Rapport

MARKER KOMMUNE

08.11.2024

Forvaltningsrevisjon

Personvern

Innhold

1 SAMMENDRAG

Revisjonens fremgangsmåte

Temaet som kontrollutvalget ønsket undersøkt, er løst gjennom en forvaltningsrevisjon i tråd med «Standard for forvaltningsrevisjon» (RSK 001/god revisjonsskikk) og ved å følge Østre Viken kommunerevisjons (ØVKR) mal for forvaltningsrevisjoner. Revisjonen er utført med bistand fra rådgivningsselskapet BDO AS. Som et ledd i etterlevelse av RSK 001 har det vært en dedikert ressurs med ansvar for å kvalitetssikre at revisjonen har fulgt standarden. Revisjonen har også hatt dialog med både ØVKR og Marker kommune under gjennomføringen av revisjonen.

Fremdriftsplanen besto av følgende elementer:

- Planlegging
    - Oppstartsmøter
    - 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.
    - Beskrivelse av datagrunnlag.
    - Analyse, vurdering og konklusjon.
- Sluttføring
    - Utarbeidelse av rapport.
    - Verifisering av faktagrunnlag fra Marker kommune.
    - Gjennomgang av rapport med Marker kommune.

Revisjonens funn og konklusjoner

Revisjonslaget har jobbet ut fra følgende problemstilling: Har Marker kommune sikret at kommunen etterlever kravene i personopplysningsloven, herunder personvernforordningen (GDPR)?

Revisjonslaget vurderer at Marker kommune har etablert flere hensiktsmessige tiltak for å sikre at kommunen etterlever kravene i personopplysningsloven og GDPR. Kommunen har, til tross for kommunens størrelse, etablert et internkontrollsystem for personvern som består av styrende, gjennomførende og kontrollerende elementer i tråd med veiledning fra Datatilsynet.

Revisjonslaget har likevel identifisert flere krav som ikke er ivaretatt på en tilfredsstillende måte. Dette gjelder i hovedsak omfang og innhold i rutiner og retningslinjer. Mens kommunens rutiner og retningslinjer ikke dekker alle områdene som er anbefalt i Datatilsynets veiledning om hvordan kravet til internkontroll etter GDPR artikkel 24 skal forstås, er det revisjonslagets vurdering at kommunen har et mindre omfang av rutiner, retningslinjer og arbeidsinstrukser for personvern, enn forventet. Revisjonslaget mener at rutiner og retningslinjer, samt konkretisering av roller og ansvar for gjennomføring av personvernaktiviteter, er det området der Marker kommunes internkontroll har størst potensial for forbedring.

Videre mener revisjonslaget at kommunen har potensial for forbedring når det gjelder fastsetting av slettefrister og etablering av sletterutiner, etablering av rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter, etablering av rutiner for å sørge for kontroll av at databehandlere

ivaretar krav til personvern, og kartlegging av overføringer av personopplysninger til land utenfor EU/EØS.

Revisjonslaget har gjort følgende vurderinger knyttet til revisjonskriteriene for problemstillingen:

Marker kommune har i noen grad etablert en tilfredsstillende internkontroll for personvern	Gul
Marker kommune har i stor grad en oppdatert protokoll over behandlingsaktiviteter som tilfredsstiller kravene i GDPR artikkel 30	Lysegrønn
Marker kommune har i stor grad sørget for rettslig grunnlag for behandling av personopplysninger blir vurdert og dokumentert	Lysegrønn
Marker kommune har i liten grad etablert sletterutiner for sin behandling av personopplysninger	Oransje
Marker kommune har i stor grad sørget for å informere de registrerte om behandlingen av deres personopplysninger	Gul
Marker kommune oppfyller ikke revisjonskriteriet om å ha etablert rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter	Rød
Marker kommune har i noen grad har etablert egnede tiltak for å ivareta personopplysningssikkerheten	Gul
Marker kommune har i noen grad sørget for å gjennomføre personvernkonsekvensvurderinger når det er nødvendig	Gul
Marker kommune har i liten grad sørget for at databehandlere ivaretar krav til personvern og sikret at det inngås databehandleravtaler	Gul
Marker kommune har i liten grad kartlagt overføring av personopplysninger til utenfor EU/EØS og gjennomført nødvendige vurderinger og tiltak ved overføringer	Oransje
Marker kommune har utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39	Grønn
Marker kommune har i noen grad sørget for at avvik knyttet til personvern blir meldt, registrert og håndtert	Gul

Revisjonens anbefalinger

Revisjonslaget konkluderer med at Marker kommune har etablert flere hensiktsmessige tiltak for å sikre at kommunen etterlever kravene i personopplysningsloven og GDPR.

Basert på våre vurderinger og konklusjon anbefaler vi at Marker kommune bør:

a) Utarbeide en oversikt over alle rutiner og retningslinjer for vern av personopplysninger i kommunen, samt dokumentere hvordan internkontrollsystemet henger sammen. Videre bør kommunen oppdatere malene for risikovurdering slik at de inkluderer muligheten for å vurdere hvilke konsekvenser identifiserte risikoer kan ha for enkeltpersoners rettigheter, i samsvar med GDPR artikkel 24 og 32. Kommunen bør også gjennomføre oppdaterte risikovurderinger på personvernområdet der formålet er å identifisere ytterligere behov for skriftlige rutiner og retningslinjer for håndtering av personopplysninger.

   Videre bør kommunen oppdatere styrende dokumenter for å inkludere detaljerte beskrivelser av ansvar og roller for personvernoppgaver. Dette inkluderer å sikre at nøkkelpersoner og virksomhetsledere har en klar forståelse av sine roller og ansvar innen personvern. Kommunen bør også sørge for regelmessig og rollebasert opplæring innen personvern. Dette inkluderer å sikre at alle ansatte

får tilstrekkelig opplæring i personvernprinsipper, kommunens retningslinjer og sentrale krav i GDPR. Etablering av et personvernteam kan bidra positivt til dette arbeidet.

b) Sørge for at alle felter i behandlingsprotokollen fylles ut med nøyaktige og relevante opplysninger. For eksempel, under feltet «Mottakere av personopplysninger», bør det spesifiseres hvem som mottar opplysningene, i stedet for å angi at opplysningene ikke overføres til tredjeland. Tilsvarende bør feltet «Sletting og lagring» inneholde konkrete opplysninger om sletting og lagring av data, i stedet for å nevne at det ikke er automatiske avgjørelser i behandlingen. Kommunen bør også tydelig dokumentere hvem som har ansvar for å fylle ut og oppdatere behandlingsprotokollen.

c) Etablere klare og spesifikke sletterutiner for sin behandling av personopplysninger. Dette innebærer å utarbeide skriftlige rutiner for sletting og lagring av data for hver behandlingsaktivitet. Hvilke sletterutiner som gjelder, bør dokumenteres i kommunens behandlingsprotokoll.

d) Oppdatere personvernerklæringene slik at de inneholder identitet og kontaktinformasjon til den behandlingsansvarlige, samt kontaktopplysningene til personvernombudet, i samsvar med GDPR artikkel 13 nr. 1 a og b. Kommunen bør også sørge for at formålet med behandlingen beskrives så tydelig som mulig. Videre bør kommunen også sikre at informasjonen i personvernerklæringene samsvarer med overskriftene de er plassert under. Dette kan oppnås ved å gjennomgå og revidere erklæringene for å sikre at informasjonen er korrekt plassert og lett forståelig. Til sist bør kommunen sikre at alle ansatte er kjent med hvordan deres personopplysninger behandles. Dette kan for eksempel gjennomføres gjennom opplæringsprogrammer.

e) Etablere skriftlige rutiner for hvordan kommunen skal håndtere forespørsler fra de registrerte om å utøve sine rettigheter etter GDPR. Rutinene bør beskrive hvordan forespørsler fra registrerte om å utøve sine rettigheter etter GDPR skal mottas, behandles og besvares innen fastsatte frister, med klare ansvarsfordelinger, dokumentasjon og rutiner for verifisering av identitet.

f) Etablere skriftlige rutiner for når personvernkonsekvensvurderinger skal gjennomføres. Rutinene bør beskrive hvem som er ansvarlig for å gjennomføre vurderingene, hvilket malverk som skal benyttes, når personvernombudet skal involveres og når forhåndsdrøfting med Datatilsynet skal finne sted. Kommunen bør også vurdere å oppdatere malen for personvernkonsekvensvurdering med flere hjelpetekster. Dette vil gi brukerne bedre veiledning om hva de skal beskrive i hver del av vurderingen, og sikre at alle nødvendige elementer blir dekket.

g) Etablere skriftlige rutiner for inngåelse og oppfølging av databehandleravtaler, med det formål å sikre at alle avtaler, enten basert på kommunens eller leverandørens mal, oppfyller kravene i GDPR artikkel 28. Rutinen bør inkludere tydelige roller og ansvar, krav om risikovurdering av leverandør før avtaleinngåelse, en kvalitetssikringsprosess ved bruk av leverandørens avtale med klar ansvarsfordeling for eventuell godkjenning, samt rutiner for oppdatering og fornyelse av avtalene ved behov. I tillegg bør kommunen etablere en prosess for regelmessig kontroll og revisjon av databehandlere, inkludert periodiske gjennomganger for å sikre at databehandlere etterlever avtalene og ivaretar krav til personvern.

h) Gjennomføre en grundig kartlegging av alle mulige overføringer av personopplysninger til tredjeland. Dette inkluderer å identifisere alle databehandlere og underleverandører som kan ha tilgang til personopplysninger utenfor EU/EØS.

i) Etablere skriftlige rutiner for rapportering, registrering og oppfølging av avvik. Dette inkluderer å sikre at alle ansatte er kjent med hva et personvernavvik utgjør, samt etablere beskrivelser av hvordan slike avvik skal rapporteres og håndteres. Videre bør kommunen gjennomføre opplæring og bevisstgjøringsaktiviteter for alle ansatte for å øke kompetansen om personvernavvik. For å sikre at alle rapporteringspliktige avvik meldes til Datatilsynet og at underretningsplikten til de registrerte overholdes, bør kommunen etablere en rutine for regelmessig gjennomgang og oppdatering av avvikssystemet.

2 MANDAT FOR FORVALTNINGSREVISJONEN

Revisjonen skal i henhold til kommunelovens § 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, som vil si å følge *Standard for forvaltningsrevisjon* (RSK 001) (NKRF[1], 2020). Dette innebærer blant annet at rapporten skal skille klart mellom innsamlede data (fakta) og revisjonens vurderinger. Det skal være en tydelig sammenheng mellom problemstillinger, faktaopplysninger[2], 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 Marker kommune i sak 21/86 (14.12.2021)

Plan for gjennomføring av forvaltningsrevisjonen ble vedtatt i kontrollutvalget møte 21. mai 2024, i sak 24/14. Prosjektplanen ble vedtatt i tråd med revisjonens forslag

Forvaltningsrevisjonen er gjennomført etter vedtatt prosjektplan i tidsrommet 02.06.2024– 12.11.2024. Vi har gjennomført et oppstartsmøte med kommuneadministrasjonen slik at også administrasjonens innspill er vurdert i planleggingsprosessen.

Vi har kvalitetssikret innsamlet data/fakta underveis, både gjennom verifisering av intervjuer og intern kvalitetssikring. I tillegg er faktaopplysningene i sin helhet verifisert av kommunen, slik at eventuelle feil eller misforståelser er rettet opp. Revisjonen avholdte avsluttende møte med administrasjonen 23.10.2024 hvor revisjonens vurderinger, konklusjoner og anbefalinger ble gjennomgått. I etterkant av møtet er rapporten sendt på høring til rådmannen/kommunedirektøren. Kommunedirektørens uttalelse fremgår av vedlegg 6.1.

Forvaltningsrevisjonen er gjennomført av forvaltningsrevisorer Anine Klepp, Elisabeth Aspaas Runsjø, Ovidia Andersen, og kvalitetssikret av Arnt Olav Aardal. Oppdragsansvarlig revisor er Casper Støten. 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 for et godt samarbeid i forbindelse med gjennomføringen av forvaltningsrevisjonen.

Østre Viken kommunerevisjon IKS
Rolvsøy, 8. november 2024

Casper Støten (sign.)
oppdragsansvarlig revisor

Elisabeth Aspaas Runsjø (sign.)
utførende forvaltningsrevisor

[1] NKRF er en faglig interesseorganisasjon og et kompetanseorgan for kontroll og revisjon av kommunal/offentlig virksomhet.

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

3 FREMGANGSMÅTE

3.1 Problemstilling og avgrensninger

3.1.1 Problemstilling

Rapporten besvarer følgende problemstilling:

«Har Marker kommune sikret at kommunen etterlever kravene i personopplysningsloven, herunder personvernforordningen (GDPR)?»

3.1.2 Avgrensninger

Revisjonen har i hovedsak vært avgrenset til en overordnet gjennomgang av sentrale krav i personvernforordningen (GDPR), det vil si en vurdering av hvorvidt Marker kommune har etablert rutiner og andre tiltak for å sikre at kravene etterleves og hvorvidt kommunen har gjennomført og dokumentert nødvendige vurderinger.

Revisjonslaget har i begrenset grad gjennomført stikkprøvekontroller og tester av om kommunen faktisk etterlever rutinene på personvernområdet. Revisjonslaget har heller ikke gjennomgått alle databehandleravtaler og personvernkonsekvensvurderinger kommunen har utført i detalj. Revisjonen har heller ikke utført en fullstendig kvalitetssikring av vurderingene som revisjonen har mottatt fra kommunen.

Revisjonen er basert på fremlagt dokumentasjon, og revisjonen forutsetter at denne informasjonen er fullstendig og korrekt. Vi gjør oppmerksom på at forvaltningsrevisjonen ikke kan erstatte kommunens egne kontrollaktiviteter som internrevisjon, stikkprøvekontroller og tester av at tiltak har ønsket effekt.

3.2 Om revisjonskriterier

I henhold til forskrift om kontrollutvalg og revisjon § 15 skal revisor fastsette revisjonskriterier for den enkelte forvaltningsrevisjon. Revisjonskriteriene er den objektive målestokk som setter revisor i stand til å gjøre vurderinger på de fleste områder uten å ha formell fagspesifikk kompetanse. Revisjonskriteriene og revisors kunnskap og erfaring innen forvaltningsrevisjonsmetodikk, gjør at revisor kan gjøre objektive og holdbare vurderinger.

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 vanligvis med basis i en eller flere følgende kilder: lovverk, politiske vedtak og føringer, kommunens egne retningslinjer, anerkjent teori på området, eller andre sammenlignbare virksomheters løsninger og resultater.

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. I denne forvaltningsrevisjonen har vi benyttet data fra ulike kilder, og brukt ulike metoder for innsamling av data, for å sikre et faktagrunnlag med 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
- Stikkprøver

Dokumentanalyse

Revisjonslaget har gjennomgått sentrale dokumenter på området, med hovedvekt på de deler som er relevante for revisjonskriteriene de skal belyse. Dokumentene er oversendt fra Marker kommune og hentet ut gjennom stikkprøver av kommunens kvalitets- og internkontrollsystem. Fullstendig oversikt over dokumentene fremgår av kildehenvisningene i kapittel 5.

Intervjuer

Det er totalt gjennomført totalt 10 intervjuer: Blant de intervjuede er det informanter fra sentrale stillinger generelt og rettet mot personvern, deriblant representanter fra virksomhetene «teknikk og samfunn», «beredskap og innbyggerdialog», «økonomi», «HR/organisasjon», «oppvekst», og «helse og velferd». Se fullstendig liste over informanter i kapittel 6.

Alle intervjuer er verifisert og gjennomgått av intervjuobjektene. Det betyr at den som er intervjuet, har fått lese gjennom referatet fra intervjuet for å bekrefte at referatet er i overenstemmelse med det som ble sagt under intervjuet, og rette opp eventuelle misforståelser.

Spørreundersøkelse

Det er gjennomført en spørreundersøkelse blant alle ansatte i Marker kommune. Undersøkelsen er gjennomført ved hjelp av BDOs nettbaserte spørreundersøkelsesverktøy, Feedback. Revisjonslaget mottok 95 svar på undersøkelsen av totalt 364 mottakere.

Spørreundersøkelsen besto av 9 ordinære spørsmål og 1 tilleggsspørsmål. Formålet med spørreundersøkelsen var å kartlegge personvernkulturen i kommunen. Undersøkelsen tok for seg temaer som opplæring, kjennskap til rutiner, kjennskap til avvikssystem og egen oppfatning av risikoområder innen personvern. Tilleggsspørsmålet var knyttet til ansatte som oppga å arbeide innenfor virksomhetsområdet oppvekst.

Stikkprøver

Ved avholdelse av enkelte intervjuer ble det gjennomført stikkprøver. Stikkprøver benyttes som metode for å verifisere fakta ved å vise til konkrete dokumenterte «bevis».

3.4 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.

Rød	Avdekkede forhold oppfyller ikke revisjonskriteriet. Det er avdekket vesentlige forbedringspotensial som bør gis høy prioritet.
Oransje	Avdekkede forhold oppfyller i liten grad revisjonskriteriet. Det er avdekket vesentlige forbedringspotensial.
Gul	Avdekkede forhold oppfyller i noen grad revisjonskriteriet. Det er avdekket forbedringspotensial.
Lysegrønn	Avdekkede forhold oppfyller i stor grad revisjonskriteriet. Det er imidlertid avdekket enkelte forbedringspotensial.
Grønn	Avdekkede forhold anses å være av uvesentlig betydning, og i praksis oppfylles dermed revisjonskriteriet.

Figur 1, Symbolbruk for vurdering av funn

4 PERSONVERN I MARKER KOMMUNE

Problemstilling: Har Marker kommune sikret at kommunen etterlever kravene i personopplysningsloven, herunder personvernforordningen (GDPR)?»

4.1 Revisjonskriterier

Revisjonskriteriene er basert på sentrale krav i personopplysningsloven[3] og EUs personvernforordning 2016/679 (heretter GDPR), med hovedvekt på sistnevntes kapittel II til V. Kravene i GDPR er i stor grad generelt utformet. Revisjonen har derfor sett hen til Datatilsynets veiledere som utdyper hvordan kravene skal tolkes. Krav til behandling av personopplysninger i spesiallovgivning, herunder for områder som arbeidsmiljø, helse, arkiv, samt plan og bygg, faller utenfor revisjonens område.

Plikten til å etablere Internkontrollsystem for personvern

Kravet om å utarbeide et Internkontrollsystem for personvern følger av GDPR artikkel 24 nr. 1, hvor det fremgår at behandlingsansvarlig skal sikre at alle aktuelle plikter etter GDPR etterleves gjennom tekniske og organisatoriske tiltak, og at etterlevelsen kan dokumenteres. GDPR stiller ikke eksplisitte krav til hvordan Internkontrollsystemet 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 (Internkontrollsystem) hvor det er presisert at Internkontrollsystem:
«[…] 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»[4].

Ledelsen er ansvarlig for å sikre etterlevelse av GDPR. Ledelsen må derfor implementere personvern i virksomhetsstyringen, og sikre at det er tilstrekkelig med ressurser, verktøy og kompetanse for å sikre etterlevelse.

Datatilsynet definerer at Internkontrollsystemet bør bestå av styrende elementer, gjennomførende elementer og kontrollerende elementer som er proporsjonale med behandlingen virksomheten utfører.[5] 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 Internkontrollsystemet deretter. Det bør være en sammenheng mellom omfanget av gjennomførende og kontrollerende elementer, og risikoen for de registrertes rettigheter og friheter ved behandlingen. Risiko for virksomhetens verdier skal ikke vektlegges.[6]

Ledelsen må sikre at Internkontrollsystemet gir et korrekt bilde av de faktiske aktivitetene og organiseringen av personvernarbeidet i virksomheten. Dette innebærer at Internkontrollsystemet må gjennomgås og oppdateres jevnlig. De styrende elementene 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 systemer og prosesser som innebærer behandling av personopplysninger. Tonen fra ledelsen vil ha stor betydning i den gjennomførende prosessen. Det er en

[3] Lov av 15. juni 2018 nr. 38 om Lov om behandling av personopplysninger
[4] Datatilsynet veileder "Etablere internkontroll" punkt 1
[5] Datatilsynet veileder "Etablere internkontroll" punkt 1
[6] Datatilsynet veileder "Etablere internkontroll" punkt 2

forutsetning for å lykkes med etterlevelsen at ledelsen er proaktive når det gjelder å bygge en personvernkultur i virksomheten. De kontrollerende elementene 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 Internkontrollsystemet.

Kravet til kartlegging av behandlingsaktiviteter

Behandlingens art, omfang, formål og sammenhengen den utføres i får betydning for hvilke tekniske og organisatoriske tiltak den behandlingsansvarlige skal iverksette etter GDPR artikkel 24 nr. 1 og artikkel 32 nr.1. Det er derfor nødvendig å kartlegge virksomhetens behandlingsaktiviteter. Kartleggingen dokumenteres normalt i protokollen over behandlingsaktiviteter, som virksomheten er pliktig å utarbeide etter GDPR artikkel 30.

Krav til protokollens innhold fremgår av GDPR artikkel 30 nr.1. Etter bestemmelsen skal det fremgå hvem den behandlingsansvarlige er og hvordan vedkommende kan kontaktes, hvilke behandlingsaktiviteter den behandlingsansvarlige er ansvarlig for, behandlingenes formål, hvilke kategorier av personopplysninger og registrerte som omfattes av behandlingen, eventuelle mottakere av personopplysningene og hvorvidt personopplysningene overføres til tredjestater eller internasjonale organisasjoner. Dersom det er mulig skal det også fremgå slettefrister eller slettekriterier for de forskjellige kategoriene av personopplysninger, og overordnede tekniske og organisatoriske tiltak som den behandlingsansvarlige har iverksatt for behandlingen.

Protokollen er et sentralt verktøy i arbeidet med etterlevelse av personvernlovgivningen, innholdet danner grunnlaget for en rekke nødvendige vurderinger, herunder risikovurderinger.

Krav til rettslig grunnlag for behandling av personopplysninger

Lovlighet ved behandling av personopplysninger reguleres i flere bestemmelser i GDPR. For at behandling av personopplysninger skal være lovlig følger det for eksempel av GDPR artikkel 6 at behandlingen må ha et rettslig grunnlag.

Det er i utgangspunktet ulovlig å behandle særlige kategorier av personopplysninger. Dette er personopplysninger om «*rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering*». For å behandle denne typen personopplysninger må tilleggskravene i GDPR artikkel 9 være oppfylt. Det følger av personopplysningsloven §§ 6,7 og 9 at slik behandling er lovlig i spesifikke tilfeller.

Etter GDPR artikkel 10 følger det at opplysninger om straffedommer eller lovovertredelser kun kan behandles under kontroll av offentlige myndigheter eller der det er fastsatt i lov. Når denne typen personopplysninger behandles uten offentlig myndighets kontroll, følger det av personopplysningsloven § 11 at det gjelder samme krav som nevnt i artikkel 9 (2) (a) og (c) til (f) samt §§ 6, 7 og 9. Det stilles også særskilte krav til når fødselsnummer kan behandles, i personopplysningsloven § 12.

Det følger av ansvarlighetsprinsippet i artikkel 5 (2) at behandlingsgrunnlag må dokumenteres.

Krav til sletting av personopplysninger

Det er ulovlig å oppbevare personopplysninger når de ikke lenger tjener til å oppfylle formålet de ble samlet inn for. Dette innebærer at virksomheten må slette opplysninger når formålet er oppfylt, uav-

hengig av om den registrerte har bedt om det eller ikke. Når den registrerte ber om å få sine personopplysninger slettet, må den behandlingsansvarlige slette disse «uten ugrunnet opphold», med mindre det foreligger forhold som angitt i GDPR artikkel 17 (1) (a) til (f). Sletting må også gjennomføres når det ikke lenger foreligger gyldig behandlingsgrunnlag, som for eksempel samtykke.

For at sletting skal bli gjennomført, må virksomheten ha systemer og rutiner som sikrer dette.

Krav til å informere de registrerte om behandling av deres personopplysninger og krav til behandling av innsynsforespørsler

Det er krav om at de registrerte skal få informasjon om hvordan deres personopplysninger behandles. Det er ingen spesifikke krav knyttet til hvordan virksomheten skal gi informasjon til de registrerte, men den bør gis skriftlig med et enkelt og forståelig språk.

Det følger av GDPR artikkel 13 og 14 at det er ulike krav til hva slags informasjon som skal gis avhengig av om opplysningene hentes inn fra den registrerte selv eller en tredjepart. I alle tilfeller må det gis informasjon om virksomhetens og personvernombudets kontaktinformasjon, formålet med behandlingen, behandlingsgrunnlag, lagringsperiode og kriterier for denne, navn på mottakere av opplysningene og om de skal overføres til et land utenfor EU/EØS, vurderingene som ligger til grunn for overføringer til land utenfor EU/EØS, den registrertes rettigheter, retten til å trekke tilbake samtykke, retten til å klage til Datatilsynet, om det er frivillig eller påkrevet å oppgi personopplysninger og eventuelle konsekvenser av å ikke oppgi dem, forekomstens av automatiserte individuelle avgjørelser, eventuelle nye formål, og konsekvensene av behandlingen .[7]

Dersom den registrerte ber om å få innsyn i behandlingen av sine personopplysninger, så er behandlingsansvarlig forpliktet til å gi innsyn i personopplysningene. Det skal også gis informasjon om visse aspekter ved behandlingen av personopplysninger.

Når den registrerte ber om å få håndhevet sine rettigheter, har den behandlingsansvarlige plikt til å legge til rette for å vurdere, uføre og gi tilbakemeldinger uten ugrunnet opphold og senest innen en måned. I GDPR artikkel 12 stilles det formkrav til eventuelle avslag.

Kravet til informasjonssikkerhet ved behandling av personopplysninger

Internkontrollsystemet skal dekke alle aktuelle plikter etter GDPR, herunder kravet til informasjonssikkerhet i GDPR artikkel 32. Det følger av GDPR artikkel 32 nr. 1 at: «Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen»

Kravene til etablering av tekniske og organisatoriske tiltak i artikkel 32 nr. 1 må ses i sammenheng med kravene i GDPR artikkel 24. Begge bestemmelsene tar utgangspunkt i hva slags behandlinger som utføres og risikoen den medfører, og tiltakene som er påkrevd etter hver av bestemmelsene er overlappende. Et Internkontrollsystem for informasjonssikkerhet omfatter også informasjonssikkerhet knyttet til personvern, og vil kunne bidra til etterlevelse av både artikkel 24 og artikkel 32.

[7] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/gi-informasjon/informasjon-og-apenhet/hva-skal-virksomheten-gi-informasjon-om/

Kravet til inngåelse av databehandleravtaler

Dersom en tredjepart behandler personopplysninger på vegne av den behandlingsansvarlige, stiller GDPR artikkel 28 krav om inngåelse av databehandleravtale. Formålet med avtalen er å sørge for at databehandleren behandler opplysninger etter instruks fra den behandlingsansvarlige. Avtalen må derfor konkret beskrive hvordan behandlingen skal skje, behandlingens art, hva som er formålet med behandlingen, hvor lenge avtalen skal vare, hva slags personopplysninger som er registrert og hvilke kategorier av personer personopplysningene gjelder.[8]

Databehandleravtalen fungerer som et instrument som avklarer roller og ansvar, og er en viktig forutsetning for at GDPR etterleves og at de registrertes rettigheter ivaretas.[9] Personvern er et dynamisk rettsområde og GDPR er et regelverk som stadig presiseres og utvikles, for eksempel via praksis fra EU-domstolen, Datatilsynet og Personvernnemda. Den behandlingsansvarlige virksomheten bør derfor jevnlig gjennomføre kontroller av databehandleravtalene sine for å forsikre seg om at de ivaretar kravene etter GDPR, og eventuelt reviderer avtalene dersom dette ikke er tilfellet. Det er også slik at behandlingsansvarlig kun skal engasjere databehandlere som stiller tilstrekkelige garantier. Behandlingsansvarlig bør derfor kontrollere at databehandleravtalene etterleves.

Krav ved overføring av personopplysninger til land utenfor EU/EØS

Ved overføring av personopplysninger ut av EØS, må det foreligge et gyldig overføringsgrunnlag etter GDPR kapittel V for at overføringen skal være lovlig. Virksomheten må i henhold til EU-domstolens Schrems II-avgjørelse (Case C-311/18) og tilhørende veiledning fra Datatilsynet også selv vurdere om beskyttelsesnivået i landet personopplysningene overføres til er tilsvarende som i EØS, ved bruk av de vanligste overføringsgrunnlagene. Dersom virksomheten mener at beskyttelsesnivået er utilstrekkelig, så må den implementere kompenserende tiltak i disse tilfellene. Lykkes ikke virksomheten i å identifisere og implementere slike tiltak, så vil overføringen regnes som ulovlig.[10]

Kravet til gjennomføring av risikovurderinger

Den behandlingsansvarlige er indirekte pålagt å gjennomføre risikovurderinger av egne behandlingsaktiviteter. Dette følger ikke direkte av ordlyden i GDPR artikkel 24 eller 32, men kan utledes av kravet til å sørge for tilfredsstillende informasjonssikkerhet etter GDPR artikkel 32. I veileder for etablering av internkontroll uttrykker Datatilsynet at det er nødvendig for å oppfylle kravene i bestemmelsene. De tekniske og organisatoriske tiltakene som bestemmelsene pålegger virksomhetene å etablere, skal baseres på resultatet av risikovurderingene.

Krav til personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39

GDPR artikkel 37 krever at enhver offentlig myndighet og ethvert offentlig organ skal utnevne et personvernombud. Forarbeidene til personopplysningsloven angir at dette gjelder for samme organer som er omfattet av forvaltningsloven § 1.

Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner og kunnskap om personvernregelverket, i tillegg til evnen til å kunne utføre oppgavene som tilligger personvernombudet etter GDPR i artikkel 39.

[8] Datatilsynets veileder " Hvordan lage en databehandleravtale?"
[9] Åste Marie Bergseng Skullerud mfl., *Personvernforordningen. Lovkommentar*, Artikkel 28. Databehandler, Juridika (kopiert 24. januar 2023)
[10] Datatilsynets veileder "Overføring av personopplysninger ut av EØS"

Det stilles krav om at personvernombudet skal involveres i «alle spørsmål som gjelder vern av personopplysninger». Det bør etableres klare rutiner for når og hvordan ombudet skal involveres[11], og det skal settes av nok ressurser til at ombudet får utført sine oppgaver.

Det følger av artikkel 38 (3) at personvernombudet skal være uavhengig og ikke kan instrueres, avsettes eller straffes for utførelsen av sine oppgaver. Videre skal personvernombudet rapportere direkte til øverste administrative ledelse i virksomheten. Dette skal sikre at ansvaret for etterlevelsen av forordningen er plassert riktig.

Personvernombudet skal også gi råd og informasjon til virksomhetens ledelse og de ansatte om forpliktelsene de har etter GDPR og annen relevant lovgivning om behandling av personopplysninger. I utførelsen av oppgavene skal personvernombudet ha en risikobasert tilnærming.

Personvernombudet skal være virksomhetens kontaktpunkt for tilsynsmyndighetene.

Kravene til avvikshåndtering i GDPR artikkel 33 og 34

GDPR artikkel 33 og 34 beskriver hvordan den behandlingsansvarlige skal håndtere personvernavvik.

Etter artikkel 33 nr. 5 skal den behandlingsansvarlige «*dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det*».

Videre må den behandlingsansvarlige etter artikkel 33 nr. 1 «*senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet … med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter*».

Det følger også av artikkel 34 nr. 1 at «*Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet*».

Dette innebærer at den behandlingsansvarlige må sikre at personvernavvik avdekkes, dokumenteres og håndteres i samsvar med kravene og tidsfristene i bestemmelsene.

Oppsummering av revisjonskriterier

Revisjonskriteriene er punktvis oppsummert nedenfor.

Kommunen skal:

- Ha etablert en tilfredsstillende interkontroll for personvern, dette innebærer at kommunen skal ha
    - Beskrevet overordnede rammer for personvernarbeidet i styrende dokumenter
    - Gjennomført en risikovurdering for å identifisere behov for tekniske og organisatoriske tiltak
    - Etablert tilfredsstillende rutiner og retningslinjer for håndtering av personopplysninger basert på en risikovurdering og sørget for å kommunisere disse ut i organisasjonen
    - Sørget for at ansvar og roller innen personvern er kommunisert og forstått
    - Sørget for regelmessig og rollebasert opplæring innen personvern

[11] Åste Marie Bergseng Skullerud mfl., *Personvernforordningen. Lovkommentar*, Artikkel 38. Personvernombudets stilling, Juridika (kopiert 25. januar 2023)

    - Sørget for regelmessig evaluering og forbedring av internkontrollen.
- Ha en oppdatert protokoll over behandlingsaktiviteter som tilfredsstiller kravene i GDPR artikkel 30
- Ha sørget for at rettslig grunnlag for behandling av personopplysninger blir vurdert og dokumentert
- Ha etablert sletterutiner for sin behandling av personopplysninger
- Ha sørget for å informere de registrerte om behandlingen av deres personopplysninger
- Ha etablert rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter
- Ha etablert egnede tiltak for å ivareta personopplysningssikkerheten
- Ha sørget for å gjennomføre personvernkonsekvensvurderinger når det er nødvendig
- Ha sørget for at databehandlere ivaretar krav til personvern og sikre at det inngås databehandler-avtaler
- Ha kartlagt overføringer av personopplysninger til land utenfor EU/EØS og ha gjennomført nødvendige vurderinger og tiltak ved overføringer
- Ha utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39
- Ha sørget for at avvik knyttet til personvern blir meldt, registrert og håndtert.

4.2 Datagrunnlag

4.2.1 Kommunen skal ha etablert en tilfredsstillende internkontroll for personvern

4.2.1.1 Kommunen skal ha beskrevet overordnede rammer for personvernarbeidet i styrende dokumenter

Marker kommune har utarbeidet dokumentet *Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)*. Det fremgår av dokumentet at:

> *«Denne reviderte Sikkerhetshåndboken fastlegger kommunens krav til beskyttelse av personopplysninger og øvrige opplysninger som samles inn, lagres, bearbeides, overføres og formidles så vel manuelt som elektronisk.*
>
> *(…)*
>
> *Håndboken utgjør et felles rammeverk for det praktiske arbeidet med informasjonssikkerhet og personvern i kommunen, og skal benyttes (…) for å etterleve kravene til informasjonssikkerhet og personvern i Personopplysningsloven, som også inkluderer EU's/EØS' Forordning om personvern, GDPR (General Data Protection Regulation), Helseregisterloven inkl Normen for informasjonssikkerhet, Helse-informasjonssikkerhetsforskriften, Lov om Barnevern, Opplæringsloven og annet relevant lovverk og sikkerhetsprinsippene i ISO 27001-standarden».*

Det fremgår av dokumentet *Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)* at sikkerhetshåndboken, sammen med vedlegg og kommunens øvrige rutiner, omfatter de grunnleggende prinsippene og rutinene knyttet til informasjonssikkerhet og personvern i kommunen. Dette inkluderer styrende, gjennomførende og kontrollerende elementer. Kommunen har imidlertid ikke fremlagt for revisjonslaget en samlet oversikt over hvilke rutiner og retningslinjer for håndtering av personopplysninger som inngår i kommunens internkontrollsystem for personvern, herunder styrende, gjennomførende og kontrollerende elementer. Videre har kommunen ikke fremlagt beskrivelser av hvordan de ulike delene av internkontrollsystemet for personvern henger sammen. I intervju fremkom det at kommunen, som følge av manglende helhetlig virksomhetsstyring, har ulik praksis for dette på tvers av virksomhetsområdene.

Det fremgår av intervju at Marker kommune har utarbeidet flere styrende dokumenter som inngår i internkontrollen for personvern, inkludert:

- Sikkerhet, datasikkerhet og personvern i Marker kommune
- Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)
- Informasjons- og kommunikasjonsstrategi – Rådmannens forslag
- Etiske retningslinjer for ledere, medarbeidere og folkevalgte i Marker kommune
- Mål for personvernarbeidet i Marker kommune

4.2.1.2 Kommunen skal ha gjennomført en risikovurdering for å identifisere behov for tekniske og organisatoriske tiltak

Det fremgår av dokumentet *Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)* at omfanget av kommunens gjennomførende og kontrollerende rutiner må vurderes i sammenheng med risikoen for de registrertes rettigheter ved behandling av personopplysninger.

Marker kommune har fremlagt dokumentene *ROS-analyse-ASPIT, ROS-analyse-barnehage, ROS-analyse-barneverk, ROS-analyse-digisos, ROS-analyse-felles tennant med skole, ROS-analyse-hjemmekontor, ROS-analyse-IKT, ROS-analyse-legekontor, ROS-analyse-MBSS, ROS-analyse-*

Økonomikontoret, ROS-analyse-skytjenester og *ROS-analyse, vidkas.* Dokumentene inneholder tolv eksempler på gjennomførte risiko- og sårbarhetsvurderinger (ROS) av ulike løsninger, enheter og prosesser i kommunen.

Det fremgår av *ROS-analyse-skytjenester* og *ROS-analyse-IKT* at enkelte personvernrelaterte risikoer er identifisert og vurdert, herunder risikoen for at personopplysninger kommer på avveie. Risikovurderingene inneholder også beskrivelser av eksisterende og forslag til nye risikoreduserende tiltak, som for eksempel rutiner, opplæring og bevisstgjøring, kryptering og back-up.

4.2.1.3 Kommunen skal ha etablert tilfredsstillende rutiner og retningslinjer for håndtering av personopplysninger basert på en risikovurdering og sørget for å kommunisere disse ut i organisasjonen

Marker kommune har fremlagt dokumentet *Sikkerhet, datasikkerhet og personvern i Marker.* I dokumentet fremgår det at internkontrollen representerer Marker kommunes Internkontrollsystem/kvalitetssystem for å sikre at lover, forskrifter og forordninger (GDPR) etterleves, og at tiltak knyttet til kommunens internkontroll skal forbedres, dokumenteres og oppdateres ved behov.

Det opplyses gjennom intervju at virksomhetens rutiner og retningslinjer for personvern er samlet i fagsystemet Samsvar og internkontrollsystemet TQM (Total Quality Management). Revisjonslaget ble opplyst om at behandlingsprotokoller er dokumentert i Samsvar, mens TQM brukes til dokumentering av rutiner og retningslinjer, håndtering av avvik, risikokartlegging og aktivitetsplanlegging. Videre ble det gjennom intervju opplyst at flere informanter opplever det som vanskelig med å navigere i TQM. Systemet er imidlertid i en ombyggingsfase som følge av pågående organisasjonsendringer. Revisjonslaget ble opplyst om at det kun er enkelte virksomhetsområder som har utarbeidet egne rutiner om personvern.

Det fremgår av *Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)* at den enkelte virksomhetsleder har et selvstendig arbeid for gjennomføring av sikringstiltak og oppfølging knyttet til kommunens arbeid med informasjonssikkerhet og personvern, inkludert etablering av nødvendige rutiner. Som beskrevet i kapittel 4.2.1.2, fremgår det av enkelte personvernrelaterte risikovurderinger inneholder beskrivelser av eksisterende og forslag til nye risikoreduserende tiltak, som for eksempel rutiner. Kommunen har ikke fremlagt nærmere dokumentasjon på at virksomhetenes gjennomførende og kontrollerende rutiner er basert på en risikovurdering, eller hvilke ytterligere rutiner kommunen bør etablere for å møte kommunens risikoer.

Revisjonslaget har gjennom samtaler med kommunen gjennomført stikkprøver på hva som ligger dokumentert i TQM. Kommunen har også fremlagt relevante rutiner for håndtering av personopplysninger som ligger dokumentert i systemet, herunder:

- Sikkerhet, datasikkerhet og personvern i Marker kommune
- Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)
- Brudd på personopplysningssikkerheten Marker kommune
- Etiske retningslinjer for ledere, medarbeidere og folkevalgte i Marker kommune
- Informasjon om kommunikasjonsstrategi
- Innsamling og bruk av personopplysninger, Marker kommune
- Innsynsrett Marker kommune
- Mål for personvernarbeidet i Marker kommune
- Personvern på arbeidsplassen
- Samtykkeerklæring foto og film

- Samtykkeskjema fotografering
- Samtykkeskjema tverrfaglig samarbeid
- Samtykkeskjema fotografering/filming av elevene

Marker kommune har utarbeidet et årshjul for arbeidet med samfunnssikkerhet og beredskap. Årshjulet fremgår av dokumentet *Mål for personvernarbeidet i Marker kommune,* og inneholder dokumenterte aktiviteter knyttet til personvern, herunder:

Tidspunkt/Frekvens	Aktivitet	Ansvarlig	Kommentar
Årlig/januar	Gjennomgang av personvernerklæring og sikkerhetshåndbok.	Personvernombud	I samarbeid med ledelse
Februar	Opplæring av nyansatte.	HR	
April	Workshop for ledere og årlig oppfrisknings-kurs for eksisterende ansatte.	BOI	Gjennomføres av virksomhet Beredskap og innbyggerdialog i samarbeid med personvernombud
August	Risikovurdering og eventuell oppdatering av personvernstrategier i den enkelte virksomhet.	Ledergruppen	
September	Fagdag med ekstern innleder.	Kommunedirektør	Tema avklares i ledergruppen
November	Revisjon av personvernpraksis.	Kommunedirektør	Ledergruppen

Revisjonslaget har ikke mottatt informasjon om hvordan årshjulet følges opp i praksis, eller kontrollerende dokumentasjon som bekrefter at årshjulet faktisk blir etterlevd i praksis.

Marker kommune har ikke fremlagt dokumentasjon på hvordan kommunens rutiner og retningslinjer for håndtering av personopplysninger kommuniseres ut i organisasjonen. Det fremkom av spørreundersøkelsen at 65,6 % av de ansatte oppgir at de er kjent med hvor de finner kommunens retningslinjer og rutiner for personvern, mens 34,4 % svarte at de ikke er kjent med dette. Videre ble de ansatte spurt om i hvilken grad de er kjent med hvilke retningslinjer for personvern som gjelder for dem. Her svarte 7,4 % «i svært stor grad», 42,1 % «i stor grad», 41,1 % «verken eller», 23,25 % «i liten grad» og 5,3 % «i svært liten grad».

Når det gjelder spørsmålet om hvorvidt de ansatte opplever at deres respektive avdelinger etterlever retningslinjene knyttet til personvern, svarte 21,9 % «i svært stor grad», 42,7 % «i stor grad», 19,8 % «verken eller», 6,3 % «i liten grad» og 2,1 % «i svært liten grad», mens 7,3 % oppga at de ikke visste.

4.2.1.4 Kommunen skal ha sørget for at ansvar og roller innen personvern er kommunisert og forstått

Dokumentet *Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)* inneholder beskrivelser av den nærmere organiseringen av informasjonssikkerhet og personvern i kommunen, herunder:

Rolle	Ansvar
Kommunedirektør	Overordnet ansvar (behandlingsansvar) for informasjonssikkerhet og personvern i kommunen
Kommunalsjef	Overordnet operativt ansvar for å videreutvikle og overvåke arbeidet med informasjonssikkerhet og personvern i kommunen.
Den enkelte virksomhetsleder	Selvstendig ansvar for gjennomføring av sikringstiltak og oppfølging knyttet til kommunens arbeid med disse områdene. Ansvarlig for at relevant innhold i sikkerhetshåndboken formidles til sine medarbeidere.
IT-sjef	Ansvar for teknisk informasjonssikkerhet

Gjennom intervjuene ble det påpekt at både IT-ansvarlig og arkivansvarlig spiller sentrale roller i personvernarbeidet, hvor IT-ansvarlig fungerer som personvernombudets høyre hånd.

Det fremkom i intervju at ansvaret for personvern i kommunen er noe spredt, og at enkelte informanter opplever uklarhet om hvem som faktisk har ansvaret for personvern i kommunen. Det ble videre påpekt at nyansatte ofte mangler tydelige retningslinjer for hva de skal forholde seg til. Et eksempel på dette ble trukket frem i forbindelse med tilgangssystemet Visma, hvor en informant fortalte at vedkommendes tilgang ikke ble fjernet etter en rolle-/stillingsendring. Dette førte til at personen selv tok initiativ til å rydde opp i tilgangene i TQM og måtte følge opp dette i dialog med virksomhetslederne.

4.2.1.5 Kommunen skal ha sørget for regelmessig og rollebasert opplæring innen personvern

Marker kommune har utarbeidet dokumentet *Mål for personvernarbeidet i Marker kommune*. Dokumentet inneholder en beskrivelse av kommunens opplæringstiltak i personvernarbeidet, herunder:

- *«Utvikle et opplæringsprogram som dekker grunnleggende personvernprinsipper og kommunens retningslinjer.*
    - *Grunnleggende prinsipper i GDPR*
    - *Behandlingsgrunnlag*
    - *Dataminimering*
    - *Registrertes rettigheter*
    - *Sikkerhetstiltak*
    - *Meldeplikt til Datatilsynet*
- *Tilby spesialiserte opplæringsmoduler for ansatte som håndterer sensitive personopplysninger.*
- *Invitere eksterne eksperter til å holde foredrag om aktuelle temaer innen personvern.»*

Marker kommune har ikke fremlagt ytterligere dokumentasjon på innholdet i opplæringsprogrammet. Revisjonslaget ble i intervju opplyst om at personvernombudet holder jevnlig opplæring med ledergruppen når ombudet er til stede. Revisjonslaget har ikke mottatt dokumentasjon på innholdet i disse opplæringene.

Videre ble det opplyst at det per i dag ikke finnes en systematisk og formalisert opplæringsplan, men at det er foreslått å etablere en felles plan for personvern og sikkerhet. Det ble opplyst at det har vært én sesjon der de ansatte har fått en grunnleggende innføring i sikkerhet og hvordan systemene er sikret. Videre at ansatte ble oppfordret til å lese sikkerhetshåndboken som distribueres med lesekontroll. Revisjonslaget er informert om at personvernombudet gjennomfører opplæring med ledergruppen når vedkommende er til stede.

Intervjuobjektene opplyste at det er igangsatt en prosess for å sikre opplæring ved onboarding av nyansatte, og at det vurderes å etablere et eget personvernteam i kommunen. Det ble påpekt at det er utarbeidet en egen onboardings-mappe for nyansatte, som blant annet inneholder krav om taushetsplikt og innhenting av politiattest.

Det fremkom av spørreundersøkelsen at 77,1 % av de ansatte ikke har deltatt på organisert opplæring innen personvern, som for eksempel e-læring eller foredrag, mens 14,6 % svarte at de har deltatt flere ganger, og 8,3 % svarte at de har deltatt som nyansatt. Videre svarte 13,5 % at personvern jevnlig har vært tema på fellesmøter, samlinger eller liknende i avdelingen eller virksomheten, mens 42,7 % oppga at dette har vært et tema noen få ganger. 30,2 % svarte at personvern ikke har vært diskutert i slike fora, og 13,5 % oppga at de ikke visste om det har vært et tema.

4.2.1.6 Kommunen skal ha sørget for regelmessig evaluering og forbedring av internkontrollen

Det fremgår av dokumentet *Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)* at kommunens ledelse årlig skal initiere egenkontroller for å sikre at rutiner for håndtering av personopplysninger er implementert og fungerer som tiltenkt i alle tjenester. Videre er det spesifisert at sikkerhetsansvarlig har ansvaret for å følge opp gjennomføringen av disse kontrollene, for å sikre at eventuelle avvik avdekkes og nødvendige tiltak iverksettes for å opprettholde og styrke personvernarbeidet.

Revisjonslaget har ikke fått tilsendt dokumentasjon som konkretisere disse rutinene for egenkontroll. Kommunen har ikke fremlagt dokumenterte rutiner for annen regelmessig evaluering og forbedring av internkontrollen.

Marker kommune har fremlagt dokumentet *Marker kommune Rapport fra sikkerhetsvurdering februar 2024.* Det ble opplyst i intervju at personvernombudet hadde gjennomført sikkerhetsvurderingen. Det fremgår av dokumentet at formålet med sikkerhetsvurderingen var:

- *«å kontrollere at eksisterende lover og regler i forhold til informasjonssikkerhet og personvern etterleves i alle ledd i kommunen, herunder Personopplysningsloven (POL) fra 20. juli 2018 inklusive EU-/ EØS-forordningen om personvern GDPR (General Data Protection Regulation). GDPR erstatter de tidligere forskriftene til POL*
- *å sikre at etablerte rutiner knyttet til fysiske, organisatoriske og IT-/systemtekniske forhold inkl personvern benyttes og fungerer etter hensikten*
- *å vurdere om sikringstiltakene er tilstrekkelige – og foreslå relevante endringer det dette blir ansett som viktig/nødvendig»*

Denne sikkerhetsvurderingen inneholder beskrivelser av vurderinger, anbefalinger og tiltak for å styrke kommunens personvern- og sikkerhetsarbeid. Personvernombudet trekker særlig frem viktigheten av å gi opplæring til kommunens ledere og ansatte, at personvernerklæringen skal være lett tilgjengelig på kommunens nettside sammen med kontaktinformasjon til personvernombudet, samt betydningen av å vedlikeholde en oppdatert sikkerhetshåndbok. Personvernombudet trekker også frem behovet for sikker håndtering av skyggearkiv, og det anbefales at kommunedirektøren og andre ledere regelmessig setter av tid til uanmeldte besøk på kommunens ulike tjenestesteder og avdelinger.

Det ble opplyst i intervju at personvernombudet er til stede i kommunen 2-3 ganger i året for å gjennomføre intervjuer. Intervjuobjektene opplyste om at omsorgssektoren, spesielt under tidligere leder, har gjennomført et betydelig arbeid knyttet til personvern og internkontroll. Dette omfatter i stor grad bruk av kommunens internkontrollsystem, TQM.

4.2.2 Kommunen skal ha en oppdatert protokoll over behandlingsaktiviteter som tilfredsstiller kravene i GDPR artikkel 30

Marker kommune har fremlagt en protokoll over behandlingsaktiviteter (heretter behandlingsprotokoll/behandlingsprotokollen), som er opprettet og registrert i systemet Samsvar. Revisjonslaget har selv hentet ut en detaljert oversikt over protokollen, gjennom å ha blitt gitt tilgang til systemet av kommunen. Ifølge denne oversikten gir behandlingsprotokollen en oversikt over følgende områder:

- *«Behandlingsaktivitet*
- *Avdeling*
- *Område*
- *Internt ansvarlig*
- *Behandlingsansvarlig*
- *Personvernombud*
- *Kontaktperson for myndighetene*
- *Intern eller ekstern*
- *Opprettet*
- *Sist oppdatert*
- *Formålet med behandlingen / systemet*
- *Personopplysninger som registreres*
- *Sensitive personopplysninger som registreres*
- *Kategorier av registrerte*
- *Systemer som benyttes i behandlingen*
- *Innsamling av personopplysningene*
- *Behandlingsgrunnlag*
- *Hvis Lovhjemmel (Behandlingsgrunnlag)*
- *Viderebehandling av opplysningene*
- *Interne brukere av personopplysninger*
- *Interne brukere av sensitive personopplysninger*
- *Mottakere av personopplysninger*
- *Mottakere av sensitive personopplysninger*
- *Overføring til tredjeland*
- *Sletting og lagring*
- *Datalagring (hvor lagres opplysningene)*
- *Automatiske avgjørelser*
- *Vurdering av personvernkonsekvenser*
- *Vurdering av tekniske tiltak*
- *Vurdering av organisatoriske tiltak»*

I forbindelse med dokumentgjennomgangen har revisjonslaget gjennomført stikkprøver av enkelte lovpålagte områder som kommunen er forpliktet til å beskrive i behandlingsprotokollen. Det fremgår av stikkprøvene at under området «Mottakere av personopplysninger» er det for mange behandlingsaktiviteter angitt at «Personopplysninger overføres ikke til tredjeland». Videre fremgår det av stikkprøvene at under området «Sletting og lagring» er det for mange behandlingsaktiviteter oppgitt at «Det foretas ingen automatiske avgjørelser i behandlingen».

Videre har kommunen fremlagt dokumentet *Oversikt over behandling av personopplysninger i Marker kommune* fra oktober 2019*.* Dokumentet er offentlig tilgjengelig på kommunens hjemmeside og som en del av *Arkivplan for Marker kommune.* Dette dokumentet gir en oversikt over områdene:

- Behandling
- Hjemmel
- Datasystem
- Systemansvarlig
- Manuelle registreringer
- Innhold/formål med behandlingen
- Brukere
- Datasikkerhet og hvordan den ivaretas

Kommunen har videre fremlagt dokumentet *Protokoll_08_08-2024_09-36-23.* Dokumentet inneholder en oversikt over behandling av personopplysninger i Marker kommune, og inneholder 47 behandlingsaktiviteter. Kommunen har ikke fremlagt dokumentasjon som beskriver hvordan disse behandlingsprotokollene henger sammen.

Det følger av dokumentet *Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)* at IT-sjefen har det overordnede ansvaret for at behandlingsprotokollene er oppdaterte. I intervju opplyste enkelte av informantene at IT-sjefen var ansvarlig for behandlingsprotokollene, mens andre mente at ansvaret for behandlingsprotokollene lå hos de respektive virksomhetene. Kommunen har ikke fremlagt dokumentasjon som underbygger ansvarsfordelingen.

Flere av informantene revisjonslaget har snakket med var ikke kjent med at det foreligger en behandlingsprotokoll, eller hvordan arbeidet med protokollen ble fulgt opp i praksis.

4.2.3 Kommunen skal ha sørget for at rettslig grunnlag for behandling av personopplysninger blir vurdert og dokumentert

Det fremgår av intervju at Marker kommune benytter protokollen til å dokumentere rettslig grunnlag for behandlingen av personopplysninger (behandlingsgrunnlag). Marker kommunes behandlingsprotokoll inneholder egne kolonner for å angi lovlig behandlingsgrunnlag for sin behandling av personopplysninger. Det fremgår av behandlingsprotokollen at behandlingsgrunnlag er dokumentert under kolonnene «Innsamling av personopplysninger», «Behandlingsgrunnlag» og «Hvis Lovhjemmel (Behandlingsgrunnlag)»

Det fremgår av behandlingsprotokollen kommunen behandler personopplysninger basert på følgende behandlingsgrunnlag:

- GDPR artikkel 6 nr. 1 bokstav a): Den registrerte har samtykket til behandlingen
- GDPR artikkel 6 nr. 1 bokstav b): Nødvendig for å oppfylle en avtale den registrerte er part i
- GDPR artikkel 6 nr. 1 bokstav c): Nødvendig for å oppfylle rettslige forpliktelser
- GDPR artikkel 6 nr. 1 bokstav e): Nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet
- GDPR artikkel 6 nr. 1 bokstav f): Nødvendig for å ivareta en berettiget interesse
- GDPR artikkel 9 nr. 1 bokstav b): Nødvendig for at den registrerte skal kunne oppfylle sine forpliktelser og utøve sine rettigheter på området arbeidsrett, trygderett og sosialrett

For de tilfellene Marker kommune har basert seg på GDPR artikkel 6 nr. 1 bokstav c) eller e) fremgår det av behandlingsprotokollen at kommunen har dokumentert supplerende rettsgrunnlag. Under følger et utvalg av disse supplerende rettsgrunnlagene:

- opplæringsloven

- forvaltningsloven
- offentlighetsloven
- arbeidsmiljøloven
- brannvernloven
- helseregisterloven
- pasientjournalloven
- kulturloven
- kommuneloven
- arkivloven
- straffeloven
- plan- og bygningsloven
- ekteskapsloven
- valgloven.

Det fremgår av behandlingsprotokollen at Marker kommune har basert seg på GDPR artikkel 6 nr. 1 bokstav f) for behandlingsaktivitetene «Overvåkning av ansattes mobiltelefon (bruk av mobile device management)» og «Kameraovervåkning». Revisjonslaget har ikke mottatt kommunens dokumenterte berettigede interesseavveininger, slik som kreves etter GDPR artikkel 6 nr. 1 bokstav f).

Marker kommune har ikke fremlagt dokumenterte rutiner for vurdering av behandlingsgrunnlag i forbindelse med nye behandlinger av personopplysninger i kommunen. Marker kommune har ikke fremlagt dokumenterte rutiner for hvem som har ansvar for å fastsette behandlingsgrunnlag i for kommunens behandling av personopplysninger.

4.2.4 Kommunen skal ha etablert sletterutiner for sin behandling av personopplysninger

Marker kommunes behandlingsprotokoll inneholder en kolonne for å angi frister for «Sletting og lagring» av personopplysningene som behandles. Ifølge behandlingsprotokollen fremgår ulike beskrivelser i kolonnen for lagrings- og slettefrister, herunder:

- Opplysningene slettes når formålet er oppfylt
- Slettes manuelt når ansatte slutter
- Opplysningene arkiveres når formålet er oppfylt
- Vi benytter ikke automatiske avgjørelser
- Det gjøres ingen automatiske avgjørelser
- Det tas ikke automatiske avgjørelser
- Det er ingen automatiske avgjørelser i behandlingen
- Det utføres ingen automatiske avgjørelser i behandlingen
- Det inngås samtykke for de automatiske avgjørelsene

Marker kommune har utover oppføringene i behandlingsprotokollen ikke fremlagt dokumenterte sletterutiner for sin behandling av personopplysninger. Det fremkom i intervju at det som hovedregel ikke lagres informasjon på en tidligere ansatt sin PC etter avsluttet arbeidsforhold. Det ble videre opplyst at det tar omtrent én måned fra arbeidsforholdet avsluttes til brukerkonto og informasjon lagret på PC-en slettes.

4.2.5 Kommunen skal ha sørget for å informere de registrerte om behandlingen av deres personopplysninger

Marker kommune har utarbeidet dokumentet *Informasjon og kommunikasjonsstrategi*. Det fremgår av dokumentet at kommunen har utarbeidet en informasjons- og kommunikasjonsstrategi som skal sikre

helhet og sammenheng i kommunens informasjons- og kommunikasjonsarbeid, og være en veileder i arbeidet for kommunens ansatte. Dokumentet inneholder informasjon om kommunens prinsipper og forutsetninger for informasjons- og kommunikasjonsarbeid, inkludert:

> *«**Åpenhet**: I sin kommunikasjon skal Marker kommune være åpen, tydelig og tilgjengelig. Kommunikasjonen skal være pålitelig og lettfattet. Kommunen skal følge prinsippet om meroffentlighet.»*

Det fremgår av dokumentet *Informasjon og kommunikasjonsstrategi* at kommunikasjon er et lederansvar i kommunen. Videre fremgår det at kommunikasjonsansvaret skal følge «linjeprinsippet» - at den som har ansvaret for en tjeneste/enhet også har ansvaret for informasjonen og kommunikasjonen knyttet til den aktuelle tjeneste/enhet.

Kommunens hjemmeside (lenke) inneholder en samling av 181 personvernerklæringer som opplyser om hvordan kommunen samler inn og bruker personopplysninger om innbyggere og ansatte innenfor ulike avdelinger og seksjoner. I forbindelse med dokumentgjennomgangen har revisjonslaget gjennomført stikkprøver av enkelte lovpålagte områder som kommunen er forpliktet å beskrive i personvernerklæringene. Stikkprøvene har tatt utgangspunkt i tre personvernerklæringer, herunder *Skolehverdagen*, *Dagsenter*, *Administrere ansatte (personalmappe)* og *Flyktningtjenesten*.

Det kan utledes fra stikkprøvene at personvernerklæringene er utarbeidet etter en mal som inneholder beskrivelser av «formål», «behandlingsgrunnlag», «kategorier av registrerte», «kategorier av personopplysninger», «mottakere», «hvor samler vi dine personopplysninger fra», «overføring av personopplysninger til tredjeland» og «lagring av personopplysningene». Det fremgår av stikkprøvene at under området «Mottakere av personopplysninger» er det i samtlige av de kontrollerte personvernerklæringene angitt at «personopplysninger overføres ikke til tredjeland.». Tilsvarende står det under området «Lagring av personopplysningene» i samtlige av personvernerklæringene at «vi benytter ikke automatiske avgjørelser.»

På kommunens hjemmeside er overordnet personvernerklæring tilgjengelig under fanen *Generell personverninfo.* Personvernerklæringen inneholder beskrivelser av hvordan Marker kommune behandler personopplysninger om innbyggerne og hvilke rettigheter innbyggerne har som registrerte i kommunens systemer. Personvernerklæringen inneholder beskrivelser av følgende områder:

- Hvorfor behandler vi personopplysninger om deg?
- Det rettslige grunnlaget
- Hvor henter vi opplysningene fra?
- Hvilke personopplysninger behandler vi?
- På hvilken måte samler vi inn personopplysninger om deg?
- Hvordan tar vi vare på opplysningene dine?
- Hvem utleverer vi personopplysningene dine til?
- Hvor lenge oppbevarer vi personopplysningene dine?
- Hvem er behandlingsansvarlig?
- Hvilke rettigheter har du?
- Personvernombud for Marker kommune

Marker kommune har fremlagt dokumentet *Innsamling og bruk av personopplysninger, Marker kommune – Personvernerklæring.* Denne personvernerklæringen inneholder beskrivelser av hvordan Marker kommune samler inn og bruker personopplysninger, strukturert under følgende overskrifter:

- Rettigheter til grunnleggende informasjon om behandling av personopplysninger
- Generelt om kommunens behandling av personopplysninger
- Nettbasert behandling av personopplysninger
- Saksbehandling og arkiv
- E-post og telefon
- Personopplysninger ansatte
- Helseopplysninger
- Personopplysninger om elever
- Barnehagebarn og foresatte
- Personopplysninger barnevern
- Generelt om logging i Marker kommunes fagsystemer
- Innsynsrett
- Retting og sletting.

Det ble opplyst i intervju at enkelte informanter ikke var kjent med personvernerklæringene som gjelder de ansatte i kommunen.

4.2.6 Kommunen skal ha etablert rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter

Marker kommune har gjennom personvernerklæringen *Generell personverninfo* på nett (lenke) utarbeidet beskrivelser av hvilke rettigheter de registrerte kan påberope seg overfor kommunen. Her vises det til kommunens innsynsportal for forespørsler om innsyn i personopplysninger.

Marker kommune har utarbeidet dokumentet *Innsynsrett Marker kommune.* Dokumentet inneholder beskrivelser hva innsynsretten går ut på, herunder beskrivelser av hva du kan be om innsyn i, hvorfor be om innsyn og unntak fra innsynsretten, samt informasjon om kommunens innsynsskjema. Dokumentet inneholder også en lenke til Datatilsynets nettsider og informasjon om retten til innsyn.

Marker kommune har utarbeidet dokumentet *Offentlig dokumentjournal/Innsyn,* som er offentlig tilgjengelig i arkivplanen for Marker kommune (lenke). Dokumentet inneholder beskrivelser om retten til innsyn etter offentlighetsloven og forvaltningsloven. Dokumentet inneholder en setning om at innbyggerne etter personopplysningsloven har «rett til å få vite hvilke opplysninger en virksomhet har registrert og hva opplysningene brukes til.» Det fremgår av dokumentet at innsynsbegjæringer skal besvares «etter gjeldende lovverk snarets og vanligvis innen 3 virkedager».

Marker kommune har ikke fremlagt etablerte rutiner for hvordan kommunen håndterer forespørsler fra de registrerte om å utøve sine rettigheter etter personvernregelverket.

Det ble opplyst i intervju at praksis knyttet til håndtering av forespørsler fra de registrerte om å utøve sine rettigheter er noe ulik innenfor de forskjellige virksomhetsområdene. Det ble opplyst at barnevernstjenesten har mottatt innsynsforespørsler, og at disse har blitt behandlet etter barnevernstjenestens egne retningslinjer.

Det ble opplyst i intervju at flere informanter var mindre kjent med rutinene for håndtering av forespørsler om utøvelse av de registrertes rettigheter, da kommunen generelt mottar få slike forespørsler.

4.2.7 Kommunen skal ha etablert egnede tiltak for å ivareta personopplysningssikkerheten

Marker kommune har utarbeidet dokumentet *Sikkerhetshåndbok for informasjonssikkreheten i Marker kommune m/sikkerhetsmål og sikkerhetsstrategi,* som inneholder beskrivelser av kommunens sikkerhetsmål og -strategi. Det fremgår av dokumentet at sikkerhetshåndboken fastlegger kommunens krav til beskyttelse av personopplysninger som samles inn, lagres, bearbeides, overføres og formidles, både manuelt og elektronisk. Videre fremgår det av dokumentet at sikkerhetshåndboken utgjør et overordnet rammeverk for det praktiske arbeidet med informasjonssikkerhet og personvern i kommunen. Det følger også av dokumentet at sikkerhetshåndboken er utarbeidet for å sikre etterlevelse av rettslige krav og sikkerhetsstander, som blant annet Personopplysningsloven, EUs personvernforordning og ISO/IEC 27001.

Dokumentet *Forkortet/revidert - Sikkerhetshåndbok for informasjonssikkreheten i Marker kommune m/sikkerhetsmål og sikkerhetsstrategi* inneholder nærmere beskrivelser av kommunens organisering og ansvar for sikkerheten Det fremgår av dokumentet at kommunen differensierer mellom flere roller og ansvar for sikkerheten, inkludert kommunedirektør, kommunalsjef, sikkerhetsansvarlig, autorisasjonsansvarlig og medarbeidere, samt IT-avdelingen.

Beskrivelser av kommunens sikringstiltak for å ivareta informasjons- og personopplysningssikkerhet fremgår av dokumentet *Forkortet/revidert - Sikkerhetshåndbok for informasjonssikkreheten i Marker kommune m/sikkerhetsmål og sikkerhetsstrategi.* I dokumentet fremgår det at sikringstiltakene er inndelt i fire hovedkategorier: administrative og driftsmessige sikringstiltak, personellsikkerhet og annen systemteknisk sikring. Det følger av dokumentet at de konkrete tiltakene omfatter følgende:

Administrative og driftsmessige sikringstiltak	Personellsikkerhet	Systemteknisk sikring
Systemplanlegging og -anskaffelse	Etiske regler	Sikkerhetskopiering og oppbevaring av kopier
Drift av kommunens IT-systemer	Fast ansatt personell og vikarer med tidsbegrenset arbeid	Aktiviteslogging
Avvikshåndtering og forbedringsordning i kommunen	Konsulenter og leverandører	Sikringstiltak mot datavirus, spam, hacking etc.
Egenkontroll/ledelsens gjennomgang	Servicepersonell (teknikere, håndverkere, rengjøringspersonell etc.)	Destruksjon/sletting av sensitive data
Avbrudds- og beredskapsplan	Besøkende	Logisk tilgangskontroll, inkl: - Brukeridentifiskasjon/autentisering - Autorisasjonskontroll - Regler vedrørende bruk av passord og påloggingsrutiner
Utskrifter/dokumenter, kopiering og makulering	Taushetsplikt	Rutiner for bruk av e-post
Sikkerhet og orden på det enkelte kontor	Brudd på reglement/arbeidsavtale	Kommunens rettigheter mht innsyn i ansattes e-post

Som beskrevet i rapportens kapittel 4.2.1.2 har Marker kommune fremlagt tolv eksempler på gjennomførte risiko- og sårbarhetsvurderinger (ROS) av ulike løsninger, enheter og prosesser i kommunen. Det fremgår av risikovurderingene som er gjennomført i dokumentene *ROS-analyse-skytjenester* og *ROS-*

analyse-IKT at enkelte personvernrelaterte risikoer er identifisert og vurdert, herunder risikoen for at personopplysninger kommer på avveie. Vurderingene inkluderer beskrivelser av de uønskede hendelsene, årsakene til hendelsene, eksisterende risikoreduserende tiltak, samt en vurdering av sannsynlighet og konsekvens både før og etter implementering av tiltakene.

Det fremgår av dokumentet *Forkortet/revidert - Sikkerhetshåndbok for informasjonssikkreheten i Marker kommune m/sikkerhetsmål og sikkerhetsstrategi* beskrivelser av kommunens sikkerhetsutfordringer fremover. Gjennom beskrivelsene trekker kommunen frem utfordringer som phishing/hackere, mobilsikkerhet, rutiner for melding og avvik, bruk av kunstig intelligens (KI/AI), samt viktigheten av å gjennomføre risiko- og sårbarhetsanalyser (ROS) og personvernkonsekvensvurderinger (DPIA).

Svar fra spørreundersøkelsen avdekket flere gjentakende temaer knyttet til risikoer ved behandling av personopplysninger i kommunen. Det fremgår av svarene fra spørreundersøkelsen at kommunens lille størrelse, hvor «alle kjenner alle», kan skape utfordringer. Videre ble mangel på kompetanse og tilstrekkelig opplæring blant ansatte fremhevet, samt at mange er lite bevisst risikoene vedrørende personvern.

Blant de mest nevnte risikofaktorene trakk respondentene i spørreundersøkelsen frem utilsiktet eller bevisste menneskelige feil, som å forsnakke seg i møter eller unnlate å følge rutiner. Respondenter i spørreundersøkelsen pekte på at opplysninger ofte deles med personer som ikke har behov for det, og at ansatte har en overdreven tillit til at programvare og teknologi alene vil ivareta personvernet.

Andre risikoområder trukket frem av respondentene i spørreundersøkelsen var svakheter i fysiske sikkerhetstiltak, som svak lydisolering i fysiske rom og håndtering av fysiske dokumenter, spesielt i skolen. Respondentene i spørreundersøkelsen trakk frem risikoer som svake rutiner for internpost og tilgangskontroll, samt at tidligere ansatte kan ha tilgang til systemer etter arbeidsforholdets avslutning. Videre at ressursmangel og kapasitet fører til manglende overholdelse av eksisterende rutiner, noe som svekker den totale informasjonssikkerheten og bidrar til brudd på taushetsplikt og andre personvernbrudd.

4.2.8 Kommunen skal ha sørget for å gjennomføre personvernkonsekvensvurderinger når det er nødvendig

Marker kommune har fremlagt dokumentet *DPIA,* som inneholder en Excel-mal for gjennomføring av personvernkonsekvensvurderinger. Dokumentet inneholder flere faner, herunder «Forklaring på skala 1-10», «Initialvurdering», «Konsekvensutredning del 1», «Konsekvensutredning del 2» og «Rapport».

Det fremgår av fanen for «Initialvurdering» at brukerne skal legge inn beskrivelser av hvilken type behandling av personopplysninger det er snakk om, behandlingens formål, behandlingsgrunnlag, dato, informasjon om deltakerne, vurdering av proporsjonaliteten, samt innledende vurdering av behov for personvernkonsekvenser. Videre fremgår det av dokumentet at vurderingen av behovet skal baseres på ni kriterier. Dersom det er svart «Ja» på to eller flere av disse kriteriene, fremgår det av malen at en personvernkonsekvensvurdering skal gjennomføres. Det fremgår av malen at en personvernkonsekvensvurdering skal gjennomføres dersom det svares «Ja» på kun ett av kriteriene, forutsatt at behandlingen involverer innovativ bruk av ny teknologi eller organisatoriske verktøy.

Marker kommune har fremlagt dokumentene *DPIA-Digi helse – Marker kommune, DPIA-digisos, DPIA-legekontor* og *DPIA-barnehage.* Dokumentene inneholder eksempler på gjennomførte initialvurderinger og personvernvurderinger av ulike IT-systemer i kommunen, herunder den nasjonal digitale tjenesteplattformen Digi Helse, den digitale tjenesteplattformen Digisos, innføringen av nytt legesystem og den digitale løsningen Visma Flyt Barnehage. Det fremgår av dokumentene at det er gjennomført en innledende vurdering av behov for personvernkonsekvensvurdering for innføring av DigiSos, innføring av

nytt legesystem og innføring av Visma Flyt barnehage. Det fremgår av dokumentene at det ikke ble ansett som nødvendig å gjennomføre full personvernkonsekvensvurdering i disse tilfellene, basert på resultatene fra de initielle vurderingene.

Utover malen for gjennomføring av personvernkonsekvenser i dokumentet *DPIA*, har ikke Marker kommune fremlagt rutiner for gjennomføring av personvernkonsekvensvurderinger. Kommunen har videre ikke fremlagt dokumentasjon som beskriver når en vurdering av personvernkonsekvenser skal gjennomføres, når personvernombudet skal involveres eller når det er behov for forhåndsdrøfting med Datatilsynet etter GDPR artikkel 36.

4.2.9 Kommunen skal ha sørget for at databehandlere ivaretar krav til personvern og sikre at det inngås databehandleravtaler

Det ble opplyst i intervju at IT-ansvarlig har følgende ansvarsområder:

- har den overordnede oversikten over alle databehandleravtaler i kommunen.
- har hovedansvaret for å se til at alle databehandleravtaler er arkivert.
- etterlyse mangler i databehandleravtale.

Revisjonslaget ble informert om at oversikt over databehandlere for hvert system er tilgjengelig i Samsvar. Revisjonslaget er fremlagt oversikten.

Marker kommune har fremlagt dokumentene *Bilag 11 Marker databehandleravtale_generell_avtaletekst_2020* og *Bilag 11 Marker databehandleravtale_bilag_2020.* Dokumentene inneholder kommunens mal for databehandleravtale og bilag. Det fremgår av dokumentene at malen er utarbeidet av Direktoratet for forvaltning og økonomistyring (DFØ).

Kommunen har fremlagt fem eksempler på databehandleravtaler som er inngått mellom kommunen og ulike databehandlere, herunder *Databehandleravtale startlån, Custom Publish Databehandleravtale Marker kommune, Databehandleravtale AcosWebsak* og *Databehandleravtale Marker - Procon*. Revisjonslaget registrer at én av avtalene er utformet etter kommunens mal for databehandleravtaler, mens leverandørens mal for databehandleravtale er benyttet for de fire andre. I intervju ble det opplyst at det ofte er leverandørens databehandleravtale som benyttes. Revisjonslaget har ikke gjennomført en detaljert kvalitetssikring av om innholdet i de inngåtte databehandleravtalene oppfyller GDPR artikkel 28 som en del av forvaltningsrevisjonen.

Revisjonslaget er ikke fremlagt dokumenterte rutiner som sikrer at det inngås databehandleravtaler når det er nødvendig, eller oppfølging av inngåtte databehandleravtaler. Revisjonslaget er ikke fremlagt dokumenterte rutiner som sørger for at databehandlere ivaretar krav til personvern. Det ble opplyst i intervju at kommunen ikke har gjennomført evaluering eller kontroll av databehandlere de har avtaler med.

4.2.10 Kommunen skal ha kartlagt overføringer av personopplysninger til land utenfor EU/EØS og ha gjennomført nødvendige vurderinger og tiltak ved overføringer

Marker kommune har ikke fremlagt en komplett oversikt over overføringer av personopplysninger til land utenfor EU/EØS (tredjeland). Kommunens behandlingskontroll inneholder en kolonne for utfylling av informasjon om «Overføring til tredjeland». Ifølge behandlingsprotokollen fremgår ulike beskrivelser i denne kolonnen, herunder:

- På kommunens sak- og arkivsystem

- Personopplysningene lagres i kommunens journal, sak og arkivsystem
- Til land innen Schengenområdet
- I permer, hvis det ikke logges på besøkssystem
- På videosystem vi benytter
- På virksomhetens telefonsystem

Kommunens behandlingsprotokoll inneholder også en kolonne for utfylling av informasjon om «Mottakere av personopplysninger». Ifølge behandlingsprotokollen fremgår det av denne kolonnen ulike beskrivelser for at kommunen ikke overfører personopplysninger til tredjeland.

Det ble opplyst i intervju at kommunen ikke er kjent med om det overføres personopplysninger til tredjeland. Det ble videre opplyst at kommunens nåværende påloggingstjeneste benytter en server i USA, men at dette kun omfatter påloggingsinformasjon. Det ble videre forklart at denne løsningen vil bli avviklet ettersom Acos er i ferd med å migrere til en fullstendig skybasert løsning. Det fremgår av kommunens oversikt over databehandlere og systemer at kommunen benytter seg av den globale skytjenesteleverandøren Microsoft.

Kommunen har ikke fremlagt dokumenterte rutiner for vurderinger av overføringer av personopplysninger til land utenfor EU/EØS, eller eksempler på dokumenterte vurderinger som er gjort. Kommunen har ikke fremlagt dokumentasjon som beskriver hvilke tiltak som er implementert ved eventuelle overføringer av personopplysninger til land utenfor EU/EØS.

4.2.11 Kommunen skal ha utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39

Det fremgår av dokumentet *Sikkerhetshåndbok for informasjonssikkreheten i Marker kommune m/sikkerhetsmål og sikkerhetsstrategi* at kommunen har et personvernombud. Marker kommune har ikke fremlagt dokumentasjon som viser hvilken prosentandel eller stillingsbrøk personvernombudet har i kommunen. I intervju ble revisjonslaget opplyst om at personvernombudet er innleid i Marker kommune gjennom en fast avtale. Videre at personvernombudet bistår ti andre kommuner med personvernrelaterte spørsmål.

Marker kommune har fremlagt dokumentet *avtale Personvernombud,* som utgjør kommunens avtale med personvernombudet. Det fremgår av dokumentet at avtalen gjelder for to år fra 01.03.2018 og at oppsigelsestiden er 3 måneder. Dokumentet inneholder beskrivelser av personvernombudets oppgaver, herunder:

- *«Påse at behandlinger av personopplysninger blir meldt til ombudet, og at meldingene inneholder korrekte og tilstrekkelige opplysninger,*
- *Føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene,*
- *Påse at behandlingsansvarlig har et system for internkontroll som tilfredsstiller personopplysningslovens § 14, jf. personopplysningsforskriftens kapittel 3,*
- *Bistå de registrerte med å ivareta deres rettigheter etter reglene om behandling av personopplysninger,*
- *Påpeke brudd på personopplysningsloven overfor behandlingsansvarlig,*
  Gi Datatilsynet opplysninger dersom tilsynet ber om det, herunder foreta undersøkelser i konkrete saker,
- *Holde seg orientert om utviklingen innen personvern, og*
- *Gi råd og veiledning til behandlingsansvarlig om behandling av personopplysninger og reglene for dette.*

- *Bistand som kommunens personvernombud med jevnlige besøk i kommunen pluss mail-/ telefonkontakt (også direkte med publikum/innbyggere) etter behov – samt direkte og jevnlig kontakt med Datatilsynet*
- *Gjennomføring av årlig sikkerhetsrevisjon*
- *Oppdatering av kommunens Sikkerhetshåndbok inkl nye elementer/krav bl.a. i forhold til GDPR»*

Marker kommune har ikke fremlagt dokumenterte rutiner på når og i hvilke saker personvernombudet skal involveres overfor de ansatte i kommunen. Det ble opplyst i intervju at enkelte informanter involverer personvernombudet i forbindelse med avvik. Videre at kommuneledelsen har møter med personvernombudet 2-3 ganger i året. Revisjonslaget ble informert om at personvernombudet har et tett samarbeid med kommunalsjefen og IT-sjefen i kommunen.

Revisjonslaget ble informert om at det er en tydelig bevissthet rundt personvernombudets uavhengige rolle i kommunen. I intervju ble det opplyst at personvernombudet regelmessig gjennomfører interne vurderinger for å overvåke personvernarbeidet. Dersom personvernombudet avdekker svakheter eller mangler i personvernarbeidet, tar ombudet dette opp med kommunen.

Intervjuobjektene opplyste at personvernombudet utarbeider skriftlige rapporter for å dokumentere funn fra sine vurderinger. Det fremkom videre at personvernombudet gjennomfører jevnlige gjennomganger med ledergruppen for å sikre kontinuerlig oppfølging og forbedring av personvernarbeidet.

4.2.12 Kommunen skal ha sørget for at avvik knyttet til personvern blir meldt, registrert og håndtert

Det ble opplyst i intervju at Marker kommune benytter TQM for registrering og håndtering av avvik. Revisjonslaget har gjennomført stikkprøver av avvikssystemet. Det fremgår av stikkprøvene at kommunen ved registrering av avvik kan kategorisere disse som personvernavvik ved å angi GDPR/Personvern som «prosesstype». Det fremgår av intervjuer at registrerte avvik videresendes til den ansvarlige for oppfølging og lukking. Det ble opplyst at kommunedirektøren har det overordnede ansvaret for personvernavvik, mens HR-direktøren har en støttende rolle.

Marker kommune har utarbeidet dokumentet *Mål for personvernarbeidet i Marker kommune.* Dokumentet inneholder mål for kommunens avviksbehandling, herunder:

> *«**Avviksbehandling***
> *Når det oppdages avvik fra planen skal det meldes som avvik i kvalitetsssytemet TQM. Meldte avvik i perioden gjennomgås ved årlig revisjon av planen».*

Det fremgår av dokumentet *Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)* at kommunen har overordnede rutiner for avvikshåndtering og forbedringsordning, inkludert avvik knyttet til personvern. Det fremgår av dokumentet at kommunen skal ha etablerte rutiner for rapportering, registrering og oppfølging av avvik, samt forslag til forbedringer. Kommunen har imidlertid ikke fremlagt slike etablerte og dokumenterte rutiner for rapportering, registrering og oppfølging av avvik.

Videre fremgår det av dokumentet at kommunen må sikre at personvernavvik og andre typer avvik blir avdekket, dokumentert og håndtert i samsvar med gjeldende personvernbestemmelser og interne retningslinjer. For å oppfylle dette kravet, fremheves viktigheten av et avvikssystem som dekker håndteringen av alle typer avvik, slik at de blir korrekt fulgt opp og adressert i tråd med gjeldende regelverk. Det fremgår av dokumentet at avvik skal meldes i kommunens avvikssystem eller til nærmeste leder i

spesielle situasjoner, og at alvorlige hendelser skal meldes til Datatilsynet. Kommunen har imidlertid ikke fremlagt en rutine som sikrer at rapporteringspliktige avvik meldes til Datatilsynet innen den lovpålagte fristen på 72 timer eller at underretningsplikten til de registrerte overholdes.

Marker kommune har utarbeidet dokumentet *Når og hvordan skal jeg melde avvik?* Dokumentet inneholder beskrivelser om hva som utgjør et avvik eller brudd på personopplysningssikkerheten. Det fremgår av dokumentet at brudd som omfatter personopplysninger og som innebærer risiko for enkeltpersoners rettigheter og friheter, skal meldes til Datatilsynet.

I intervjuer ble det uttrykt en mistanke om underrapportering på mindre avvik. Revisjonslaget ble informert om at kommunen ikke er kjent med at det har vært større avvik som burde ha blitt rapportert. I spørreundersøkelsen, på spørsmål om ansatte kjenner til hvordan avvik knyttet til personvern skal rapporteres, svarte 54,2 % «ja» og 45,8 % «nei».

Av stikkprøven revisjonslaget gjennomførte av TQM fremkom det at det ikke er registrert noen personvernavvik i løpet av de siste fem årene. I intervju ble det opplyst om at det har vært et avvik knyttet til barnevernet. Avviket omhandlet bruken av et lukket Teams-rom. Teams-rommet ble benyttet til administrative formål som ferieplanlegging for ansatte, og ikke til behandling av sensitive opplysninger om barn. Bruken av dette teams-rommet skal ha blitt avklart med IT-avdelingen før det ble tatt i bruk. Avviket ble fulgt opp av ledelsen i samarbeid med IT-avdelingen, og nødvendige tiltak ble implementert for å sikre korrekt bruk av systemet fremover. Dette avviket fremgikk ikke av revisjonslagets stikkprøve av TQM.

4.3 Vurderinger

Marker kommune har i noen grad har etablert en tilfredsstillende internkontroll for personvern	Gul

Revisjonslaget vurderer at Marker kommune i noen grad har etablert og implementert et Internkontroll-system for personvern.

Revisjonslaget ser positivt på at internkontrollsystemet er bygd opp av enkelte styrende, gjennomførende og kontrollerende elementer som samsvarer med Datatilsynets veiledning om hvordan kravet til internkontroll etter GDPR artikkel 24 skal forstås. Revisjonslaget ser også positivt på at kommunens styrende dokumenter inneholder beskrivelser av generelle forpliktelser som er relevant for kommunen etter personvernlovgivningen, som kravet til å ha en dokumentert behandlingsprotokoll, samt andre krav som har blitt innført med den nye personvernforordningen, sammenlignet med den tidligere personopplysningsloven. Videre ser revisjonslaget positivt på at Internkontrollsystemet for personvern også dekker informasjonssikkerhet. Dette kan bidra til synergier og effektivitet, og blant annet sikre at lignende aktiviteter fra de to fagområdene slås sammen til én aktivitet. Revisjonslaget ser også positivt på at internkontrollsystemet er basert på ISO 27001-standarden.

Revisjonslaget har avdekket noen forbedringsbehov som er beskrevet i avsnittene nedenfor.

1. **Beskrevet overordnede rammer for personvernarbeidet i styrende dokumenter**

Revisjonslaget vurderer at Marker kommune har utarbeidet styrende dokumenter som i stor grad beskriver alle områder som er anbefalt i Datatilsynets veiledning om hvordan kravet til internkontroll etter GDPR artikkel 24 skal forstås.

Marker kommunes styrende dokumenter inneholder likevel ikke en oversikt over kommunens rutiner og retningslinjer for vern av personopplysninger, eller skriftlige beskrivelser av hvordan internkontrollsystemet henger sammen. Dette gjør det vanskelig for revisjonslaget å vurdere om internkontrollsystemet for personvern fungerer som helhet i praksis, og om det oppfyller kravene til effektiv kontroll og kontinuerlig forbedring av personvernarbeidet i kommunen.

2. **Gjennomført risikovurderinger for å identifisere behov for tekniske og organisatoriske tiltak**

Revisjonslaget vurderer at Marker kommune har gjennomført enkelte risikovurderinger for å identifisere behov for tekniske og organisatoriske tiltak. Revisjonslaget vurderer imidlertid at fremlagte risikovurderinger i liten grad er egnet til å belyse hvilke tekniske og organisatoriske tiltak som bør implementeres på personvernområdet. Revisjonslaget finner det heller ikke dokumentert at kommunens maler for risikovurderinger legger opp til å vurdere hvilke konsekvenser identifiserte risikoer kan ha for enkeltpersoners rettigheter og friheter slik GDPR artikkel 32 krever.

3. **Etablert tilfredsstillende rutiner og retningslinjer for håndtering av personopplysninger basert på en risikovurdering og sørget for å kommunisere disse ut i organisasjonen**

Revisjonslaget vurderer at Marker kommune har identifisert behovet for enkelte rutiner og retningslinjer for håndtering av personvern basert på risikovurderinger, som for eksempel rutiner for brudd på personopplysningssikkerheten, innsamling og bruk av personopplysninger i Marker kommune og personvern på arbeidsplassen. Revisjonslaget vurderer likevel at kommunen har et mindre omfang av rutiner, retningslinjer og arbeidsinstrukser for personvern, enn forventet. Dette gjelder både antallet rutiner og retningslinjer, og deres omfang.

Revisjonslaget ser likevel positivt på at kommunen gjennom kvalitets- og internkontrollsystemene Samsvar og TQM har etablert prosesser for å sikre at kommunens ansatte kan ivareta sentrale plikter etter personvernlovgivningen, som for eksempel varsling av personvernavvik eller gjennomføring av personvernkonsekvensvurderinger når det er nødvendig. At kommunen ikke har fremlagt nærmere skriftlige rutiner og retningslinjer for flere av disse prosessene, bidrar til at det kan oppstå usikkerhet om hvordan de ansatte skal ivareta disse pliktene i praksis. Dette kan medføre feilaktig eller mangelfull håndtering av disse prosessene, noe som kan føre til brudd på personvernlovgivningen og kommunens mål for personvernområdet.

Basert på svarene fra spørreundersøkelsen, er det revisjonslagets vurdering at det er varierende kjennskap til de etablerte rutinene og retningslinjene blant de ansatte. Det er også revisjonslagets vurdering at svarene fra spørreundersøkelsen viser også at opplevelsen av etterlevelse også varierer betydelig blant de ansatte.

4. Sørget for at ansvar og roller innen personvern er kommunisert og forstått

Revisjonslaget vurderer at Marker kommune ikke i tilstrekkelig grad har sørget for at ansvar og roller innen personvern er tydelig kommunisert eller fullt ut forstått.

Til tross for at Marker kommunes styrende dokumenter inneholder beskrivelser av den nærmere organiseringen av informasjonssikkerhet og personvern i kommunen, er det revisjonslagets vurdering at disse fremstår som overordnede og i liten grad plasserer et tydelig ansvar for konkrete personvernoppgaver i organisasjonen. Revisjonslaget vurderer også at disse beskrivelsene i liten grad tydeliggjør ansvarsfordelingen mellom kommunen og virksomhetslederne.

Intervjuene viser også at enkelte informanter opplever uklarheter om hvem som faktisk har ansvaret for personvern, og for hva. Selv om det ikke kan stilles krav om at alle ansatte besitter denne informasjonen, er det viktig at nøkkelpersoner og virksomhetsledere har en klar forståelse av sine roller og ansvar for å sikre at sentrale personvernaktiviteter blir ivaretatt på en tilfredsstillende måte. Dette er særlig viktig for personvernaktiviteter der ansvaret for gjennomføringen er delegert ned i virksomhetene.

5. Sørget for regelmessig og rollebasert opplæring innen personvern

Revisjonslaget vurderer at Marker kommune i noen grad sørger for regelmessig og rollebasert opplæring innen personvern i tilstrekkelig grad.

Revisjonslaget ser positivt på at personvernombudet holder jevnlig opplæring med ledergruppen når ombudet er til stede. Revisjonslaget mener likevel at denne informasjonen alene ikke sikrer at kommunens ansatte etterlever virksomhetens rutiner og retningslinjer på en tilstrekkelig måte. Dette støttes av svarene fra spørreundersøkelsen, som viser at det er stor variasjon i hvorvidt personvern tas opp i avdelinger og virksomheter.

Revisjonslaget vil gi en positiv bemerkning til at kommunen har igangsatt en prosess for å sikre opplæring ved onboarding av nyansatte, og at det vurderes å etablere et eget personvernteam i kommunen. Revisjonslaget vurderer at tiltak som dette, med riktig omfang, vil kunne bidra positivt til at kommunen når sitt mål om å utvikle et opplæringsprogram som dekker grunnleggende personvernprinsipper, kommunens retningslinjer og sentrale krav i GDPR. At tiltaket ikke er gjennomført er likevel utslagsgivende for revisjonslagets vurdering.

6. Sørget for regelmessig evaluering og forbedring av internkontrollen.

Revisjonslaget vurderer at Marker kommune i noen grad sørger for regelmessig evaluering og forbedring av internkontrollen.

Revisjonslaget vurderer at Marker kommune har etablert flere tiltak for å sørge for regelmessig evaluering og forbedring av internkontrollen, som personvernombudets egenkontroll gjennom intervjuer og enkelte egenkontroller gjennomført av virksomhetene. Ettersom revisjonslaget ikke har fått fremlagt dokumentasjon som konkretiserer kommunens rutiner for egenkontroll er det vanskelig å vurdere hvorvidt disse rutinene er tilstrekkelige og effektive for å sikre en helhetlig og kontinuerlig forbedring av internkontrollen.

Marker kommune har i stor grad en oppdatert protokoll over behandlingsaktiviteter som tilfredsstiller kravene i GDPR artikkel 30	Lysegrønn

Revisjonslaget vurderer at Marker kommune i stor grad har en behandlingsprotokoll som inneholder alle lovpålagte områder som skal beskrives etter GDPR artikkel 30.

Revisjonslaget har hentet ut en detaljert oversikt kommunens behandlingsprotokoll i systemet Samsvar. Mens de fleste områdene i kommunens behandlingsprotokoll for hver behandlingsaktivitet ser ut til å være fylt ut med relevante beskrivelser, er det likevel revisjonslagets vurdering at det foreligger enkelte tilfeller hvor beskrivelsene ikke samsvarer med det tilhørende lovpålagte området. For eksempel står det under feltet «Mottakere av personopplysninger» for flere behandlingsaktiviteter at «Personopplysninger overføres ikke til tredjeland», som ikke direkte svarer på hvem som mottar opplysningene. Tilsvarende står det under feltet «Sletting og lagring» for mange behandlingsaktiviteter at «Det er ingen automatiske avgjørelser i behandlingen», noe som heller ikke svarer på spørsmålet om sletting og lagring av data. Det er revisjonslagets vurdering at dette bidrar til at behandlingsprotokollen ikke gir en fullstendig og nøyaktig oversikt over kommunens behandlingsaktiviteter. Ettersom noe av hensikten med å føre behandlingsprotokoll er at behandlingsansvarlige får en slik fullstendig oversikt over behandlingsaktiviteter som utføres under virksomhetens ansvar, kan beskrivelser som fremstår som ufullstendige eller unøyaktige føre til manglende etterlevelse av personvernlovgivningen og potensielle risikoer for personvernet.

Revisjonslaget har også avdekket et forbedringspotensial knyttet til å dokumentere hvem som har ansvar for å fylle ut og oppdatere nye og eksisterende behandlingsprotokoller.

Marker kommune har i stor grad sørget for rettslig grunnlag for behandling av personopplysninger blir vurdert og dokumentert	Lysegrønn

Revisjonslaget vurderer at Marker kommune i stor grad har sørget for at rettslig grunnlag for behandling av personopplysninger blir vurdert og dokumentert.

Marker kommune har i kommunens behandlingsprotokoll dokumentert hvilke behandlingsgrunnlag som benyttes etter både GDPR artikkel 6 og artikkel 9. Revisjonslaget ønsker også fremheve at Marker kommune har dokumentert supplerende rettsgrunnlag (norsk lov) for behandlingsaktiviteter som er hjemlet i GDPR artikkel 6 nr. 1 bokstav c) eller e), i tråd med lovkravet. Revisjonslaget oppfordrer likevel kommunen til å tydeliggjøre den konkrete lovhjemmelen, ut over en generell henvisning til loven. Dette er særlig viktig for mer inngripende behandlinger, der en klar og presis hjemmel bør være ekstra fremhevet.

Mangelen på skriftlige rutiner for vurdering av behandlingsgrunnlag ved eventuelle nye behandlingsaktiviteter gjør at revisjonslaget er usikkert på hvordan kommunen sikrer at rettslig grunnlag for disse behandlingsaktivitetene blir tilstrekkelig vurdert og dokumentert.

Marker kommune har i liten grad etablert sletterutiner for sin behandling av personopplysninger	Orange

Revisjonslaget vurderer at Marker kommune i liten grad har sørget for å etablere sletterutiner for sin behandling av personopplysninger.

Selv om behandlingsprotokollen for enkelte behandlingsaktiviteter inneholder beskrivelser av frister for sletting og lagring, foreligger det for de fleste behandlingsaktivitetene beskrivelser som ikke samsvarer med området for «Sletting og lagring». For eksempel står det under området «Sletting og lagring» for de fleste behandlingsaktiviteter beskrivelser som «Vi benytter ikke automatiserte avgjørelser», «Det tas ikke automatiske avgjørelser» eller «Det inngås samtykke for de automatiske avgjørelsene».

Revisjonslaget vurderer at Marker kommune ikke har fremlagt tilstrekkelig skriftlige sletterutiner for behandling av personopplysninger, utover de generelle beskrivelsene i behandlingsprotokollen. Dette medfører at kommunen ikke oppfyller kravet om å etablere spesifikke og skriftlige sletterutiner for behandling av personopplysninger, slik det er påkrevd etter GDPR.

Marker kommune har i noen grad sørget for å informere de registrerte om behandlingen av deres personopplysninger	Gul

Revisjonslaget vurderer at Marker kommune i noen grad har sørget for å informere de registrerte om behandlingen av deres personopplysninger.

Revisjonslaget vurderer at kommunens personvernerklæringer i stor grad dekker alle lovpålagte områder som kreves etter GDPR artikkel 12-14. Revisjonslaget har imidlertid merket seg at kommunens personvernerklæringer ikke inneholder identiteten og kontaktopplysningene til den behandlingsansvarlige eller kontaktopplysningene til personvernombudet, jf. GDPR artikkel 13 nr. 1 a og b. Revisjonslaget har avdekket et forbedringspotensial knyttet til innholdet i enkelte av personvernerklæringene, spesielt når det gjelder formålet for behandlingen, som i noen tilfeller er beskrevet ganske overordnet.

Basert på de stikkprøvene som er gjort, har revisjonslaget også merket seg at informasjonen i flere personvernerklæringer ikke samsvarer med overskriften informasjonen er plassert under. Dette kan bidra til at informasjonen fremstår mindre forståelig og tilgjengelig enn det som kreves etter GDPR artikkel 12-14. Det bemerkes at revisjonslaget ikke har kontrollert alle personvernerklæringene, eller kontrollert at all behandling av personopplysninger som kommunen gjør er omtalt i personvernerklæringene.

Til slutt har revisjonslaget merket seg et forbedringspotensial knyttet til informasjon som gis til de ansatte i kommunen om hvordan deres personopplysninger behandles. Dette fremkom i intervjuer, hvor enkelte ansatte ikke kjente til at det fantes personvernerklæringer rettet mot de ansatte i kommunen.

Marker kommune oppfyller ikke revisjonskriteriet om å ha etablert rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter	Rød

Revisjonslaget vurderer at Marker kommune ikke oppfyller revisjonskriteriet om å ha etablert rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter.

Revisjonslaget vurderer at Marker kommune har etablert lovpålagt informasjon til kommunens innbyggere om hvordan de kan utøve sine rettigheter, særlig retten til innsyn i egne personopplysninger. Ettersom kommunen ikke har fremlagt skriftlige rutiner for hvordan forespørsler om innsyn, retting, sletting, begrensning og protester skal håndteres av kommunen, medfører dette at revisjonslaget ikke kan bekrefte at slike rutiner er etablert.

Marker kommune har i stor grad har etablert egnede tiltak for å ivareta personopplysningssikkerheten	Lysegrønn

Revisjonslaget vurderer at Marker kommune i stor grad har etablert egnede tiltak for å ivareta personopplysningssikkerheten.

Revisjonslaget vurderer at Marker kommune har etablert flere egnede tiltak for å oppnå kommunens mål for informasjonssikkerhet og vern av personopplysninger. Revisjonslaget ser positivt på at kommunen i gjennomførte risikovurderinger har dokumentert eksisterende og forslag til nye risikoreduserende tiltak, som for eksempel rutiner, opplæring og bevisstgjøring, kryptering og back-up. Det presiseres imidlertid at revisjonslaget ikke har foretatt en gjennomgang eller overprøving av kommunens egne vurderinger. Sett opp mot risikoene som trekkes frem i spørreundersøkelsen, har revisjonslaget imidlertid avdekket enkelte forbedringspotensial knyttet til om ytterligere eller mer målrettede tiltak burde vært implementert.

Marker kommune har i noen grad sørget for å gjennomføre personvernkonsekvensvurderinger når det er nødvendig	Gul

Revisjonslaget vurderer at Marker kommune i noen grad har sørget for å gjennomføre personvernkonsekvensvurderinger når det er nødvendig.

Revisjonslaget vurderer at Marker kommune har etablert en mal for gjennomføring av personvernkonsekvensvurderinger som samsvarer med de elementer en slik vurdering skal inneholde etter GDPR. Revisjonslaget vurderer at malen kan være et nyttig verktøy for brukerne, da den i stor grad bidrar til å sikre at vurderingen inneholder de påkrevde momentene.

Revisjonslaget har imidlertid avdekket et forbedringspotensial ved at malen kan inneholde flere hjelpetekster for å gi veiledning til brukerne om hva de skal beskrive. Det understrekes at revisjonslaget ikke har gjennomført en kvalitetssikring av de fremlagte personvernkonsekvensvurderingene, eller kartlagt om det er gjennomført personvernkonsekvenser i alle tilfeller hvor det er nødvendig.

Revisjonslaget har også avdekket et forbedringspotensial knyttet til skriftlige rutiner og veiledninger for gjennomføring av personvernkonsekvensvurderinger, da Marker kommune ikke har fremlagt dokumentasjon som beskriver når en personvernkonsekvensvurdering skal gjennomføres, informasjon om når personvernombudet skal involveres, eller når forhåndsdrøfting med Datatilsynet skal finne sted.

Videre er det heller ikke fremlagt dokumentasjon som beskriver kommunens krav til fremgangsmåte i en personvernkonsekvensvurdering. Selv om det ikke er et uttrykkelig krav i GDPR, vurderer revisjonslaget at dette utgjør en nødvendig forutsetning for å sikre en enhetlig praksis og høy kvalitet i vurderingene som utføres.

Marker kommune har i liten grad sørget for at databehandlere ivaretar krav til personvern og sikret at det inngås databehandleravtaler	Gul

Revisjonslaget vurderer at Marker kommune i liten grad har sørget for at databehandlere ivaretar krav til personvern og sikret at det inngås databehandleravtaler.

Revisjonslaget vurderer at Marker kommune har etablert en mal for databehandlere, og har inngått databehandleravtaler med flere leverandører som behandler personopplysninger på vegne av kommunen. Selv om noen av databehandleravtalene er inngått etter kommunens mal, benyttes leverandørenes maler i de fleste tilfelle.

Revisjonslaget vurderer at kommunens mal for databehandleravtaler er godt egnet til å sikre at databehandlere forplikter seg til å oppfylle kravene til personvern i henhold til GDPR artikkel 28. Videre vurderer revisjonslaget at de fremlagte eksterne databehandleravtalene også er tilstrekkelige for å sikre at databehandlere forplikter seg til å oppfylle kravene til personvern etter samme bestemmelse. Revisjonslaget har ikke gjennomført en detaljert kvalitetssikring av om innholdet i de fremlagte databehandleravtalene som en del av forvaltningsrevisjonen.

Ettersom det ikke er fremlagt rutiner for inngåelse og oppfølging av databehandleravtaler, og revisjonslaget har fått opplyst at det ikke er gjennomført kontroll av databehandlere, kan revisjonslaget imidlertid ikke bekrefte at kommunen har tilstrekkelige mekanismer på plass for å kvalitetssikre at databehandlere ivaretar krav til personvern ved inngåelse av databehandleravtaler. Dette gjelder spesielt i tilfeller hvor leverandørens mal benyttes.

Marker kommune har i liten grad kartlagt overføring av personopplysninger til land utenfor EU/EØS og gjennomført nødvendige vurderinger og tiltak ved overføringer	Oransje

Revisjonslaget vurderer at Marker kommune i liten grad har kartlagt overføring av personopplysninger til land utenfor EU/EØS og gjennomført nødvendige vurderinger og tiltak ved overføringer.

Revisjonslaget vurderer at Marker kommune har etablert en mulighet for å beskrive eventuelle overføringer av personopplysninger til land utenfor EU/EØS i behandlingsprotokollen. Selv om det fremgår av både behandlingsprotokollen og informasjon fra intervjuer at kommunen ikke overfører personopplysninger til land utenfor EU/EØS, viser imidlertid systemoversikt i Samsvar at kommunen benytter den globale skyleverandøren Microsoft. Gjennom databehandleravtalen med sine kunder forbeholder Microsoft seg retten til å overføre personopplysninger til alle land hvor selskapet eller deres underleverandører driver virksomhet. Revisjonslaget vurderer derfor at bruk av Microsofts tjenester innebærer en risiko for at personopplysninger kan overføres til tredjeland. Dette kan eksempelvis skje ved supporthenvendelser på plattformen i forbindelse med hastesaker utenfor vanlig arbeidstid ("follow the sun"-prinsippet) eller ved behov for eksperthjelp fra lokasjoner utenfor EU/EØS.

Dette indikerer at kommunen ikke har gjennomført en tilstrekkelig kartlegging av mulige overføringer av personopplysninger til tredjeland. Revisjonslaget har imidlertid ikke kontrollert geografisk lokasjon hos kommunens øvrige databehandlere. Revisjonslaget har heller ikke kontrollert dataflyt i forbindelse med bruk av databehandlere. Videre finner revisjonslaget ingen dokumentasjon som viser at Marker kommune har iverksatt nødvendige tiltak for å håndtere slike overføringer på en lovmessig forsvarlig måte.

Marker kommune har utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39	Mørke-grønn

Revisjonslaget vurderer at Marker kommune har utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GPDR artikkel 37-39. Selv om personvernombudet er engasjert i flere relevante personvernaktiviteter i kommunen, har revisjonslaget identifisert et forbedringspotensial når det gjelder etablering av rutiner for ansatte om hvordan personvernombudet kan benyttes, for å sikre at ombudets rolle utnyttes fullt ut.

Revisjonslaget ønsker til sist å bemerke at den fremlagte avtalen med personvernombudet gjelder for to år «fra 01.03.2018», noe som kan indikere at avtalen med personvernombudet ikke formelt er oppdatert.

Marker kommune har i noen grad sørget for at avvik knyttet til personvern blir meldt, registrert og håndtert	Gul

Revisjonslaget vurderer at Marker kommune i noen grad har sørget for at avvik knyttet til personvern blir meldt, registrert og håndtert.

Revisjonslaget vurderer at Marker kommune har etablert et avvikssystem i TQM. Systemet ble i intervjuer beskrevet som enkelt å bruke. Revisjonslaget finner det likevel ikke dokumentert at kommunen har etablert nærmere beskrivelser eller skriftlige rutiner for rapportering, registrering og oppfølging av avvik. Dette omfatter også dokumentasjon som sikrer at rapporteringspliktige avvik meldes til Datatilsynet eller at underretningsplikten til de registrerte overholdes.

Stikkprøvene revisjonslaget gjennomførte i TQM viste at det ikke er registrert noen personvernavvik i avvikssystemet de siste fem årene. Dette kan indikere at kommunen ikke har hatt personvernavvik. Dette kan også indikere en underrapportering av personvernavvik i kommunen. Når dette ses i sammenheng med svarene fra spørreundersøkelsen, der 45,8% av respondentene oppga at de ikke er kjent med hvordan de rapporterer personvernavvik, vurderer revisjonslaget at det er et vesentlig forbedringspotensial knyttet til å sikre at ansatte er kjent med hva et personvernavvik utgjør, samt hvordan slike avvik skal rapporteres, registreres og håndteres.

4.4 Konklusjon og anbefalinger

Revisjonslaget vurderer at Marker kommune har etablert flere hensiktsmessige tiltak for å sikre at kommunen etterlever kravene i personopplysningsloven og GDPR. Kommunen har, til tross for kommunens størrelse, etablert et internkontrollsystem for personvern som består av styrende, gjennomførende og kontrollerende elementer i tråd med veiledning fra Datatilsynet.

Revisjonslaget har likevel identifisert flere krav som ikke er ivaretatt på en tilfredsstillende måte. Dette gjelder i hovedsak omfang og innhold i rutiner og retningslinjer. Mens kommunens rutiner og retningslinjer ikke dekker alle områdene som er anbefalt i Datatilsynets veiledning om hvordan kravet til internkontroll etter GDPR artikkel 24 skal forstås, er det revisjonslagets vurdering at kommunen har et mindre omfang av rutiner, retningslinjer og arbeidsinstrukser for personvern, enn forventet. Revisjonslaget mener at rutiner og retningslinjer, samt konkretisering av roller og ansvar for gjennomføring av personvernaktiviteter, er det området der Marker kommunes internkontroll har størst potensial for forbedring.

Videre mener revisjonslaget at kommunen har potensial for forbedring når det gjelder fastsetting av slettefrister og etablering av sletterutiner, etablering av rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter, etablering av rutiner for å sørge for kontroll av at databehandlere ivaretar krav til personvern, og kartlegging av overføringer av personopplysninger til land utenfor EU/EØS.

Basert på våre vurderinger og konklusjon anbefaler vi at Marker kommune bør:

a) Utarbeide en oversikt over alle rutiner og retningslinjer for vern av personopplysninger i kommunen, samt dokumentere hvordan internkontrollsystemet henger sammen. Videre bør kommunen oppdatere malene for risikovurdering slik at de inkluderer muligheten for å vurdere hvilke konsekvenser identifiserte risikoer kan ha for enkeltpersoners rettigheter, i samsvar med GDPR artikkel 24 og 32. Kommunen bør også gjennomføre oppdaterte risikovurderinger på personvernområdet der formålet er å identifisere ytterligere behov for skriftlige rutiner og retningslinjer for håndtering av personopplysninger.

b) Videre bør kommunen oppdatere styrende dokumenter for å inkludere detaljerte beskrivelser av ansvar og roller for personvernoppgaver. Dette inkluderer å sikre at nøkkelpersoner og virksomhetsledere har en klar forståelse av sine roller og ansvar innen personvern. Kommunen bør også sørge for regelmessig og rollebasert opplæring innen personvern. Dette inkluderer å sikre at alle ansatte får tilstrekkelig opplæring i personvernprinsipper, kommunens retningslinjer og sentrale krav i GDPR. Etablering av et personvernteam kan bidra positivt til dette arbeidet.

c) Sørge for at alle felter i behandlingsprotokollen fylles ut med nøyaktige og relevante opplysninger. For eksempel, under feltet «Mottakere av personopplysninger», bør det spesifiseres hvem som mottar opplysningene, i stedet for å angi at opplysningene ikke overføres til tredjeland. Tilsvarende bør feltet «Sletting og lagring» inneholde konkrete opplysninger om sletting og lagring av data, i stedet for å nevne at det ikke er automatiske avgjørelser i behandlingen. Kommunen bør også tydelig dokumentere hvem som har ansvar for å fylle ut og oppdatere behandlingsprotokollen.

d) Etablere klare og spesifikke sletterutiner for sin behandling av personopplysninger. Dette innebærer å utarbeide skriftlige rutiner for sletting og lagring av data for hver behandlingsaktivitet. Hvilke sletterutiner som gjelder, bør dokumenteres i kommunens behandlingsprotokoll.

e) Oppdatere personvernerklæringene slik at de inneholder identitet og kontaktinformasjon til den behandlingsansvarlige, samt kontaktopplysningene til personvernombudet, i samsvar med GDPR artikkel 13 nr. 1 a og b. Kommunen bør også sørge for at formålet med behandlingen beskrives så tydelig som mulig. Videre bør kommunen også sikre at informasjonen i personvernerklæringene samsvarer med overskriftene de er plassert under. Dette kan oppnås ved å gjennomgå og revidere erklæringene for å sikre at informasjonen er korrekt plassert og lett forståelig. Til sist bør kommunen sikre at alle ansatte er kjent med hvordan deres personopplysninger behandles. Dette kan for eksempel gjennomføres gjennom opplæringsprogrammer.

f) Etablere skriftlige rutiner for hvordan kommunen skal håndtere forespørsler fra de registrerte om å utøve sine rettigheter etter GDPR. Rutinene bør beskrive hvordan forespørsler fra registrerte om å utøve sine rettigheter etter GDPR skal mottas, behandles og besvares innen fastsatte frister, med klare ansvarsfordelinger, dokumentasjon og rutiner for verifisering av identitet.

g) Etablere skriftlige rutiner for når personvernkonsekvensvurderinger skal gjennomføres. Rutinene bør beskrive hvem som er ansvarlig for å gjennomføre vurderingene, hvilket malverk som skal benyttes, når personvernombudet skal involveres og når forhåndsdrøfting med Datatilsynet skal finne sted. Kommunen bør også vurdere å oppdatere malen for personvernkonsekvensvurdering med flere hjelpetekster. Dette vil gi brukerne bedre veiledning om hva de skal beskrive i hver del av vurderingen, og sikre at alle nødvendige elementer blir dekket.

h) Etablere skriftlige rutiner for inngåelse og oppfølging av databehandleravtaler, med det formål å sikre at alle avtaler, enten basert på kommunens eller leverandørens mal, oppfyller kravene i GDPR artikkel 28. Rutinen bør inkludere tydelige roller og ansvar, krav om risikovurdering av leverandør før avtaleinngåelse, en kvalitetssikringsprosess ved bruk av leverandørens avtale med klar ansvarsfordeling for eventuell godkjenning, samt rutiner for oppdatering og fornyelse av avtalene ved behov. I tillegg bør kommunen etablere en prosess for regelmessig kontroll og revisjon av databehandlere, inkludert periodiske gjennomganger for å sikre at databehandlere etterlever avtalene og ivaretar krav til personvern.

i) Gjennomføre en grundig kartlegging av alle mulige overføringer av personopplysninger til tredjeland. Dette inkluderer å identifisere alle databehandlere og underleverandører som kan ha tilgang til personopplysninger utenfor EU/EØS.

j) Etablere skriftlige rutiner for rapportering, registrering og oppfølging av avvik. Dette inkluderer å sikre at alle ansatte er kjent med hva et personvernavvik utgjør, samt etablere beskrivelser av hvordan slike avvik skal rapporteres og håndteres. Videre bør kommunen gjennomføre opplæring og bevisstgjøringsaktiviteter for alle ansatte for å øke kompetansen om personvernavvik. For å sikre at alle rapporteringspliktige avvik meldes til Datatilsynet og at underretningsplikten til de registrerte overholdes, bør kommunen etablere en rutine for regelmessig gjennomgang og oppdatering av avvikssystemet.

5 KILDER OG LITTERATUR

Intervjuobjekter

- Stig Arne Holtedahl – Kommunedirektør
- Vidar Østenby – Virksomhetsleder teknikk og samfunn/beredskap og innbyggerdialog
- Anne-Kari Grimsrud – Virksomhetsleder økonomi
- Marianne Hermanseter – Virksomhetsleder HR/organisasjon
- Line Andersen – Virksomhetsleder oppvekst
- Øystein Ramdal – Virksomhetsleder helse og velferd
- Ellen Bunes – Ansvar for arkivet
- Dan-Ove Moberget – Ansvarlig for IKT
- Torbjørn Sjølstad – Personvernombud
- Ingrid Nøstvedt – Fagsykepleier, systemansvarlig TQM

Dokumentasjon fra Marker kommune

- Avtale IT-drift Marker kommune 2024-07-02
- Avtale med personvernombud (L)(28186)
- avtalePersonvernombud
- Bilag 11 Marker databehandleravtale_bilag_2020
- Bilag 11 Marker databehandleravtale_generell_avtaletekst_2020
- Brudd på personopplysningssikkerheten Marker kommune
- Brudd på personopplysningssikkerheten(1)(1)
- Databehandleravtale startlån
- DPIA-digisos
- Etiske retningslinjer, endelig versjon (L)(60434)
- Helhetlig ROS Marker_05.07.24
- Informasjon og kommunikasjonsstrategi – (L)(52152)
- Innledning
- Innsamling og bruk av personopplysninger, Marker kommune – Personvernerklæring
- Innsynsrett Marker kommune
- Innsynsrett(1)
- Mål for personvernarbeidet i Marker kommune
- Marker kommune – revidert Sikkerhetshåndbok mars 2024 (002)
- Marker kommune Rapport fra sikkerhetsvurdering februar 2024
- Personoppl i Marker kommune ny – GDPDR
- Personvern på arbeidsplassen(1)
- Personvern på arbeidsplassen(2)
- Politisk organisasjonskart 2024
- Protokoll_08-08-2024_09-36-23
- Samtykkeerklæring foto og film
- Samtykkeskjema fotografering
- Samtykkeskjema tverrfaglig samarbeid
- Samtykkeskjema_ny
- Signeringsfil
- Sikkerhet, datasikkerhet og personvern i Marker kommune
- 2020-07-03 – Støtteprodukter NSMs grunnprinsipper for IKT-sikkerhet
- Avtale Netsecurity SOC Marker Kommune

- Custom Publish Databehandleravtale Marker kommune
- Databehandleravtale AcosWebsak
- Databehandleravtale Marker – Procon
- DPIA- Digi helse – Marker kommune
- DPIA
- DPIA-barnehage
- DPIA-legekontor
- Marker kommune – Presentasjon 14.. februar 2024 – justert
- Marker kommune Rapport fra sikkerhetsvurdering februar 2024 (1)
- Protokoll_hjemmesykepleie
- Protokoll_Ikt avhending
- Protokoll_landbruksveg
- Protokoll_Ledsagerbevis
- Rayvn_databehandleravtale_signert
- ROS-analyse-ASPIT
- ROS-analyse-barnehage
- ROS-analyse-barnevern
- ROS-analyse-digisos
- ROS-analyse-felles tennant med skole
- ROS-analyse-hjemmekontor
- ROS-analyse-IKT
- ROS-analyse-legekontor
- ROS-analyse-Økonomikontoret
- ROS-analyse-vidkas
- ROS-analyse-MBSS
- ROS-analyse-skytjenester

Stikkprøver

- Stikkprøve av etablerte rutiner og retningslinjer i TQM
- Stikkprøve av behandlingsprotokollen i Samsvar
- Stikkprøve av 2 avvik i avvikssystemet i TQM

6 VEDLEGG

6.1 Kommunedirektørens uttalelse

Revisjonen mottok kommunedirektørens uttalelse per epost 06.11.2024:

«Vi har nyttiggjort oss de funnene som er gjort, og vil følge opp rapportens innhold videre.»