for hvordan de skal arbeide med å etterleve kravene i personvernlovgivningen fremover. Dersom kommunen lykkes med å gjennomføre de planlagte aktivitetene, vil kommunen ha sikret et godt styringssystem på personvern etter revisjonslagets vurdering.

Basert på våre vurderinger og konklusjon anbefaler vi at kommunen bør:

- Prioritere arbeidet med å utarbeide en fullstendig protokoll over behandlingsaktiviteter.
- Gjennomføre og dokumentere risikovurderinger basert på behandlingsaktivitetene.
- Ferdigstille og utarbeide nødvendig dokumentasjonen i styringssystemet. Revisjonslaget vil særlig anbefale kommunen å ferdigstille styrende dokumentasjon for personvern, utarbeide tydelige rutiner for å håndtere anmodninger om håndheving av de registrertes rettigheter og utarbeide en rutine for hvilke krav ledere må ta hensyn til ved oppstart eller endring av behandlingsaktiviteter.
- Gjennomføre kontrolltiltak, herunder ledelsens gjennomgang og internrevisjon.
- Tydeliggjøre ansvarsfordelingen på personvern og hva dette ansvaret innebærer.
- Gjennomføre målrettet og regelmessig opplæring av linjeledere.

5 PROBLEMSTILLING 2: HAR KOMMUNEN SIKRET AT DE ANSATTE ETTERLEVER RUTINENE PÅ PERSONVERNOMRÅDET?

5.1 Utledning av revisjonskriterier

I henhold til GDPR artikkel 24 skal den behandlingsansvarlige etablere en internkontroll som sikrer at alle plikter etter GDPR etterleves av de ansatte i kommunen. Dette innebærer blant annet at den behandlingsansvarlige må sørge for å kontrollere at rutiner og tiltak etterleves blant de ansatte. Eksempler på kontrolltiltak er sikkerhetsrevisjoner, egenkontroller og ledelsens gjennomgang.[5]

Videre skriver Datatilsynet i sin veileder at den behandlingsansvarlige må sørge for at internkontrollen gjøres kjent og etterleves blant de ansatte i virksomheten.[6] Revisjonslaget mener derfor at kommunen må sikre at styringssystemet integreres i kommunens prosesser og kommuniseres til kommunens ansatte.

Det følger av Datatilsynets veileder for å etablere internkontroll at den behandlingsansvarlige må sørge for opplæring av sine ansatte for å sikre at de er i stand til å etterleve virksomhetens rutiner og retningslinjer.

Både GDPR artikkel 33-34 og Datatilsynets veileder for å etablere internkontroll fastsetter at virksomheter skal sørge for at avvik blir håndtert. For å sikre at avvik blir håndtert mener revisjonslaget at kommunen derfor må implementere et system for å melde avvik og sørge for at dette er kjent blant kommunens ansatte.

5.2 Revisjonskriterier

Basert på utledningen ovenfor har revisjonslaget utarbeidet følgende revisjonskriterier:

Moss kommune skal:

- gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar personvernforordningen (GDPR artikkel 24).
- sikre at styringssystemet for personvern integreres i kommunens prosesser og kommuniseres til kommunens ansatte.
- sørge for opplæring av ansatte for å sikre at de er i stand til å etterleve rutiner og retningslinjer (Datatilsynets veileder – Informasjonssikkerhet og internkontroll).
- Implementere et system for å melde avvik.

5.3 Datagrunnlag

5.3.1 Behandlingsansvarliges ansvar

Som beskrevet under problemstilling 1 er det operative ansvaret for personvern i Moss kommune i stor grad delegert nedover i linjen. For å sørge for at dette ansvaret utøves og at ansatte etterlever rutinene på området har kommunen etablert kvalitetsutvalg i alle kommunalområdene. Det er opplyst om at utvalgene skal sørge for bevisstgjøring av krav og rutiner knyttet til personvern nedover i organisasjonen

[5] Datatilsynet veileder "Etablere internkontroll" punkt 4 og 5
[6] Datatilsynet veileder "Etablere internkontroll" punkt 4

og at utvalgene skal gjennomføre kontrollaktiviteter av sine enheter. I intervju er det opplyst om at enkelte kvalitetsutvalg er godt etablert, mens andre ikke er etablert ennå.

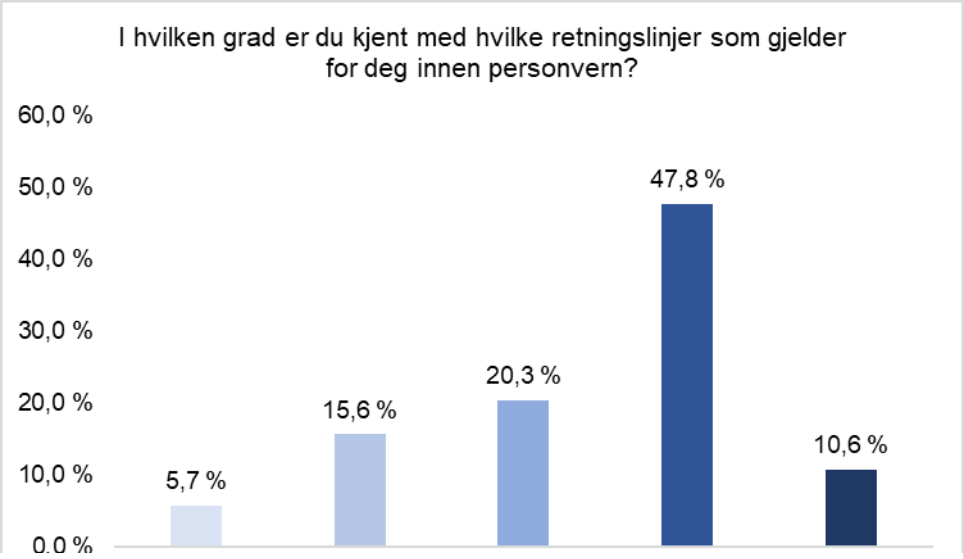
I tillegg til kvalitetsutvalgene har Moss kommune etablert et sikkerhet- og personvernutvalg som ledes av personvernombudet og hvor alle kommunalområdene er representert. Dette utvalget skal også bidra til å bevisstgjøre og sørge for at problemstillinger knyttet til personvern blir kommunisert både oppover og nedover i organisasjonen.

Det er opplyst at kommunen har planlagt å gjennomføre flere systematiske kontrolltiltak for å undersøke om ansatte etterlever rutinene knyttet til personvern, herunder ledelsens gjennomgang, internrevisjoner og egenkontroller. Det er opplyst at enkelte kvalitetsutvalg har gjennomført egenkontroller, men at det ikke er gjennomført noen systematiske kontrolltiltak fra kommunen sentralt. De kontrolltiltakene som har blitt gjennomført, har blitt gjennomført ad hoc.

5.3.2 Integrering av styringssystemet i kommunens prosesser og kommunikasjon til kommunens ansatte

Moss kommune tilgjengeliggjør og kommuniserer styringssystemer for personvern på kommunens kvalitetssystem kalt «Risk Manager». Flertallet av intervjuobjektene har sagt at de er kjent med kommunens kvalitetssystem og at de opplever det som enkelt å finne rutiner og retningslinjer knyttet til personvern. Enkelte mener imidlertid at det kan være vanskeligere for ansatte som ikke nødvendigvis sitter ved en PC, eksempelvis sykepleier og lærere. Det er også gitt tilbakemeldinger om at kommunen har nok av rutiner og retningslinjer, men at det er mangler knyttet til kommuniseringen av dem. Det er opplyst at linjeledere er ansvarlig for å kommunisere ansvar og rutiner og retningslinjer nedover i organisasjonen. Det er imidlertid gitt tilbakemeldinger om at linjeledere har for lite kompetanse innen personvern til å forstå hva sitt ansvar innebærer og at det ikke gjennomføres systematisk og regelmessig opplæring av disse.

Gjennom spørreundersøkelsen fremgår det at et flertall (59,3%) er kjent med hvor de finner Moss kommune sine retningslinjer og rutiner for personvern. Det er likevel 40,7% som svarer «nei» på spørsmål om de er kjent med rutiner og retningslinjer knyttet til personvern. På spørsmål om i hvilken grad de er kjent med rutiner som gjelder for dem svarer et flertall at de i stor grad (47,8%) eller i svært stor grad (10,6%) er kjent med dette. Det er 20,3% som svarer verken eller.



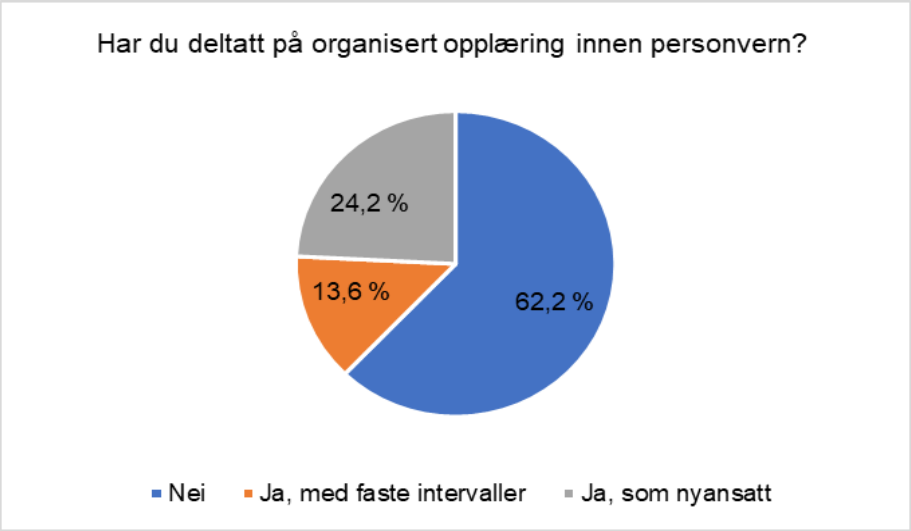
Figur 1 Svar fra spørreundersøkelsen "I hvilken grad er du kjent med hvilke retningslinjer som gjelder for deg innen personvern?"

Revisjonslaget er informert om at Moss kommune har hatt fokus på å kommunisere styringssystemet ut til organisasjonen. Da Covid-19 brøt ut og ansatte ble sendt på hjemmekontor ble eksempelvis *«MK Hjemmekontor og personvern»* utarbeidet og kommunisert til de ansatte. Intervjuobjektene har gitt tilbakemeldinger på at kommunen har lykkes med å få ansatte til å bli klar over sitt ansvar knyttet til inngåelse av databehandleravtaler. Det er også etablert kvalitetsutvalg i hvert kommunalområde som skal sørge for å kommunisere styringssystemet til ansatte i linjen. Det er opplyst at kommunalområdet for kultur, oppvekst og aktivitet ikke har etablert kvalitetsutvalg.

5.3.3 Opplæring

Det er opplyst i intervju at Moss kommune ikke har utarbeidet en overordnet opplæringsplan for ansatte innen personvern. Revisjonslaget er informert om at det ble gjennomført opplæring av ledere da GDPR ble innført og at personvern har vært et tema på ledersamlinger. Videre fremkom det av intervjuene at Moss kommune ikke har gjennomført regelmessig eller tilpasset opplæring av ansatte. Etter kommunens gjennomgang av datagrunnlaget ble revisjonslaget informert om at det frem til desember 2020 ble gjennomført opplæring av ansatte på personvern. Revisjonslaget er informert om at kommunen ved enhet HR arbeider med å utarbeide en opplæringsplan for nyansatte hvor personvern inkluderes.

I intervju har revisjonslaget fått tilbakemeldinger på at det er god kompetanse på personvern sentralt i kommunen, men at det er mindre kompetanse hos linjeledere. Det fremkom i intervju at det i varierende grad gis opplæring i personvern til de ansatte på de ulike kommunalområdene, og at ansvaret for opplæring av de ansatte i stor grad er lagt til linjeledere.



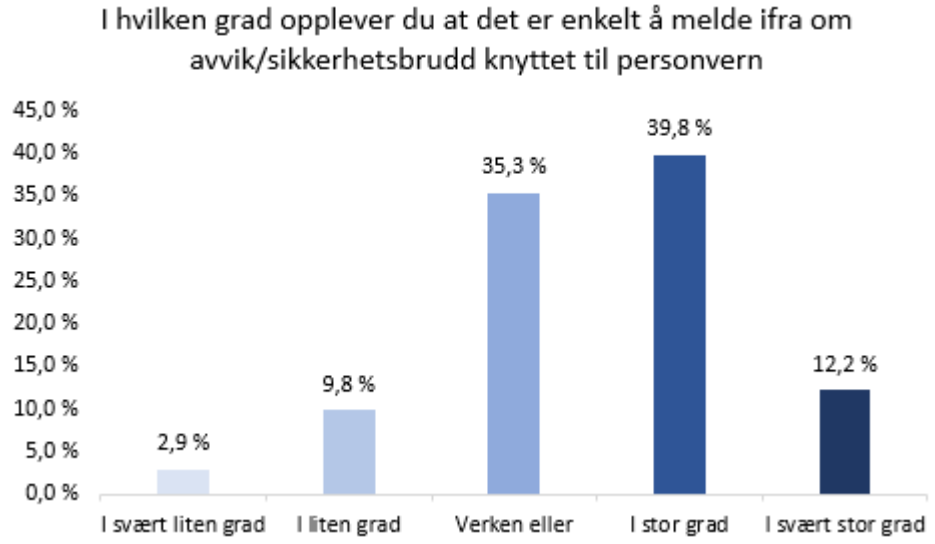
Figur 2 Svar fra spørreundersøkelsen "Har du deltatt på organisert opplæring innen personvern?".

At kommunen ikke gjennomfører organisert og regelmessig opplæring av ansatte bekreftes gjennom spørreundersøkelsen som revisjonslaget har gjennomført hvor 62,2% har svart at de ikke har mottatt organisert opplæring innen personvern. Det er kun 13,6% som svarer at de har fått organisert opplæringen med faste intervaller, mens 24,5% har svart at de har fått opplæring som nyansatt.

5.3.4 Avvikssystem

Moss kommune har implementert et avvikssystem og rutiner for avviksbehandling. Dette er nærmere beskrevet under problemstilling 1, punkt 4.3.21. Intervjuobjektene ga uttrykk for at avvikssystemet anses å være godt kjent og kommunisert nedover i linjen. Det er likevel noen av intervjuobjektene som opplyser at enkelte kommunalområder ikke har så mange avvik som det burde vært. Det er også gitt tilbakemelding om at enkelte sliter med å få linjen til å forstå at avvik skal meldes i avvikssystemet slik at de dokumenteres, og ikke bare til nærmeste leder.

I spørreundersøkelsen svarer et flertall (62,3%) at de er kjent med hvordan de melder avvik, mens et mindretall (37,7%) har svart at de ikke er kjent med dette. I tillegg har et flertall svart at de i stor grad (39,8%) eller svært stor grad (12,2%) opplever det som enkelt å melde fra om avvik. Et mindretall har svart at de verken eller (35,3%), i liten grad (9,8%) eller svært liten grad (2,9%) opplever dette som enkelt (se figur 3).



Figur 3, Svar fra spørreundersøkelsen "I hvilken grad opplever du at det er enkelt å melde ifra om avvik/sikkerhetsbrudd knyttet til personvern".

5.4 Vurderinger

Moss har i noen grad gjennomført tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen	

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller revisjonskriteriet om å gjennomføre tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen, jf. GDPR artikkel 24.

Det er avdekket forbedringspotensial knyttet til Moss kommunes gjennomføring av kontrollaktiviteter både sentralt og i linjen for å sørge for at ansatte etterlever rutinene knyttet til personvern. Det er ikke gjennomført systematiske kontrollaktiviteter fra kommunen sentralt, og ikke alle kvalitetsutvalg er etablert. Revisjonslaget ser imidlertid positivt på at enkelte kvalitetsutvalg er etablert og at kommunen planlegger å gjennomføre en rekke kontrollaktiviteter både sentralt og i linjen.

Moss kommune har i noen grad sikret at styringssystemet for personvern integreres i kommunens prosesser og kommuniseres til kommunens ansatte

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller revisjonskriteriet knyttet til å sikre at personvern integreres i kommunens prosesser og at dette kommuniseres til de ansatte.

Revisjonslaget sitter med et inntrykk av at kommunens ledelse har et høyt fokus på personvern og en vilje til å etterleve regelverket. Det er utarbeidet flere rutiner og retningslinjer for personvern og disse gjøres tilgjengelig for ansatte nedover i organisasjonen gjennom kvalitetssystemet. Det er imidlertid avdekket forbedringspotensial knyttet til kommunens kommunisering av rutinene og retningslinjene da hele 40,7% har svart at de ikke er kjent med hvor de finner rutiner og retningslinjer for personvern. Revisjonslaget mener dette kan forbedres ved å sørge for systematisk og regelmessig opplæring av ledere og ansatte (se punkt om dette nedenfor) og ved å sikre at kvalitetsutvalgene etableres og gjennomfører sine oppgaver.

Moss kommune har i liten grad etablert tiltak for å sørge for opplæring av de ansatte for å sikre at de er i stand til å etterleve rutiner og retningslinjer

Revisjonslaget vurderer at Moss kommune i liten grad oppfyller revisjonskriteriet knyttet til å sørge for opplæring av de ansatte slik at de er i stand til å etterleve rutiner og retningslinjer, jf. Datatilsynets veileder – Informasjonssikkerhet og internkontroll.

Det er avdekket vesentlig forbedringspotensial tilknyttet opplæring av ansatte for å sikre at de er i stand til å etterleve rutiner og retningslinjer, da flertallet av ansatte (62,2%) har svart at de ikke har mottatt organisert opplæring innen personvern. Dette er også revisjonslagets inntrykk etter de gjennomførte intervjuene. Revisjonslaget ser positivt på at det er gjennomført noe opplæring for linjeledere, men også her har revisjonslaget fått tilbakemeldinger på det ikke er gjennomført systematisk og regelmessig opplæring.

Revisjonslaget vil bemerke at det er positivt at Moss kommune arbeider med å utarbeide en opplæringsplan for ansatte hvor personvern inkluderes, men kommunen må også sikre at det gjennomføres målrettet opplæring av både linjeledere og ansatte regelmessig.

Moss kommune har i stor grad etablert et avvikssystem

Revisjonslaget vurderer at Moss kommune i stor grad oppfyller revisjonskriteriet knyttet til å implementere et system for å melde avvik.

Det er imidlertid avdekket mindre forbedringspotensial knyttet til kommuniseringen av hvordan de ansatte skal melde avvik da det er et ganske stort antall ansatte (37,7%) som svarer at de ikke er kjent med hvordan de melder avvik. Revisjonslaget mener dette kan forbedres ved å sørge for systematisk og regelmessig opplæring av ledere og ansatte (se punkt om dette nedenfor) og ved å sikre at kvalitetsutvalgene etableres og gjennomfører sine oppgaver.

5.5 Konklusjon og anbefalinger

Moss kommune har i noen grad sikret at de ansatte etterlever rutinene til kommunen på personvernområdet.

Revisjonslaget ønsker å fremheve at Moss kommune har et høyt fokus på personvern, både på ledelsesnivå og nedover i organisasjonen. Revisjonslaget har imidlertid avdekket at Moss kommune ikke har lykkes helt med å sørge for at ansatte er kjent med rutiner og retningslinjer for personvern eller med opplæring av både ledere og ansatte. Kommunen er heller ikke helt i mål med kontrollere at rutinene og retningslinjene faktisk etterleves i praksis. Revisjonslaget vil likevel bemerke at Moss kommune selv er klar over disse avvikene og at de arbeider med å utbedre dem.

Basert på våre vurderinger og konklusjon anbefaler vi at kommunen bør:

- Fortsette arbeidet med å utarbeide et opplæringsprogram for nyansatte som inkluderer personvern.
- Gjennomføre målrettet og regelmessig opplæring av både ledere og ansatte.
- Sikre at alle kommunalområdene etablerer kvalitetsutvalg.
- Gjennomføre kontrolltiltak, herunder ledelsens gjennomgang og internrevisjon.

6 PROBLEMSTILLING 3: HAR KOMMUNEN ETABLERT ET TILFREDSSTILLENDE STYRINGSSYSTEM (INTERNKONTROLL) FOR INFORMASJONSSIKKERHET?

6.1 Utleding av revisjonskriterier

I henhold til forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) § 15 andre ledd skal forvaltningsorganet ha en internkontroll på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Revisjonslaget er informert om at Moss kommune baserer sitt styringssystem på ISO/IEC 27001 - Ledelsessystemer for informasjonssikkerhet. Det fremgår av dokumentet «*MK Retningslinje informasjonssikkerhet og personvern*» at retningslinjene er basert på ISO, herunder ISO/IEC 27001.

ISO/IEC 27001 stiller krav til at virksomheten skal ha fastsatte roller og tydelig en ansvarsfordeling knyttet til informasjonssikkerhet.

Forskrift om kommunal beredskapsplikt § 2 pålegger kommuner å gjennomføre helhetlige risiko- og sårbarhetsanalyser. ISO/IEC 27001 stiller krav til at organisasjonen skal definere og benytte en prosess for informasjonssikkerhetsrisiko som inkluderer kriterier for risikoaksept, vurdering av konsekvenser ved tap av konfidensialitet, integritet og tilgjengelighet (KIT), sannsynlighet for forekomst av risikoene og prioritering knyttet til håndtering av risikoene. Organisasjoner skal i henhold til ISO/IEC 27001 utføre risikovurderinger av informasjonssikkerheten med planlagte intervaller eller når betydelige endringer er foreslått eller inntreffer. Resultatene fra risikovurderingene av informasjonssikkerheten skal dokumenteres.

Både ISO/IEC 27001 og Datatilsynets veileder for informasjonssikkerhet og internkontroll stiller krav til at virksomheter skal ha fastsatte rutiner for avviksbehandling. For å evaluere ledelsessystemet for informasjonssikkerhet skal det i henholdt til ISO/IEC 27001 og Datatilsynets veileder for informasjonssikkerhet gjennomføres revisjoner knyttet til informasjonssikkerhet.

I henhold til forskrift om kommunal beredskapsplikt § 4 skal kommunen utarbeide en overordnet beredskapsplan som skal inkludere:

- Oversikt over kriseledelsen, ansvar og fullmakter.
- Varslingsliste over aktører med en rolle i krisehåndteringen.
- Ressursoversikt med opplysninger om ressurser kommen har til rådighet og som er tilgjengelig hos andre aktører ved uønskede hendelser.
- Evakueringsplan og plan for befolkningsvarsling.
- Plan for krisekommunikasjon.

Kommunen skal i henhold til forskrift om kommunal beredskapsplikt § 7 gjennomføre beredskapsøvelser hvert andre år. Scenarioene for øvelsen bør ta utgangspunkt i funn fra kommunens helhetlige risiko- og sårbarhetsanalyse (ROS).

6.2 Revisjonskriterier

Basert på utledningen ovenfor har revisjonslaget utarbeidet følgende revisjonskriterier:

Moss kommune skal:

- ha en internkontroll på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet (eforvalningsforskriften § 15).
- ha fastsatt mål og strategi for informasjonssikkerhet i virksomheten (eForvaltningsforskriften § 15).
- etablere en sikkerhetsstrategi som omfatter de grunnleggende beslutningene om organiseringen og gjennomføringen av sikkerhetsarbeidet (eForvaltningsforskriften §15).
- ha fastsatte roller og ansvarsområder (eForvaltningsforskriften §15 og ISO/IEC 27001.).
- gjennomføre risikovurderinger (Forskrift om kommunal beredskapsplikt, p.2; ISO-IEC 27001)
- ha fastsatte rutiner for avviksbehandling (Datatilsynets – Informasjonssikkerhet og internkontroll).
- gjennomføre sikkerhetsrevisjon eller andre kontrollaktiviteter (Datatilsynets – Informasjonssikkerhet og internkontroll).
- ha en beredskapsplan (Jf. Forskrift om kommunal beredskapsplikt § 4).
- gjennomføre beredskapsøvelser minimum annethvert år (Jf. Forskrift om kommunal beredskapsplikt § 7).

6.3 Datagrunnlag

6.3.1 Styringssystem for informasjonssikkerhet basert på anerkjent standard

Det fremgår av utkast-versjonen til dokumentet *«Retningslinjer informasjonssikkerhet og personvern»* at Moss kommune baserer sine retningslinjer for informasjonssikkerhet på ISO/IEC 27001 – Ledelsessystemer for informasjonssikkerhet. Det fremgår også av dokumentet at kommunens retningslinjer for informasjonssikkerhet er forankret i ISO/IEC-27002:2017, ISO/IEC-27004:2017, ISO/IEC-27005:2018. Det fremgår av dokumentet *«Ansatte med kompetanse på ISO-IEC 27001»* at en enkeltperson har kompetanse i ISO/IEC 27001. Moss kommune har ikke fremlagt dokumentasjon eller vurderinger tilknyttet hvilke kontroller basert på anerkjente standarder som bør implementeres eller bakgrunnen for valg av sikringstiltak. Ved faktasjekk bemerkes det fra Moss kommune at dette ikke er lovkrav, men kun anbefalinger.

I dokumentet *«Retningslinjer informasjonssikkerhet og personvern»* fremgår det at retningslinjene inkluderer både styrende og kontrollerende tiltak samt at det refereres til utførende dokumenter. Retningslinjene er gjeldene for alle medarbeidere i kommunene, i foretakene, folkevalgte og for leverandører og tilsynsmyndigheter som skal ha tilgang til Moss kommunes systemer. Det fremkom av dokumentet *«Retningslinjer informasjonssikkerhet og personvern»* at denne ikke var vedtatt og implementert på tidspunktet for revisjonen.

6.3.2 Mål og sikkerhetsstrategi for informasjonssikkerhetsarbeidet

Det er fastsatt sikkerhetsmål for arbeidet med informasjonssikkerhet i dokumentet *«Retningslinjer informasjonssikkerhet og personvern».* Mottatt versjon er i utkast-versjon med arbeidskommentarer og har ikke en godkjennelsesdato. Det fremgår i dokumentet *«IT-Strategi for Moss kommune 2021-2025»* at «*IT-enheten skal ivareta oppgaver knyttet til informasjonssikkerhet, herunder tekniske tiltak, fysiske tiltak og organisatoriske tiltak for å øke informasjonssikkerhetskompetansen og evnen i organisasjonen*».

Strategi knyttet til sikkerhet fremgår av dokumentet *«IT-strategi for Moss kommune 2021-2025».* Målet er at IT-enheten skal bidra til å sørge for at kommunen kan opprettholde et hensiktsmessig sikkerhetsnivå. De definerte aktivitetene for å oppnå dette er:

- Utarbeidelse av dokumentasjon.
- Gjennomføring av opplæring.
- Gjennomføring av risikovurderinger.
- Kompetanseheving i prosjekter.
- Kontinuerlig arbeid med forbedring.

Revisjonslaget er informert om at IT-enheten i Moss kommune har basert arbeidet med informasjonssikkerhet på en risikobasert tilnærming, hvor kostnad ved et tiltak skal veies opp mot tiltakets effekt. I tillegg er følgende hovedprinsipper lagt til grunn for IT-sikkerhet i kommunen:

- Tilgjengelighet: IT-systemene, informasjonen som behandles i systemene og tjenestene tilknyttet systemene er tilgjengelig når det trengs for brukerne.
- Integritet: IT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene endres ikke utilsiktet eller uautorisert.
- Konfidensialitet: IT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene er kun tilgjengelig for dem som rettmessig skal ha tilgang.

Det er også fastsatt som en del av IT-strategien at Moss kommune skal benytte skyteknologi. Ved faktasjekk opplyste Moss kommune at strategien ikke er knyttet til tilgjengelighet, men til eksempelvis økonomi, skalerbarhet, tilgang til moderne løsninger og ressursinnsats.

6.3.3 Roller og ansvarsområdet

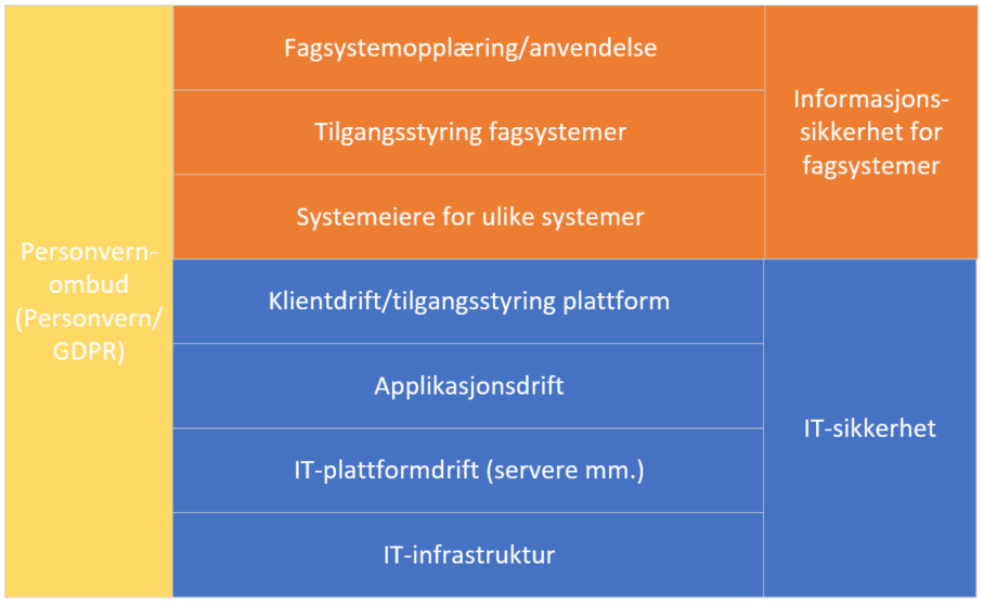
Det fremgår av dokumentet *«Retningslinjer informasjonssikkerhet og personvern»* at det er fastsatt et sikkerhet- og personvernutvalg. Revisjonslaget fikk dette bekreftet i intervju. Sikkerhet- og personvernutvalget møtes en gang i måneden. Tema for møtene i utvalget er varierende, enkelte av temaene har vært:

- Prosesser for innføring av nye systemer.
- Ansvar og rollefordeling.
- Gjennomgang av avvik og tiltak.

Det fremgår av dokumentet *«Organisering av sikkerhetsarbeidet»* at ansvarsfordelingen knyttet til sikkerhet er fordelt i to dimensjoner:

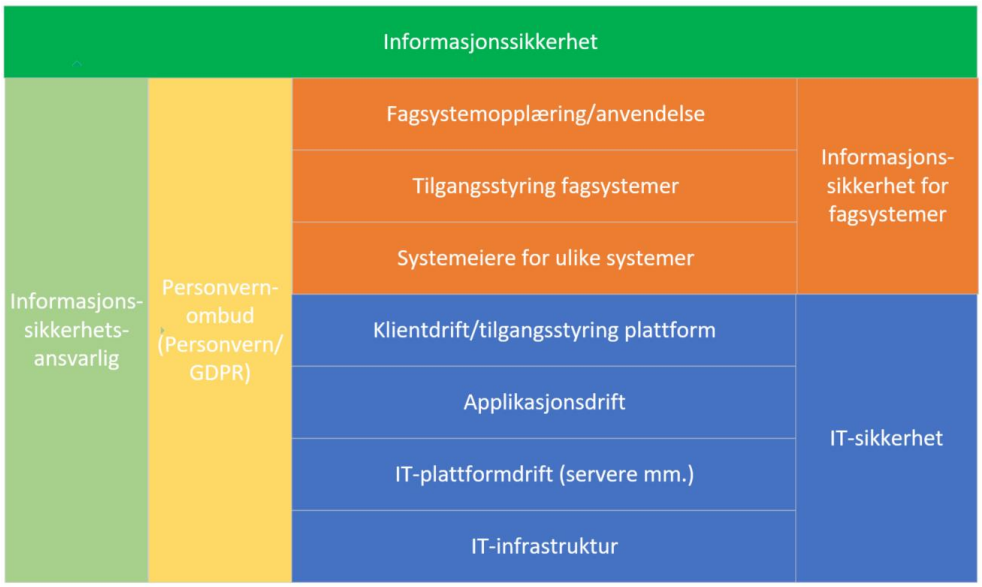
- Organisatorisk.
- Teknisk.

I dokumentet *«Organisering av sikkerhetsarbeidet»* er det illustrert slik:



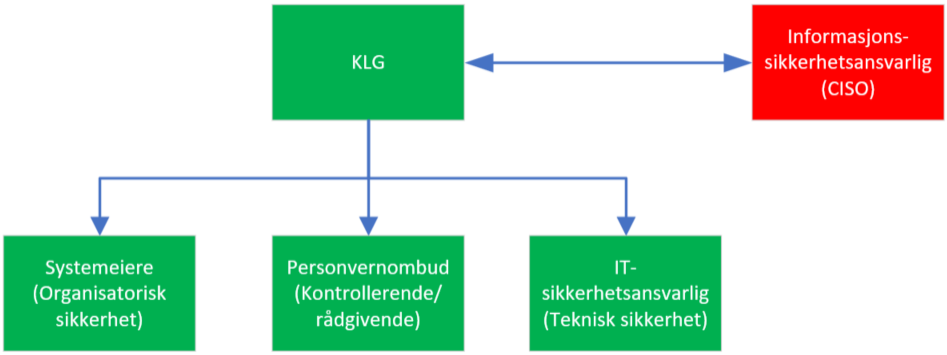
Figur 4, Illustrasjon av ansvarsfordeling knyttet til sikkerhetsarbeidet utarbeidet av Moss kommune

Revisjonslaget er orientert om at Moss kommune i dag på «teknisk» side har en IT-sikkerhetsansvarlig, i tillegg til IT-sjef som har det overordnede ansvaret. Når det gjelder «organisatorisk» side er det fagansvarlige og systemeiere som har et ekstra ansvar knyttet til informasjonssikkerhet. Revisjonslaget er informert om at det er igangsatt et arbeid med å ansette en informasjonssikkerhetsansvarlig (CISO), som da skal koordinere ansvaret for informasjonssikkerhet på tvers. Det er planlagt å etablere ny organisering som ut fra dokumentet *«Organisering av sikkerhetsarbeidet»* er illustrert ved figur 3.



Figur 5, Illustrasjon av ønsket ansvarsfordeling knyttet til sikkerhetsarbeidet utarbeidet av Moss kommune

Det er tiltenkt at informasjonssikkerhetsansvarlig vil være organisert sentralt, og ha direkte forbindelse med kommunens ledelse, jf. figur 6 nedenfor:



Figur 6, Illustrasjon av ønsket organisering av sikkerhetsarbeidet utarbeidet av Moss kommune.

Det fremgår av dokumentene «MK *Retningslinje informasjonssikkerhet og personvern*» og *«IT-strategi for Moss kommune 2021-2025»* at det er forskjellige beskrivelser av hvem som er ansvarlig for kompetanseutvikling innen informasjonssikkerhet.

Det fremgår av dokumentet *«MK Retningslinje informasjonssikkerhet og personvern»* at personvernombudet skal forberede inngangsfaktorene til ledelsens gjennomgang og at dette skal gjennomføres årlig. I dokumentet «*MK Ledelsens gjennomgang informasjonssikkerhet*» fremgår det at det er ledelsen ved virksomheten som har ansvar for å gjennomføre ledelsens gjennomgang og at dette skal gjennomføres tre ganger i året. Videre fremgår det at dokumentet gjelder for rådmannen og rådmannens ledergruppe. Det er fastsatt at personvern sammen med sikkerhetsansvarlig og sikkerhetsutvalget har ansvar for å tilrettelegge gjennomgangen.

6.3.4 Risiko- og sårbarhetsanalyse

Moss kommune har gjennomført en helhetlig risiko- og sårbarhetsanalyse (ROS) i 2019 (kommune-ROS). ROS-analysen tok ikke for seg informasjonssikkerhetshendelser. Det fremgår av dokumentet «*ROS og analyser*» at det er påstartet en prosess for å etablere prosess for ROS av informasjonssikkerhet og eget IKT-driftsmiljø.

Moss kommune har ikke fremlagt en helhetlig risikovurdering knyttet til informasjonssikkerhet. Revisjonslaget er forelagt *«ROS IT-sikkerhet»*, som utgjør mal for risikovurderinger knyttet til informasjonssikkerhet. Det fremgår av dokumentet «*Risikovurderinger*» at det er gjennomført risikovurderinger på fagsystemnivå. Moss kommune har ikke fremlagt dokumentasjon knyttet til den enkelte risikovurdering.

I intervju var det ulike oppfatninger knyttet til gjennomføring av og kompetanse innen risikovurderinger. Det ble trukket frem at det mangler en strukturert og systematisert måte å gjennomføre risikovurderinger på og at det per i dag i større grad gjennomføres ad-hoc. Det er tiltenkt at den nye CISO-rollen skal ta tak i dette. Det fremgår også av *«stillingsbeskrivelse informasjonssikkerhetsansvarlig»* at rollen vil innebære å *«[…] følge opp risiko- og trusselbildet og forvalte metodikk for risikostyring relatert til informasjonssikkerhet*». Flere av intervjuobjektene formidlet at IT besitter kompetanse knyttet til informasjonssikkerhet og gjennomføring av risikovurderinger. I dokumentet *«MK Retningslinje informasjonssikkerhet og personvern»* fremgår det at Moss kommune skal «gjennomfører risikovurderinger og internrevisjon innen informasjonssikkerhet». Dokumentet *«MK Retningslinje informasjonssikkerhet og personvern»* er ikke godkjent og implementert på tidspunktet for revisjonen.

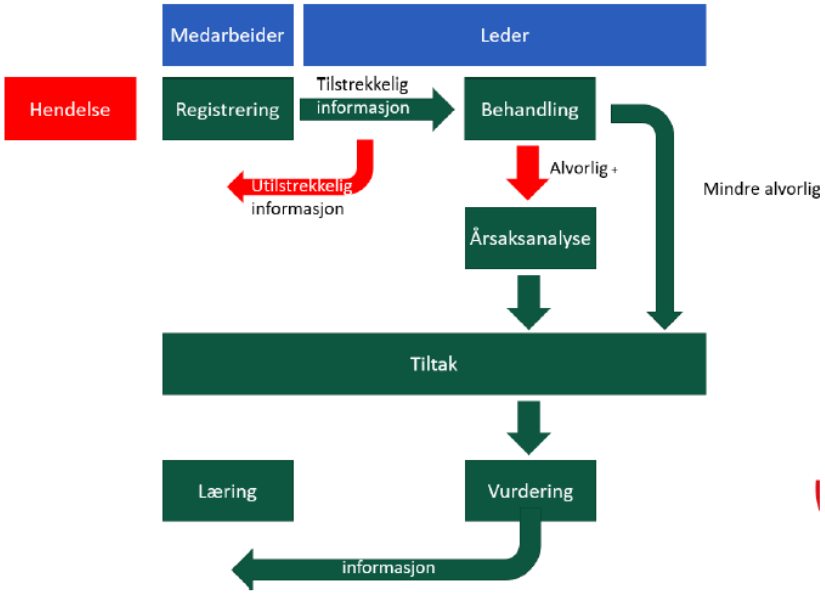
6.3.5 Rutiner for avviksbehandling

Det ble informert i intervju at Moss kommune benytter ett enhetlig system for innmelding av avvik, både knyttet til personvern og informasjonssikkerhet. Revisjonslaget fikk innføring i Moss kommunes helhetlige avvikssystem, som også er beskrevet i dokumentet *«Hvordan håndtere avvik og uønskede hendelser- trinn for trinn».* Samlingen av retningslinjer knyttet til avviksbehandling (6.2.5) er tilgjengelig på kommunens kvalitetssystem «Risk Manager». Det fremkom i intervju at alle kommunens ansatte, utenom tilkallingsvikarer i barnehage og midlertidige knyttet til vaksineringen av COVID-19, får kommunal e-post adresse og derav tilgang til kvalitetssystemet. Ved faktasjekk presiserte Moss kommune at de får en M365-lisens som gir tilgang til sharepoint som RISK er bygget på. Avviksrutiner er også kommunisert gjennom dokumentet «*Internkontroll og kvalitet i Moss kommune»*.

Moss kommune har definert hva som anses som avvik og uønskede hendelser i dokumentet *«MK definisjoner for avvik og uønskede hendelser, skader og varslinger»*. Det fremgår av dokumentet *«Retningslinjer for avvikshåndtering og årsaksanalyse»* at Moss kommune har et styringsdokument for avvikshåndtering og årsaksanalyser som ble godkjent 29.09.2021. Dokumentet beskriver prosessen for avvikshåndtering (illustrert i figur 5). Videre har Moss kommune dokumenterte retningslinjer for hele avvikshåndteringsprosessen, herunder følgende dokumenter:

- *«Slettede avvik og skader»*
- *«Oversikt over avviksområder og avvikskategorier»*
- *«Melde avvik i web-applikasjonen for avvik»*
- *«Hvordan melde avvik på sikkerhets – og personvernbrudd»*
- *«Hvordan håndtere avvik og uønskede hendelser»*
- *«Retningslinjer for avvikshåndtering og årsaksanalyser»*.

Prosessen for avviksbehandling er illustrert i figur 7.



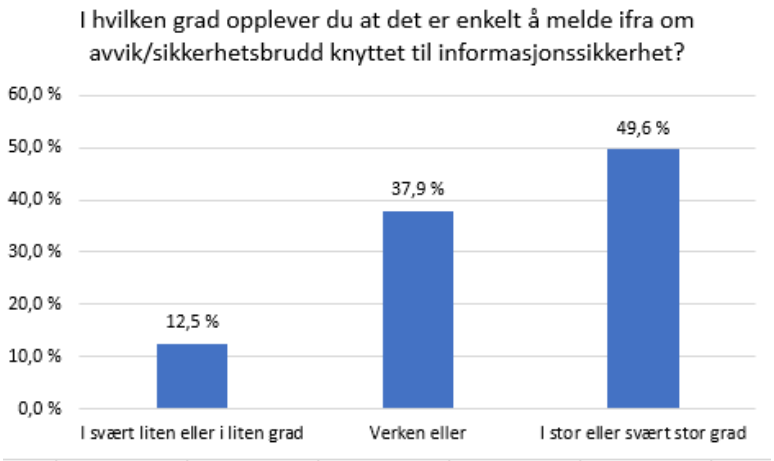
Figur 7. Prosesskart for avviksbehandling.

Det fremgår av *«Internkontroll og kvalitet i Moss kommune»* at rutiner for avvik er en del av kvalitetssystemet.

Figur 8, Svar fra spørreundersøkelsen "Er du kjent med hvordan du rapporterer avvik knyttet til personvern og informasjonssikkerhet?".

I spørreundersøkelsen svarte 62,3% «ja» og 37,7% «nei» på spørsmål om man var kjent med hvordan man rapporterer avvik knyttet til personvern og informasjonssikkerhet (se figur 8). Revisjonslaget er forelagt presentasjonen som har blitt benyttet ifm. opplæring i hvordan å melde avvik på sikkerhets- og personvernbrudd. Det fremkom i intervju at denne presentasjonen ble gitt som en del av et større opplæringsprogram i 2018 for ledere. Det er opplyst i faktasjekk av datagrunnlag at opplæringsprogrammet har vært gjennomført flere ganger, herunder i 2019 og 2020.

På spørsmål om i hvilken grad man opplevde at det er enkelt å melde ifra om avvik/sikkerhetsbrudd knyttet til informasjonssikkerhet var det 12,5 % som svarte enten «i svært liten grad» eller «i liten grad», mens 49,6% svarte enten «i stor grad» eller «i svært stor grad» (se figur 9).



Figur 9, Svar fra spørreundersøkelsen "I hvilken grad opplever du at det er enkelt å melde ifra om avvik/sikkerhetsbrudd knyttet til informasjonssikkerhet".

6.3.6 Gjennomføre sikkerhetsrevisjon eller andre kontrollaktiviteter

Det fremgår av dokumentet *«Internrevisjon Moss kommune 26082021»* at det planlegges å gjennomføre internrevisjon av informasjonssikkerhet i Q3 i 2021.

Dokumentet *«MK Internkontroll og kvalitet i Moss kommune»* og *«MK Retningslinje informasjonssikkerhet og personvern»* fastsetter at det årlig skal gjennomføres ledelsens gjennomgang. I dokumentet «*MK Ledelsens gjennomgang informasjonssikkerhet»* fremgår det at det er ledelsen ved virksomheten som har ansvar for å gjennomføre ledelsens gjennomgang og at dette skal gjennomføres tre ganger i året. Ledelsens gjennomgang omfatter kommunens arbeid med interkontroll generelt, men informasjonssikkerhet er en del av dette. Det er også fremlagt et eget dokument for ledelsens gjennomgang hvor det er beskrevet hva som skal gjennomgås knyttet til informasjonssikkerhet og personvern. Det er opplyst i intervju at ledelsens gjennomgang ikke er gjennomført på tidspunkt for revisjonen. Moss kommune har ikke fremlagt referat fra ledelsens gjennomgang. Ved faktasjekk opplyser Moss kommune at grunnlaget for kommunedirektørens ledergruppe er underlaget for ledelsens gjennomgang.

I dokumentet *«MK Ledelsens gjennomgang informasjonssikkerhet og personvern»* fremgår det at formålet med prosedyren er at rådmannen og rådmannens ledergruppe skal:

- Følge opp de mål som er satt.
- Gjøre korrigerende tiltak.
- Vurdere oppfølging av korrigerende tiltak.
- Endring av mål for prosess.
- Sørge for at internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessige, tilstrekkelige og effektive og at det tilfredsstiller relevante krav i personopplysningsloven og forskriften.

I tillegg til at det skal gjennomføres en ledelsens gjennomgang sentralt, skal også de enkelte kvalitetsutvalgene gjennomføre ledelsens gjennomgang innen sitt kommunalområde. Dette er fastsatt *i «MK Internkontroll og kvalitet i Moss kommune».* Det er opplyst gjennom intervju at enkelte kvalitetsutvalg er godt etablert og at de har gjennomført ledelsens gjennomgang, mens andre kvalitetsutvalg ennå ikke er etablert.

Kommunen har utarbeidet *«MK Sjekkliste for egenkontroll av informasjonssikkerhet og GDPR»* som inneholder en rekke spørsmål om informasjonssikkerhet og personvern som er rettet til virksomhetene/enhetene i linjen, herunder innen kategoriene ansvar og organisering, opplæring, tilganger, avvikshåndtering, risikovurderinger og de registrertes rettigheter. I intervju er det opplyst at dette skjemaet ble sendt ut til alle ledere som er systemeiere for første gang ved utgangen av 2020 fra kommunen sentralt.

Moss kommune har diskutert status på informasjonssikkerhetsområdet i kommunegruppens ledergruppe (KLG), det fremgår av *«KLG 26 august informasjonssikkerhet».* Det fremkom i intervju at status på avvik og hendelser er tema på møter i enkelte lokale kvalitetsutvalg samt det nyetablerte sikkerhets- og personvernsutvalget.

6.3.7 Beredskapsplan og øvelser

Moss kommune har en beredskapsplan som ble godkjent 16.02.2020, dette er dokumentert i *«MK Overordnet beredskapsplan*». Det fremgår av dokumentet *«MK Overordnet beredskapsplan»* hvordan varsling og eskalering av kriseledelse skal foregå, samt hvem som har det overordnede ansvaret for å iverksette varsling av alle faste medlemmer av kriseledelsen og krisestaben. Det er fastsatt varslingsliste i «Vedlegg I – Varslingsliste IKT», hvor kontaktinformasjon er oppført.

Moss kommune har lagt til grunn de fire hovedprinsippene for beredskap:

- Ansvarsprinsippet.
- Likhetsprinsippet.
- Nærhetsprinsippet.
- Samvirkeprinsippet.

I dokumentet *«MK Overordnet beredskapsplan»* er det fastsatt at kriseledelsen og krisestaben ved uønskede hendelser skal samarbeide med og samordne innsatsen fra offentlige myndigheter, private aktører og frivillige organisasjoner for å best utnytte beredskapsressursene.
Det fremkom i intervju at beredskapsplanen med tilhørende tiltakskort er basert på kommunes helhetlige ROS-analyse.

I dokumentet *«Overordnet beredskapsplan del 2»* fremgår det plan for krisekommunikasjon. Det er den utvidede kommunikasjonsstabens leder eller dens stedfortreder som har ansvar for å iverksette planen for krisekommunikasjon og informasjonsberedskap etter samråd med ordfører og/eller rådmann. Moss kommune har utarbeidet tiltakskort ut fra rollene hver enkelt har i en krisesituasjon, hvilket også innebærer at oppgaver knyttet til krisekommunikasjon og informasjonsberedskap skal utføres i henhold til tiltakskortene. I *«Vedlegg A – tiltakskort – etablering og bemanning av kommunikasjonsstab*» til beredskapsplanen operasjonaliseres tiltakene ved at det vises til hva som må vurderes og spørsmål som bør stilles. Revisjonslaget er forelagt eksempel på tiltakskort knyttet til informasjonssikkerhet «*Krisestab-svikt i kommunale IKT-systemer»*. Tiltakskortet inkluderer sjekkliste for varsling, etablering av krisestab, håndtering av hendelsen og normalisering.

Det fremkom i intervju at det ikke har vært avholdt beredskapsøvelser for nye Moss kommune (sammenslått 01.01.2020). Moss kommune har påbegynt arbeidet med å planlegge beredskapsøvelse knyttet til andre kommunale ansvarsområder, som også vil inkludere håndtering av IKT-systemer i krisesituasjon. Det fremkom i intervju at detaljene i øvelsene enda ikke er fastsatt. I dokumentet «*Øvelsesplaner sikkerhet*» fremgår det at Moss kommune har valgt å avvente øvelser tilknyttet informasjonssikkerhetshendelser frem til prosessen med å rekruttere informasjonssikkerhetsansvarlig er ferdigstilt.

6.4 Vurderinger

Moss kommune har i noen grad etablert et styringssystem på anerkjente standarder

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller revisjonskriteriet.

Revisjonslaget ble informert om at Moss kommune baserte sitt styringssystem på ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet. Det fremgår av dokumentet «MK Retningslinjer informasjonssikkerhet og personvern» at disse er basert på ISO/IEC 27001. Det er ikke et lovkrav å være i samsvar med ISO/IEC 27001, men det er både i henhold til beste praksis og eForvaltningsloven §15 at organisasjonen organiserer sitt sikkerhetsarbeid i henhold til anerkjente standarder for styringssystem. Revisjonslaget har derfor lagt til grunn at Moss kommune baserer sitt styringssystem for informasjonssikkerhet på den anerkjente standarden ISO/IEC 27001. Revisjonslaget mener derfor at Moss kommune bør etterleve overordnede føringer som standarden stiller krav til, herunder styrende dokumenter knyttet til informasjonssikkerhet, roller og ansvar, risikostyring knyttet til informasjonssikkerhet, kompetanseheving og opplæring, kontrolltiltak og forbedringstiltak (avvik og korrigerende tiltak). Revisjonslaget mener at nøkkelpersoner i kommunen må ha kompetanse innen ISO/IEC 27001 for å kunne basere ledelsessystemet på standarden.

Det er avdekket forbedringspotensial knyttet til at kun én person har kompetanse i ISO/IEC 27001, samt én annen som har gjennomført introduksjonskurset til ISO/IEC 27701 (Foundation). I likhet med ISO/IEC 27001 stiller eForvaltningsforskriftens § 15 krav til at forvaltningsorganet skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten. I tillegg bør det skilles mellom de ulike hierarkiske nivåene i styringssystemet. *«MK Retningslinje informasjonssikkerhet og personvern»* inneholder en blanding av strategiske og operasjonelle føringer, som fremstår uoversiktlig og lite hensiktsmessig. Overordnede strategiske føringer knyttet til informasjonssikkerhet burde vært fastsatt i en overordnet policy for informasjonssikkerhet. Videre er ikke *«MK Retningslinje informasjonssikkerhet og personvern»* formelt godkjent og implementert i kommunen.

Moss kommune har i stor grad etablert mål og sikkerhetsstrategi for informasjonssikkerhet

Revisjonslaget vurderer at Moss kommune i stor grad oppfyller revisjonskriteriet.

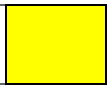
Moss kommune har etablert mål og sikkerhetsstrategi for informasjonssikkerhet i sitt dokument «*IT-Strategi for Moss kommune 2021-2025».* I dokumentet er det fastsatt hvilke målsetninger Moss kommune har knyttet til informasjonssikkerhet samt hvilke aktiviteter som skal utføres for å nå målene.

Det er fastsatt sikkerhetsmål for arbeidet med informasjonssikkerhet i dokumentet *«Retningslinjer informasjonssikkerhet og personvern».* Revisjonslaget er innforstått med at dette også er et styrende dokument for kommunen, tilgjengelig på deres QRM-system og ment å være et referansepunkt for alle kommunalt ansatte.

Det er imidlertid avdekket mindre forbedringspotensial til at dokumentet ikke er ferdigstilt eller implementert. I tillegg inneholder dokumentet en blanding av styrende, gjennomførende og kontrollerende

elementer samt utydelighet knyttet til hvorvidt dokumentet er ment som en policy, prosess eller retningslinje. Dette kan bidra til å skape forvirring knyttet til etterlevelse for den enkelte ansatte. Moss kommune bør som et minimum dele opp dokumentet slik at styrende elementer på policy nivå skilles ut i eget dokument, retningslinjer for den enkelte ansatte i et annet og retningslinjer på ledelsesnivå i et tredje.

Moss kommune har i noen grad definert roller og ansvar for informasjonssikkerhet



Revisjonslaget vurderer at Moss kommune i noen grad oppfyller revisjonskriteriet.

Det eksisterer en nåværende organisering av roller og ansvarsområder på informasjonssikkerhet og en fremtidig plan med justeringer og forbedringer av dette som følge av ny CISO-rolle. Dette fremgår av flere styrende dokumenter. Det er både gjennomført nyansettelser for å forbedre kompetanse i kommunen samt foreslått andre ansettelser for å forbedre.

Ut fra mottatt dokument *«Organisering av sikkerhetsarbeidet»* vurderer revisjonslaget at beskrevet fordeling og organisering av ansvar og roller er hensiktsmessig, som også vil forsterkes av planlagte tiltak knyttet til etablering av CISO-rollen.

Imidlertid, er det avdekket forbedringspotensial knyttet til tydeliggjøring av dagens rolle -og ansvarsfordeling. Dette fremgår av den tvetydige kommunikasjonen om rolle -og ansvarsfordelingen i *«MK Retningslinje informasjonssikkerhet og personvern»* og *«IT-strategi for Moss kommune 2021-2025».* Videre fremstår det noe uklart hvem som er ansvarlig for gjennomføring av ledelsens gjennomgang på ledelsesnivå i kommunen samt hvor hyppig dette skal gjennomføres.

Moss kommune har i liten grad gjennomført risikovurderinger knyttet til informasjonssikkerhet

Revisjonslaget vurderer at Moss kommune i liten grad oppfyller revisjonskriteriet.

Det er avdekket vesentlig forbedringspotensial knyttet til å etablere en strukturert prosess for gjennomføring av risikovurderinger tilknyttet informasjonssikkerhet. Revisjonslaget er informert om at det er tiltenkt at den nye CISO-rollen vil ha dette som et prioritert ansvarsområde og at risikovurderinger i dag gjøres ad-hoc. Moss kommune har gjennomført helhetlig kommune-ROS, men denne inkluderer ikke informasjonssikkerhet. Revisjonslaget er også forelagt oversikt over risikovurderinger på fagsystemnivå.

Moss kommune har i stor grad et godt etablert system for avvik

Revisjonslaget vurderer at Moss kommune i stor grad oppfyller revisjonskriteriet.

Det er imidlertid avdekket mindre forbedringspotensial knyttet til kommuniseringen av hvordan de ansatte skal melde avvik da det er et ganske stort antall ansatte 37,7% som svarer at det ikke er kjent med hvordan avvik rapporteres. Revisjonslaget mener dette kan forbedres ved å sørge for systematisk og regelmessig opplæring av ledere og ansatte og ved å sikre at kvalitetsutvalgene etableres og gjennomfører sine oppgaver.

Moss kommune gjennomfører ikke sikkerhetsrevisjoner, men har i noen grad andre kontroller knyttet til informasjonssikkerhet

Revisjonslaget vurderer at Moss kommune i noen grad oppfyller revisjonskriteriet.

Revisjonslaget bemerker at Moss kommune har etablert et sikkerhets- og personvernutvalg, hvor oppfølging av avvik er ett av hovedtemaene. I tillegg har status på informasjonssikkerhetsområdet vært tema i kommunegruppens ledergruppe (KLG).

Det er imidlertid avdekket mindre forbedringspotensial knyttet til at det ikke er gjennomført en sikkerhetsrevisjon av informasjonssikkerhet og heller ikke avholdt beredskapsøvelser. Revisjonslaget er imidlertid informert om at det planlegges gjennomført en internrevisjon av informasjonssikkerhet i Q3 i 2021 samt en beredskapsøvelse. Moss kommune har gjennomført ledelsens gjennomgang for informasjonssikkerhet og personvern for enkelte kvalitetsutvalg, som da har som hensikt å gi ledelsen oversikt over gjennomførte aktiviteter og forbedringspotensialet for å sikre at styringssystemet kontinuerlig forbedres og bidrar til å oppnå fastsatte mål. Dermot, har ikke ledelsens gjennomgang vært gjennomført for alle kvalitetsutvalg eller på kommuneledelsesnivå. Det fremstår uklart for revisjonslaget hvor hyppig ledelsens gjennomgang skal avholdes.

Moss kommune har i stor grad etablert en beredskapsplan og øvelser.

Revisjonslaget vurderer at Moss kommune i stor grad oppfyller revisjonskriteriet.

Moss kommune har fastsatt en helhetlig beredskapsplan som inkluderer alle elementer fastsatt i forskrift om kommunal beredskapsplikt. Beredskapsplanen fremstår som tydelig og enhetlig.

Det er imidlertid avdekket mindre forbedringspotensial knyttet til å avholde øvelse og/eller trening av informasjonssikkerhetshendelser. Revisjonslaget er informert om at det er planlagt gjennomført en beredskapsøvelse i løpet av året som også i noen grad vil omfatte informasjonssikkerhet.

6.5 Konklusjon og anbefalinger

Moss kommune har i noen grad etablert et tilfredsstillende styringssystem (internkontroll) for informasjonssikkerhet.

Moss kommune har et godt system for avvikshåndtering, mål for arbeidet med informasjonssikkerhet samt en detaljert og oversiktlig beredskapsplan.

Det er derimot avdekket forbedringspotensial, hvor revisjonslaget anbefaler at kommunen bør:

- Ha ytterligere kompetanseheving av nøkkelpersoner innen ISO/IEC 27001 for å kunne basere styringssystemet på standarden.
- Godkjenne, implementere og kommunisere styrende dokumenter for styringssystemet.
- Arbeide aktivt med kommunikasjon av kommunens retningslinjer på tvers og nedover i kommunen.
- Gjennomføre ytterligere formelle kompetansehevende tiltak blant kommunens ansatte.
- Ha en systematisk tilnærming til risikostyring knyttet til informasjonssikkerhet.
- Gjennomføre og dokumentere kontrolltiltak, herunder sikkerhetsrevisjoner og ledelsens årlige gjennomgang (for øverste ledelse i kommunen).

7 PROBLEMSTILLING 4: I HVILKEN GRAD HAR DE ANSATTE KJENNSKAP TIL KOMMUNENES RETNINGSLINJER OG RUTINER FOR INFORMASJONSSIKKERHET

7.1 Utleding av revisjonskriterier

I henhold til ISO/IEC 27001 skal det sikres at alle ansatte er klar over og oppfyller sitt ansvar for informasjonssikkerhet. Alle ansatte i virksomheten skal få hensiktsmessig bevisstgjøring, utdanning og opplæring samt regelmessige oppdateringer i organisasjonens interne føringer som er relevant. Det tolkes derfor at kommunen må kommunisere styringssystemet for informasjonssikkerhet for å sikre at dette blir kjent for ansatte i kommunen.

Kommunen skal i henhold til forskrift om kommunal beredskapsplikt § 7 andre ledd ha et system for opplæring som sikrer at alle som er tiltenkt en rolle i krisehåndteringen har tilstrekkelige kvalifikasjoner. Det tolkes derfor at kommunen bør ha en systematisk tilnærming til opplæring av kriseledelsen.

I henhold til lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) § 13 skal enhver som utøver tjeneste eller arbeid for et forvaltningsorgan, plikte å hindre at uautoriserte får adgang eller kjennskap til personlige forhold. Forvaltningslovens § 13 f stiller krav til taushets- og opplysningsplikt dersom man er pålagt taushetsplikt ved bestemmelse i annen lov, forskrift eller instruks av hensyn til private interesser. Det tolkes dermed at Moss kommune må innhente taushetserklæringer fra ansatte der det er hensiktsmessig.

7.2 Revisjonskriterier

Basert på utledningen ovenfor har revisjonslaget utarbeidet følgende revisjonskriterier:

Moss kommune skal:

- sikre at styringssystemet for informasjonssikkerhet integreres i kommunens prosesser og kommuniseres til kommunens ansatte (eForvaltningsforskriften §15 og ISO/IEC 27001).
- skal ha et system for opplæring som sikrer at alle som er tiltenkt rolle i krisehåndteringen har tilstrekkelige kvalifikasjoner (Jf. Forskrift om kommunal beredskapsplikt § 7).
- skal sørge for at hver ansatt har signert en taushetserklæring (Forvaltningslovens §13).

7.3 Datagrunnlag

7.3.1 Sikre at styringssystemet for informasjonssikkerhet integreres i kommunens prosesser og kommuniseres til kommunens ansatte (eForvaltningsforskriften §15 og ISO/IEC 27001)

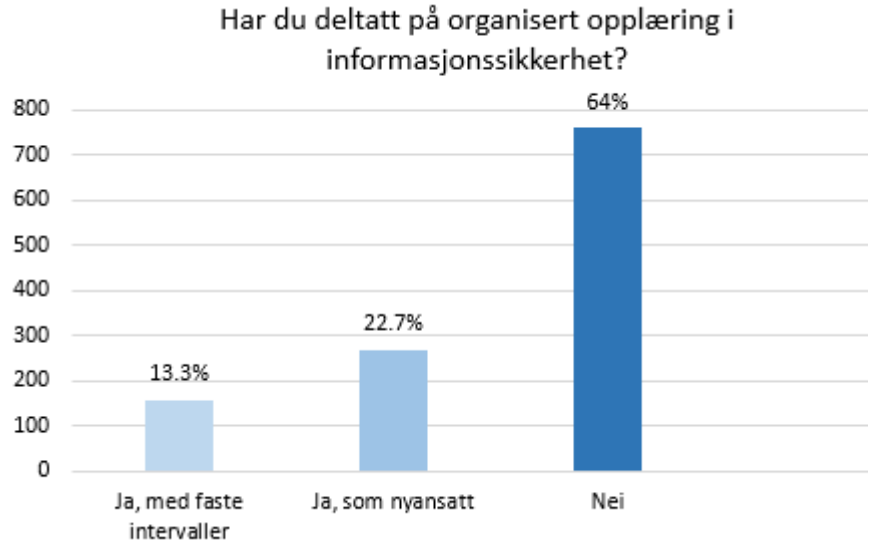
Det fremgår av «*Retningslinjer informasjonssikkerhet og personvern*» at det er leders ansvar å sørge for at alle medarbeidere har gjennomgått innholdet i retningslinjene for informasjonssikkerhet, og at kommunen skal sette kompetansekriterier for medarbeidere og ledere som skal arbeide med informasjonssikkerhet.

Det fremkom i intervju at det er flere kanaler som benyttes for internkommunikasjon ut til de ansatte, eksempelvis Teams. I tillegg var alle intervjuobjektene kjent med at de kunne finne informasjon om

føringer for informasjonssikkerhet i «Risk manager». Imidlertid, mente flere av intervjuobjektene at det var utfordrende å kommunisere fastsatte retningslinjer til de ansatte. Det ble formidlet at enkelte av retningslinjene oppleves kompliserte og omfattende, som intervjuobjektene mente kunne være noe av årsaken til at ansatte har utfordringer med å sette seg inn i fastsatte føringer. Det fremkom i intervju at det er store forskjeller i modenhetsnivå mellom de ulike enhetene og kommunalområdene i kommunen når det gjelder bevissthet knyttet til informasjonssikkerhet.

Det fremkom i intervju tvetydighet knyttet til hvem som er ansvarlig for gjennomføring av opplæring knyttet til informasjonssikkerhet. Flere av intervjuobjektene var ikke innforstått med hva informasjonssikkerhet gikk ut på utover beskyttelse av personopplysninger. Det fremkom i intervju at ledere mangler opplæring innen informasjonssikkerhet. Enkelte enhetsledere har tidligere igangsatt avdelingsrettede tiltak knyttet til informasjonssikkerhet, herunder leselister med relevant innhold knyttet til informasjonssikkerhet eller personvern. Flere av intervjuobjektene mente det var for lite kunnskap knyttet til informasjonssikkerhet i organisasjonen, både på ledernivå og i linjen.

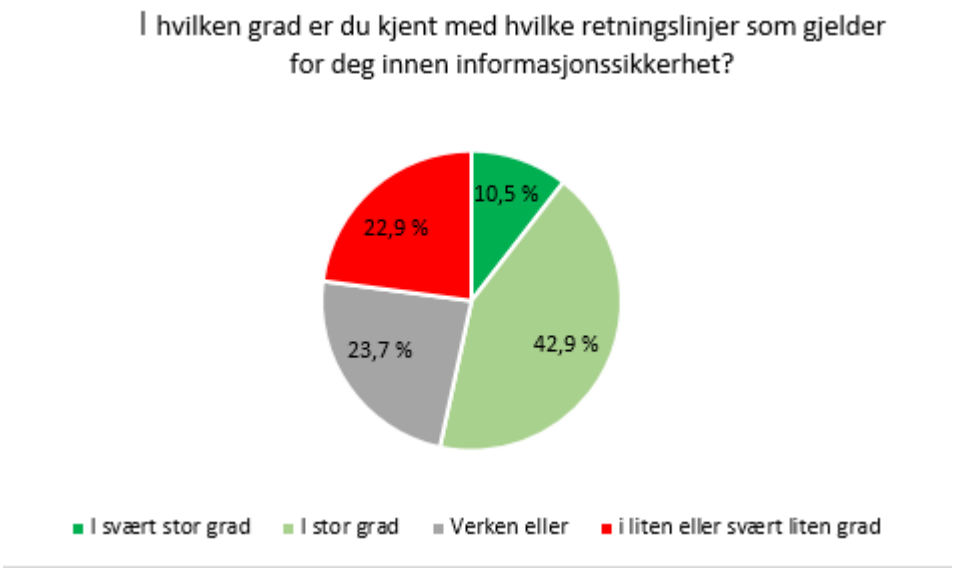
På spørsmål knyttet til opplæring i informasjonssikkerhet i spørreundersøkelsen svarte 64% «nei» på spørsmål om man har deltatt på organisert opplæring innen informasjonssikkerhet (se figur 10).



Figur 10, Svar fra spørreundersøkelsen: "Har du deltatt på organisert opplæring i informasjonssikkerhet?".

Moss kommune har benyttet nyhetsbrev og alternative kommunikasjonskanaler slik som Teams og Yammer for å nå ut til ansatte. Informasjon som har blitt formidlet har vært mindre føringer, slik som informasjonsbehandling av sensitive opplysninger over e-post, bruk av passord og deling av tilganger. Enkelte dokumenter viser til at informasjonssikkerhet har vært på agendaen blant ledergruppen i Moss kommune, som blant annet «*MK IT-sikkerhet og hjemmekontor*» som inneholder retningslinjer for bruk av IKT-utstyr på hjemmekontor.

På spørsmål om man er kjent med hvor man finner retningslinjer og rutiner for informasjonssikkerhet i Moss kommune svarte et flertall (53,6%) «ja», mens 46,4 % svarte «nei» i utsendt spørreundersøkelse. Ut fra svarene i spørreundersøkelsen illustrert i figur 11 svarte 10,5% at de i «svært stor grad» var kjent med hvilke retningslinjer som gjaldt for dem, mens 22,9% svarte «i liten grad» eller «i svært liten grad». Det var 23,7% som svarte «verken eller».



Figur 11, Svar fra spørreundersøkelsen: "I hvilken grad er du kjent med hvilke retningslinjer som gjelder for deg innen informasjonssikkerhet?".

7.3.2 Skal ha et system for opplæring som sikrer at alle som er tiltenkt rolle i krisehåndteringen har tilstrekkelige kvalifikasjoner (Jf. Forskrift om kommunal beredskapsplikt § 7)

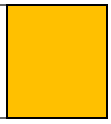
Det fremkom i intervju at det er fastsatt en opplæringsplan for personer med tiltenkt rolle og funksjon i kriseledelsen. I dokumentet *«Opplærings- og kompetanseplan Moss kommune»* er det vist til hvilken kompetanse de ulike funksjonene i kriseledelsen som et minimum skal besitte, samt hyppighet av kompetanseheving. På grunn av covid-19 og medfølgende restriksjoner har derimot opplæring ikke blitt gjennomført i henhold til plan. Det ble formidlet at Moss kommune har nøkkelpersoner med tilstrekkelig kompetanse knyttet til å håndtere en uønsket informasjonssikkerhetshendelse. Det fremkom i intervju at kompetanse til å benytte krisehåndteringsverktøyet CIM er varierende for de med dedikerte roller i krisehåndtering.

Det fremkom i intervju at majoriteten av intervjuobjektene ikke hadde gjennomført opplæring knyttet til håndtering av informasjonssikkerhetshendelser i regi av Moss kommune.

7.3.3 Taushetserklæring

Det ble formidlet i intervju at alle ansatte skal signere taushetserklæring. Alle intervjuobjektene som ble spurt bekreftet å ha signert taushetserklæring.

7.4 Vurderinger

Moss kommune har i liten grad sikret at styringssystemet for informasjonssikkerhet integreres i kommunens prosesser og kommuniseres til kommunens ansatte	

Revisjonslaget vurderer at Moss kommune i liten grad oppfyller revisjonskriteriet.

Det er avdekket vesentlig forbedringspotensialet til å bekjentgjøre roller og ansvar for ansatte i kommunen. Gjennom intervjuer var enkelte av den oppfatning av at informasjonssikkerhet var noe IKT-avdelingen hadde ansvar for. Informasjonssikkerhet krever et helhetlig arbeid, både på ansatt- og ledelsesnivå. Det er få som har gjennomført regelmessig opplæring innen informasjonssikkerhet i regi av Moss kommune. Videre er det avdekket forbedringspotensial knyttet til at 37,7% av de spurte i spørreundersøkelsen ikke var kjent med hvordan avvik knyttet til personvern og informasjonssikkerhet skal rapporteres. Imidlertid, har Moss kommune flere dokumenterte rutiner for å melde avvik – det er allikevel ikke godt nok kjent blant kommunens ansatte.

Moss kommune har i stor grad et system for opplæring som sikrer at alle som er tiltenkt rolle i krisehåndteringen har tilstrekkelige kvalifikasjoner	

Revisjonslaget vurderer at Moss kommune i stor grad oppfyller revisjonskriteriet.

Det er imidlertid avdekket mindre forbedringspotensial knyttet til å øke kompetanse på håndtering av rene informasjonssikkerhetshendelser.

Moss kommune har i svært stor grad sørget for at hver ansatt har signert taushetserklæring	

Revisjonslaget vurderer at Moss kommune oppfyller revisjonskriteriet fullt ut.

7.5 Konklusjon og anbefalinger

Kommunen har sørget for at de ansatte har signert taushetserklæring, samt at alle som er tiltenkt en rolle i krisehåndteringen til stor grad har tilstrekkelige kvalifikasjoner.

Samtidig har Moss kommune i liten grad sikret at styringssystemet for informasjonssikkerhet er blitt integrert i kommunenes prosesser og blitt kommunisert til kommunenes ansatte. Kommunen har sørget for at de ansatte har signert taushetserklæring, samt at alle som er tiltenkt en rolle i krisehåndteringen til stor grad har tilstrekkelige kvalifikasjoner.

Basert på våre vurderinger og konklusjon anbefaler vi at kommunen bør:

- Tydeliggjøre roller og ansvar for informasjonssikkerhet i sine styrende dokumenter.
- Gjennomføre regelmessig og omfattende program for opplæring innen informasjonssikkerhet.
- Sørge for dokumenterte rutiner på kommunikasjon til sine ansatte.
- Gjennomføre beredskapsøvelser på hendelser knyttet til informasjonssikkerhet.

Moss kommune,
Rådhuset, Kirkegata 15,
Postboks 175, 1501 Moss.

+47 69 24 80 00
Org.nr.: 920817521

Østre Viken Kommunerevisjon Iks
Råkollveien 103
1664 ROLVSØY

Deres ref.: Vår ref.: 21/4068-34- ARSO Dato: 06.12.2021

Kommunedirektørens kommentar til forvaltningsrevisjonen personvern og informasjonssikkerhet

Moss kommune tar forvaltningsrevisjonens konklusjoner og anbefalinger til etterretning, samt vil bruke den som støtte og prioritering i det videre arbeidet.

I forvaltningsrevisjonen beskriver forhold som kommuneorganisasjonen selv har registrert, enten som avvik, forbedringsforslag eller oppgaver og aktiviteter, men som vi ikke har kunnet ferdigstille pga. utfordringer grunnet pandemi og etablering av ny kommune med omstillinger. Spesielt opplæring har vært utfordrende å organisere i denne perioden.

Rapporten beskriver at Moss kommune som organisasjon er forholdsvis modne på personvernområdet og med høyt fokus på personvern. Videre er det etablert god internkontroll for informasjonssikkerhet og det vurderes at kommunen har kontroll på informasjonen om ansatte som eksponeres på internett gjennom bevisste valg knyttet til hva som publiseres og eksponeres.

Det administrasjonen vil prioritere først er arbeidet med behandlingsprotokoll, systematiserte personvernkonsekvensvurderinger og opplæring.

Om penetrasjonstesten, offentliggjør Moss kommune en rekke epostadresser til blant annet politikere, og det er derfor naturlig at det ble funnet en del epostadresser. Moss kommune har også en rekke aktiviteter som benytter nettsider, og det er derfor naturlig at det ble funnet en del domener og subdomener.

Med hilsen

Dette dokumentet er elektronisk godkjent av

Hans Reidar Ness
Kommunedirektør

Are Hammervold Solvang
Direktør organisasjon
Stab organisasjon

Mottakere:
Bjørnar Bakker Eriksen
Østre Viken
kommunerevisjon IKS

VEDLEGG

10.1 Oversikt over mottatt dokumentasjon

10.2 Rapport fra penetrasjonstest

Oversikt over mottatt dokumentasjon

- 191010-ID 054-Tekstbidrag i økonomiplanen 2020-IT-enheten
- 200302-ID 056-Stillingsbeskrivelse Sikkerhetsansvarlig IT
- 200706-ID 056-Stillingsbeskrivelse Teamkoordinator -klient -sikkerhet
- 200821-ID 048-ROS IT-sikkerhet MK
- 201020-ID 049-Anbefalingsnotat PWD-policy i MK
- 201215-ID 049-Anbefalingsnotat – Enhetlig epostklient på mobiler
- 210303-ID 054 Årsberetning 2021- IT
- 210510-Standard sikkerhetskrav for skytjenester
- 210511-ID 051- IT-strategi for Moss kommune 2021-2025 v.1.0
- 210920-ID 047-Overordnet IKT beredskapsplan ny-revisjon
- 210921-ID 060-Backup miljø i Moss kommune
- 210922-Dokumentoversikt forsendelse fra IT
- 210922-ID 043-Organisering av sikkerhetsarbeidet
- 210922-ID 044-Årshjul sikkerhetsarbeidet
- 210922-ID 045-KPI-er for sikkerhetsarbeidet
- 210922-ID 046-Øvelsesplaner sikkerhet
- 210922-ID 048-ROS og analyser
- 210922-ID 049-Ledergruppereferater med tema sikkerhet
- 210922-ID 050-Dokumenterte gjennomganger
- 210922-ID 052-Prosess, rutiner, metodikk, strategier sikkerhet
- 210922-ID 053-2 Krisestab- Svikt i kommunale IKT-systemer
- 210922-ID 053-3 MK Helhetlig ROS_Moss kommune
- 210922-ID 053-4 MK Vedlegg B til overordnet beredskapsplan roller og ansvar
- 210922-ID 053-Roller og ansvar i internkontroll og sikkerhetsarbeid
- 210922-ID 054-Budsjetter og årsrapport infosikk
- 210922-ID 055-Ressursoversikt
- 210922-ID 057-Bistandsavtaler
- 210922-ID 058-Ansvar og roller sikkerhets, sivilbesk, POL
- 210922-ID 061-Kompetanse- og opplæringsplan
- 210922-ID 062-Ansatte som utarbeider styrende dokumenter
- 210922-ID 063-Ansatte med kompetanse på ISO/IEX 27001, 2, 5
- 210922-ID 064-Ansatte med kompetanse på vurdering-håndtering infosikkrisk
- 210922-ID 065-Ansatte kurs i IKT-sikkerhet-informasjonssikkerhet og personvern
- 210922-ID 066-Kompetansekartlegging sikkerhet
- Certificate DPO AB
- DOK Barnehagemapper
- DOK Bestilling av tilganger i WebSak
- DOK Elevmapper
- DOK Innsynsbegjæringer (generelle og spesielle)
- DPIA Familieteam
- EH – Opplæringskompendium for nyansatte og lærlinger
- Helse – Innsyn i dokumenter for myndige personer over 18 år

- Helse – Innsyn i dokumenter for umyndige personer under 18 ¨r
- HR Rolle- og oppgavebeskrivelse personvernombud
- HR Stillingsbeskrivelse koordinator team internkontroll og kvalitet
- HR Stillingsbeskrivelse kvalitetskonsulent
- ID 060-Veeam restore prosedyrer
- ID 067-Stillingsbeskrivelse informasjonssikkerhetsansvarlig
- Innovasjonsstrategi 1.0
- Internrevisjon Moss kommune 26082021
- Investeringer budsjett 2020 HR-behandlingskartleggingsverktøy
- Investeringer budsjett 2020 HR-system for samtykkeerklæring.
- KLG 26 august informasjonssikkerhet
- KLG 26 august personvern og informasjonssikkerhet
- Kommunedirektøren april 2021
- Kommuneplanens samfunnsdel Moss 2030
- Kompetanse – opplæringsplan personvern, notat til revisjon 2021
- Kopi av gjennomføring av DPIA KINS-versjon – Visma sikker sak - Familieteam
- Kursdeltakere GDPR
- MK- Rutiner for automatiserte individuelle avgjørelser
- MK Akseptkriterier
- MK Analyse Dataflyt spørreskjema til personopplysningsloven
- MK Behandlingsoversikt og protokoller modul 1 GDPR
- MK Bruk av videokonsultasjon i Teams
- MK Databehandleravtale ENG
- MK Databehandleravtale NO
- MK Definisjoner for avvik og uønskede hendelser, skader og varsling
- MK GDPR og internkontroll Modul 4 GDPR
- MK Generelt om GDPR og informasjonssikkerhet Modul 2 GDPR
- MK Hjemmekontor og personvern
- MK HMS Håndtering av varsling
- MK HMS Intern varsling
- MK Hvordan håndtere avvik og uønskede hendelser
- MK Hvordan melde avvik på sikkerhets- og personvernbrudd Modul 5 GDPR
- MK Hvordan skal jeg som ansatt forholde meg til GDPR
- MK Håndtering av brudd på personopplysningsloven
- MK Innsyn i og overvåking av ansattes e-post, private filer og logger, samt bruk av elektronisk lagret materiale
- MK Innsyn i og overvåking av ansattes e-post, private filer og logger
- MK Internkontroll og kvalitet i Moss kommune
- MK IT-sikkerhet på hjemmekontor
- MK Ledelsens gjennomgang informasjonssikkerhet og personvern
- MK Melde avvik i web applikasjonen for avvik
- MK Oversikt over avviksområder og avvikskategorier
- MK Oversikt over fagsystem personopplysningsloven (behandlingsprotokoll)
- MK Oversikt over årsakskategorier og årsaker
- MK Personopplysningsloven GDPR spørsmål og svar
- MK Personvern oversikt oppgaver og ansvar
- MK Personvernerklæring generell

- MK Personvernveileder
- MK Retningslinje for avvikshåndtering og årsaksanalyser NY GODKJ
- MK Retningslinje for brudd på personopplysningsloven
- MK Retningslinje for databehandleravtale
- MK Retningslinje informasjonssikkerhet og personvern
- MK Risikovurdering og DPIA Modul 3 GDPR
- MK Sikring av databehandleravtale
- MK Sjekkliste for databehandleravtale
- MK Sjekkliste for egenkontroll av informasjonssikkerhet og GDPR
- MK Slettede avvik og skader
- Opplæringskalender IKK 2020
- Oversikt dokumenter – utklipp internkontroll og kvalitet
- Oversikt dokumenter under informasjonssikkerhet
- Oversikt dokumenter under IT
- Oversikt over rutiner for journalføring i Acos WebSak pr. 17.09.2021
- Plan for krisekommunikasjon og informasjonsberedskap
- Risikovurderinger
- Utskrift avvik personvern fra 01 jan 2020 til 18 sep 2021
- Utskrift forbedringsforslag personvern inklusiv 01 jan 2020 til 18 sep 2021
- Varsling og informasjon om varsling
- Vedlegg G Opplæring kompetanseplan Moss
- Årsberetning 2020 kvalitet
- Årsrapport og årsregnskap 2020 side 55.