KPMG

Informasjons-sikkerhet & personvern

Sluttrapport fra undersøkelsen

Innholdsfortegnelse

1 Sammendrag

Møre og Romsdal fylkeskommune er en stor virksomhet med viktige samfunnsoppdrag. For å sikre at fylkeskommunen er i stand til å oppfylle interne og eksterne forventninger forbundet med samfunnsoppdragene, er det avgjørende at fylkeskommunen har kontroll på informasjonssikkerhet og behandling av personopplysninger.

Kontrollutvalget i Møre og Romsdal fylkeskommune engasjerte i september 2021 KPMG til å gjennomføre en undersøkelse av informasjonssikkerhet og personvern. Prosjektets hovedformål har vært å undersøke om fylkeskommunen har tilfredsstillende interkontroll, og om etablerte standarder og gjeldende lover og regler er fulgt.

Det har også vært et mål å undersøke fylkeskommunens sikring av konfidensielle opplysninger, og om fylkeskommunen etterlever sentrale krav i personopplysningsloven og personvernforordningen. Bestillingen fra fylkeskommunen er å undersøke fem hovedproblemstillinger:

1. Har fylkeskommunen etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet og personvern?
2. I hvilken grad er ansvar og oppgaver knyttet til informasjonssikkerhet og personvern tydeliggjort, plassert og forstått?
3. I hvilken grad innehar fylkeskommunen nødvendig kompetanse og kapasitet for en tilstrekkelig internkontroll vedrørende informasjonssikkerhet og personvern?
4. I hvilken grad har fylkeskommunen fulgt myndighetenes anbefalinger for å bygge robusthet mot digitale trusler?
5. I hvilken grad etterlever fylkeskommunen sentrale krav i personvernlovgivningen?

KPMG har benyttet et utvalg av god praksis-kriterier som vurderingsgrunnlag for å evaluere hvordan fylkeskommunen står i forhold til disse, bla. er det lagt til grunn sentrale elementer fra ISO/IEC 27001, NSMs grunnprinsipper for IKT-sikkerhet v. 2.0, og sentrale bestemmelser i personvernforordningen (GDPR).

KPMG overordnede vurdering er at selv om fylkeskommunen har på plass viktige funksjoner og kapabiliteter, så mangler det sentrale risikostyringsperspektivet som styring av fagområdene informasjonssikkerhet og personvern baserer seg på. Det er også behov for en revisjon av sentrale dokumenter, samt operasjonalisering og etterlevelse av krav.

De tekniske aspektene ved fylkeskommunens robusthet mot digitale trusler er jevnt over på et tilstrekkelig nivå, men det er identifisert enkelte forbedringsområder. Det er identifisert mangler ved fylkeskommunens planverk for krise- og kontinuitet for IKT som kan medføre utfordringer ved håndtering av større sikkerhetsbrudd.

Dette sammenfaller også med KPMGs undersøkelse av virksomhetsstyring og internkontroll i fylkeskommunen fra 2021. Her ble det påpekt at fylkeskommunen blant annet hadde behov for å innføre en mer formalisert, systematisk og risikobasert styring og internkontroll.

Fylkeskommunen jobber for tiden med å forbedre sin generelle styring og internkontroll. Om fylkeskommunen lykkes i dette arbeidet vil forutsetningene også bedres for heve arbeidet med informasjonssikkerhet og personvern.

HOVEDOBSERVASJON 1

Fylkeskommunen har etablert et styringssystem for informasjonssikkerhet og personvern, men det etterleves i liten grad

Fylkeskommunen har etablert et styringssystem for informasjonssikkerhet som inneholder sentrale elementer av hva et styringssystem bør inneholde. Styringssystemet har definert og spesifisert mål, strategi, og styrende dokumenter for arbeidet med informasjonssikkerhet i fylkeskommunen. Fylkeskommunen har også definert roller og tilordnet ansvar.

Ut fra foreliggende dokumentasjon fremstår imidlertid implementeringen og operasjonaliseringen av fylkeskommunens styringssystem som mangelfull. Ledelsen har ikke i tilstrekkelig grad fulgt opp at styringssystemet implementeres og etterleves i fylkeskommunen, blant annet ved å følge opp status på implementering eller ved gjennomføring av ledelsen gjennomgang.

Fylkeskommunen har ikke gjennomført sentrale aktiviteter for å vurdere om styringssystemet fungerer i tråd med hensikten, herunder slik som egenkontroll, revisjoner og øvelser. Dette er avgjørende for å kunne si om styringssystemet virker som tiltenkt og oppnår ønskede effekter og mål.

Undersøkelsen har også avdekket mangler forbundet med fylkeskommunens risikostyring, hvor de definerte prosessene ikke i tilstrekkelig grad fremstår operasjonalisert og implementert. Det gjennomføres risikovurderinger, men ikke i alle tilfeller hvor dette skal gjennomføres. Videre er det heller ikke i tilstrekkelig grad bestemt hvem som kan akseptere risiko.

Det er startet opp flere initiativer i fylkeskommunen som samlet vil kunne bedre ledelsens involvering og eierskap til arbeidet med informasjonssikkerhet og personvern. Herunder siktes det særlig til program for nye digitale arbeidsformer, og det pågående arbeidet med å bedre virksomhetsstyring og internkontroll.

For å forbedre situasjonen mener KPMG det vil være viktig å prioritere arbeid med implementering og oppfølging av egenkontroll, revisjoner, og øvelser, samt å sikre gjennomføring av ledelsens gjennomgang. Dette gjelder både for å kunne si om styringssystemet fungerer etter hensikten og for å sikre forankring. Det vil også være viktig å prioritere arbeid med risikostyring, og sikre at risikovurderinger gjennomføres når dette er påkrevd.

HOVEDOBSERVASJON 2

Fylkeskommunen har definert og plassert roller i arbeidet med informasjonssikkerhet og personvern, men rollene er ikke i tilstrekkelig grad spesifisert

Ut fra de gjennomførte undersøkelser så har fylkeskommunen definert sentrale roller i arbeidet med informasjonssikkerhet og personvern. Roller er plassert, men det fremstår som om det er varierende grad av bevissthet rundt rollenes innhold og kjennskap til ansvaret som ligger til rollene.

Enkelte roller, for eksempel sikkerhetsansvarlig og personvernkoordinator, er kortfattet beskrevet, og det fremgår ikke tydelig hva som ligger i de ulike rollene. Ansvarslinjer, rapportering, kontroll og godkjenning, er ikke tilstrekkelig tydelig beskrevet, og det er heller ikke grensegangene mellom de ulike rollene.

Det er i liten grad definert prosesser for koordinering, samarbeid og ansvarsfordeling mellom sikkerhetsansvarlig og personvernkoordinator. Det er heller ikke beskrevet hvordan rollen som personvernkoordinator skal utføres, og hvilken involvering og kapasitet det

krever. Faggruppens mandat, ansvar og oppgaver fremstår uklart ut fra beskrivelsene i styringssystemet og basert på informasjon fra intervju.

Fylkeskommunen bør etter KPMGs syn tydeliggjøre rollebeskrivelser og kommunisere dette til rolleinnehavere på en egnet måte for å redusere risiko for at oppgaver faller mellom to stoler og dermed ikke blir utført. Det bør utarbeides tydelige rollebeskrivelser og instrukser for å sikre at oppgaver, roller og ansvar i tilstrekkelig grad er forstått av rolleinnehavere.

HOVEDOBSERVASJON 3

Fylkeskommunen har god kompetanse hos sentrale sikkerhetsfunksjoner, men arbeider for lite systematisk med kompetanse i organisasjonen og har kapasitets-utfordringer for sentrale roller

Fylkeskommunen har etablert en rutine som definerer et minimumsnivå for kompetanse innenfor personvern og informasjonssikkerhet. Det gjennomføres videre e-læringskurs der tema er informasjonssikkerhet og personvern. Ut fra undersøkelsen fremstår likevel ikke fylkeskommunens arbeid med kompetanse som systematisk.

Innenfor sentrale sikkerhetsfunksjoner er det ikke gjennomført kartlegging av kompetanse-behov, og særlig for faggruppe for informasjonssikkerhet fremstår det klart at det vil måtte gis opplæring dersom faggruppen skal fungere i tråd med sin hensikt. Fylkeskommunen har ikke utarbeidet kompetanseoversikt eller vurderinger av kompetansebehov. Fylkeskommunen arbeider med å øke systematisering av kompetanse i det pågående prosjektet om kompetansestyring.

Med hensyn til kapasitet, er det indikasjoner på at fylkeskommunen har dedikert for lite ressurser til arbeidet med informasjonssikkerhet og personvern. En stor andel av belastningen, og også ansvaret for å gjennomføre styringssystemet i fylkeskommunen, har falt på enkeltpersoner som også har annet ansvar. Dette kommer til syne ved at en del oppgaver og aktiviteter som er beskrevet i styringssystemet har blitt nedprioritert.

Fylkeskommunen bør sikre at informasjonssikkerhet og personvern inkluderes i fylkeskommunens prosjekt for etablering av kompetansestyring, og gjennomføre kartlegginger av kompetansebehov på ulike nivå av organisasjonen innenfor informasjonssikkerhet og personvern. KPMG anbefaler også at det settes av tilstrekkelig tid og ressurser for å sikre at sentrale sikkerhetsfunksjoner kan opparbeide og opprettholde et tilstrekkelig kompetansenivå.

HOVEDOBSERVASJON 4

Fylkeskommunen har et godt grunnivå for robusthet mot digitale trusler, men det er identifisert mangler på spesielt krise- og kontinuitetsplanverk for IKT som kan ha konsekvenser for evne til å håndtere en større sikkerhetshendelse.

Fylkeskommunen har en IT-infrastruktur som ikke skiller seg negativt ut sammenlignet med andre organisasjoner. Det er etablert et godt basisnivå som gir et fundament av robusthet mot digitale trusler. Det er enkelte tiltak fylkeskommunen bør se på som er nevnt i kapitlene nedenfor. På den tekniske siden trekkes det spesielt frem at fylkeskommunen med fordel kan vurdere utvalgte tiltak for å herde klientplattformen, f.eks. hvitelisting av tillatt programvare og fjerning av ikke-essensiell programvare og funksjonalitet på standard-plattformen.

Tilsvarende som for flere av de andre observasjonene, så er også fylkeskommunens robusthet mot digitale trusler farget av en manglende overordnet struktur og tilnærming til

risikostyring og kravspesifikasjon av sikkerhet. Selv om fylkeskommunen gjør mye bra i praksis, så er det gjennomgående mangler i form av utdaterte eller ikke-eksisterende dokumentasjon av sentrale IT-prosesser. Spesielt er det identifisert mangler i planverk for krise og kontinuitetsberedskap som kan ha potensielt store konsekvenser ved håndtering av en sikkerhetshendelse.

Kritiske avvik må lukkes, og det bør gjøres en vurdering av implementering av øvrige anbefalte tiltak. Det er mye utdatert og manglende dokumentasjon og prosesser som må utbedres, spesielt innenfor planverk for krise- og kontinuitet. Det anbefales at fylkeskommunen ser på hvordan risikostyring kan benyttes for å understøtte et gjennomtenkt, dokumentert og konsistent sikkerhetsnivå.

HOVEDOBSERVASJON 5

> *Fylkeskommunen har implementert en rekke sentrale krav for personvern på overordnet nivå, men har ikke i tilstrekkelig grad operasjonalisert arbeidet med personvern på en måte som sikrer etterlevelse.*

Fylkeskommunen har på et overordnet nivå etablert rutiner som er ment å sikre ivaretakelse av personvernforordningen. Ut fra undersøkelsen er inntrykket at disse rutinene ikke i tilstrekkelig grad er operasjonalisert og gjennomført i organisasjonen.

Det er avdekket at fylkeskommunen ikke i tilstrekkelig grad kan dokumentere etterlevelse av de grunnleggende prinsippene for behandling av personopplysninger, herunder med hensyn til prinsippet om lovlighet, åpenhet og rettferdighet, samt prinsippet om lagringsbegrensning.

Fylkeskommunen gir ikke tilstrekkelig informasjon til de registrerte om sine behandlinger. Dette gjelder både eksternt, og internt for egne ansatte. Det er kjente mangler ved personvernerklæringen som ikke er rettet, og det gis generelt for lite informasjon om fylkeskommunens behandling av personopplysninger på innsamlingstidspunktet.

Fylkeskommunen har ikke gjennomført risikovurderinger for alle sine behandlinger, og det er ikke gjennomført vurderinger av personvernkonsekvenser (DPIA) selv om fylkeskommunen har identifisert behandlingsaktiviteter som kan innebære høy risiko for personvernet.

Fylkeskommunen har et personvernombud, men undersøkelsen viser klare svakheter med dagens organisering. Dette gjelder særlig mht. ombudets tilgang til ledelsen og informasjon, samt involvering av personvernombudet.

Fylkeskommunen har ikke gjennomført kartlegginger av sine potensielle overføringer av personopplysninger til tredjeland, og dermed heller ikke identifisert overføringsgrunnlag, eller gjennomført tiltak i de tilfellene der det kan være behov for dette for å sikre et tilsvarende beskyttelsesnivå som innenfor EU/EØS.

KPMG anbefaler at fylkeskommunen prioriterer arbeidet med å kunne påvise overholdelse av de grunnleggende personvernprinsippene, eksempelvis mht. informasjon til de registrerte og at personopplysninger ikke lagres lenger enn det som er nødvendig til formålene de behandles for.

Fylkeskommunen bør også sikre at krav som stilles til databehandlere og IT-løsninger er basert på en vurdering av risiko og personvernkonsekvenser, og at databehandlere følges opp på en systematisk måte. KPMG anbefaler i tillegg at personvernombud sikres tilstrekkelig tilgang til informasjon slik at det kan utføre sine oppgaver. Det bør også sikres at ombudet har tilstrekkelig tilgang til fylkeskommunens ledelse.

2 Innledning

2.1 Bakgrunn

Fylkestinget i Møre og Romsdal fylkeskommune vedtok i juni 2020 at kontrollutvalget skal gjennomføre en undersøkelse av informasjonssikkerheten i fylkeskommunen, og av fylkeskommunen sin etterlevelse av personvernreglementet.

Følgende forhold utgjør bakgrunnen for undersøkelsen:

- ✓ Kontrollutvalget gjennomførte i 2018 en forenklet undersøkelse på området, hvor det ble avdekket at tilpasningen til personvernregelverket ikke var fullført og at behandlingsaktiviteter ikke var fullstendig.
- ✓ Datatilsynet har vedtatt flere overtredelsesgebyrer rettet mot norske kommuner for brudd på personvernforordningen.
- ✓ Det digitale trusselbildet for kommuner og fylkeskommuner er økende, som vist i rapporter fra kommune CSIRT og hendelser som i Østre-Toten kommune.
- ✓ Fylkeskommunen har innført Microsoft 365 som felles samhandlingsplattform og arbeider med diverse prosjekter knyttet til nye digitale arbeidsformer, noe som kan medføre økt sårbarhet knyttet til informasjonssikkerheten.
- ✓ Fylkeskommunen har etablert nye system/prinsipper for klassifisering/sikring av konfidensiell informasjon i Microsoft 365.

Kontrollutvalget ønsker gjennom denne undersøkelsen å være proaktive og bidra til å redusere risikoen for uønskede hendelser i fylkeskommunen. Viktige mål med undesøkelsen er derfor å avdekke eventuelle sårbarheter og gi tydelige innspill til kvalitetsforbedrende og forebyggende tiltak.

Undersøkelsen av informasjonssikkerhet og personvern i fylkeskommunen må sees i sammenheng med undersøkelsen av virksomhetsstyring og internkontroll, som KPMG gjennomførte på oppdrag for kontrollutvalget i 2020-2021. Mens sistnevnte undersøkelse i hovedsak tok for seg den overordnede styringen og internkontrollen i fylkeskommunen, er undersøkelsen av informasjonssikkerhet og personvern konsentrert om disse områdene. Konklusjonene i forrige undersøkelse var blant annet at fylkeskommunen i liten grad hadde etablert en forsvarlig tilfredsstillende internkontroll, som er systematisk, risikobasert og formalisert.

Det ble samtidig påpekt at det er igangsatt flere gode initiativer i fylkeskommunen for å forbedre virksomhetsstyringen og internkontrollen. Av betydning for informasjonssikkerhet og personvern, har Fylkeskommunen iverksatt programmet «Nye digitale arbeidsformer», som er etablert for å svare ut behovene omtalt i organisasjonsstrategien for perioden 2020-2032. Det inngår syv prosjekter i programmet, som i større eller mindre grad omhandler informasjonssikkerhet og personvern. Det ble utarbeidet rapporter for programmet og prosjektene i desember 2021.

2.2 Problemstillinger

Denne undersøkelsen søker å svare ut problemstillingene som utgjorde utgangspunktet og rammene for undersøkelsen. Kontrollutvalget har oppstilt følgende fem hovedproblemstillinger:

1. Har fylkeskommunen etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet og personvern?
2. I hvilken grad er ansvar og oppgaver knyttet til informasjonssikkerhet og personvern tydeliggjort, plassert og forstått?
3. I hvilken grad innehar fylkeskommunen nødvendig kompetanse og kapasitet for en tilstrekkelig internkontroll vedrørende informasjonssikkerhet og personvern?
4. I hvilken grad har fylkeskommunen fulgt myndighetenes anbefalinger for å bygge robusthet mot digitale trusler?
5. I hvilken grad etterlever fylkeskommunen sentrale krav i personvernlovgivningen?

2.3 Rapportens videre oppbygging

Rapporten er videre inndelt i tre. I dette andre kapitlet beskriver vi metodene vi har benyttet for å besvare de fem problemstillingene, og vårt rammeverk for undersøkelser av informasjonssikkerhet og personvern. I kapittel 3 belyser vi undersøkelsens problemstillinger. I kapittel 4 presenterer vi våre anbefalinger.

2.4 Metode

For å besvare de fem problemstillingene har KPMG valgt en metodisk tilnærming basert på:

- ✓ Dokumentanalyse
- ✓ Arbeidsmøter
- ✓ Intervjuer
- ✓ Sikkerhetstester
- ✓ Dialogmøter med fylkeskommunen

Det er gjennomført en dokumentanalyse av fylkeskommunens interne dokumenter. Disse omfatter blant annet styrende dokumenter knyttet til informasjonssikkerhet og personvern, rapporter fra programmet «Nye digitale arbeidsformer» og dokumentasjon fra ulike fag- og tjenesteområder. En fullstendig oversikt over dokumentgrunnlaget framkommer av vedlegg 2.

Det er gjennomført en workshop med sentrale ressurser i fylkeskommunen knyttet til informasjonssikkerhet og personvern. Formålet med workshopen var å identifisere de mest vesentlige risikoområdene i fylkeskommunen.

Det er gjennomført intervjuer med ledere og ansatte i fylkeskommunen, herunder fra:

- ✓ Fylkeskommunedirektørens ledergruppe
- ✓ Stab for strategi og styring
- ✓ Stab for organisasjon og tjenesteutvikling
- ✓ Stab for juridiske og administrative tjenester
- ✓ Kompetanse- og næringsområdet

- ✓ Tannhelsetjenesten
- ✓ Samferdselsområdet
- ✓ IT-seksjonen
- ✓ Innkjøpsseksjonen
- ✓ HR
- ✓ Faggruppe informasjonssikkerhet
- ✓ Programmet «Nye digitale arbeidsformer»

Det er gjennomført sikkerhetstester, for å avdekke om fylkeskommunens arbeid med informasjonssikkerhet fungerer etter sin hensikt i praksis. Utgangspunktet for sikkerhetstestingen har vært å simulere angrepsteknikker som benyttes av trusselaktører for å oppnå uautorisert tilgang til informasjonssystemer. KPMG har gjennomført følgende tester som en del av denne undersøkelsen

- ✓ Phising-angrep – Det er gjennomført et simulert phishing-angrep for å undersøke hvor sårbar fylkeskommunen er for denne typen angrep. Angrepet ble designet i dialog med sentrale ressurser i fylkeskommunen og drøftet med både hovedverneombud og personvernombud.
- ✓ Penetrasjonstest - Formålet med testen var å oppdage og verifisere tekniske sårbarheter, samt å utnytte disse til å oppnå uautorisert tilgang til IT-systemer, interne nettverk og/eller sensitiv informasjon. I tillegg til sårbarhetsskanning, manuell rekognosering, søk i åpne kilder og passordgjetting, ble det gjennomført en rekke manuelle målrettede angrepsforsøk mot webapplikasjoner og andre tilgjengelige tjenester.
- ✓ Innsidetest (assumed breach) - Hensikten med innsidetesten var å avdekke skadepotensialet dersom noen skulle klare å bryte seg inn. Det er i denne forbindelse gjennomført intern sårbarhetsanalyse av nettverk og applikasjoner, analyse av muligheter for utnyttelse av sikkerhetshull og eskalering av rettigheter, samt muligheter for spredning til andre enheter og systemer i nettverket.

Det er underveis gjennomført dialogmøter med sentrale ressurser i fylkeskommunen for å verifisere fakta, og for å sikre at observasjoner bygger på et riktig faktisk grunnlag.

Rapporten ble sendt til fylkeskommunen til uttalelse den 20. april 2022, med endelig høringsfrist 11. mai 2022. Fylkeskommunedirektørens uttalelse framgår av kapittel 5.

2.5 Vurderingskriterier

2.5.1 Overordnet

For denne undersøkelsen er følgende rammeverk benyttet som utgangspunkt, og som standard for god praksis innenfor informasjonssikkerhet og personvern:

- ✓ Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet 2.0
- ✓ ISO/IEC 27001, ledelsessystem for informasjonssikkerhet
- ✓ Personopplysningsloven og personvernforordningen (GDPR)

De tre rammeverkene utfyller og supplerer hverandre innenfor de områdene som er dekket av denne undersøkelsen.

2.5.2 ISO/IEC 27001

For å ivareta informasjonssikkerhet og personvern i tråd med god praksis, må det etableres et styringssystem for informasjonssikkerhet. For denne undersøkelsen er det tatt utgangspunkt i standarden ISO/IEC 27001, samt NSMs grunnprinsipper for IKT-sikkerhet 2.0. Standardene inneholder prinsipper for oppbygging, tilpasning, implementering og oppfølging av styringssystem for informasjonssikkerhet.

For at et styringssystem for informasjonssikkerhet skal være i tråd med ISO/IEC 27001, må det på et overordnet nivå

- ✓ Være tilpasset organisasjonens kontekst
- ✓ Ha tilstrekkelig forankring i virksomhetens ledelse
- ✓ Inneholde prinsipper for risikostyring, herunder med tanke på vurdering, identifisering og håndtering av risiko, og ha definerte mål for arbeidet med informasjonssikkerhet
- ✓ Inneholde prinsipper for drift og kontroll
- ✓ Understøttes av tilstrekkelig ressurser og kompetanse på ulike nivå i organisasjonen
- ✓ Inneholde rutiner og prosesser for evaluering av prestasjon, slik som overvåkning, egenkontroll og ledelsens gjennomgang
- ✓ Inneholde etablerte rutiner for forbedring, gjennom avvik og avvikshåndtering og at arbeidet baseres på en tankegang om kontinuerlig forbedring

Hva som må inngå i et styringssystem for informasjonssikkerhet, og hva som ellers følger av alminnelige anerkjente prinsipper for god internkontroll, er i stor grad sammenfallende. Denne undersøkelsen har derfor klare paralleller til KPMGs forrige undersøkelse om virksomhetsstyring og internkontroll. Problemstillingene knyttet til roller og ansvar, samt kompetanse og kapasitet er for denne undersøkelsen oppstilt som egne hoved-problemstillinger. For å unngå dobbeltbehandling, er disse temaene skilt ut og besvares i egne delkapitler.

2.5.3 NSMs grunnprinsipper for IKT-sikkerhet v. 2.0

NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Prinsippene er utarbeidet for å redusere risiko forbundet med cybertrusler, og inneholder en rekke anbefalte tiltak. Prinsippene bygger på følgende fire hovedkategorier, som hver inneholder en rekke grunnprinsipper

- ✓ Identifisere og kartlegge – Virksomheter bør kartlegge styringsstrukturer, ledelsesprioriteringer, leveranser, IKT-systemer og brukere.
- ✓ Beskytte og opprettholde – Ivareta og opprettholde IKT-sikkerhet over tid og ved endringer.
- ✓ Oppdage – Oppdage og fjerne kjente sårbarheter og trusler og etablere sikkerhetsovervåkning.
- ✓ Håndtere og gjenopprette – Håndtere sikkerhetshendelser effektivt.

Alle grunnprinsippene inneholder nærmere beskrivelser av hvilke sikkerhetstiltak som bør gjennomføres. Ivaretakelse av grunnprinsippene er, i likhet med utgangspunktet etter ISO 27001, en kontinuerlig aktivitet. KPMG har for denne undersøkelsen gjennomført en kontroll av fylkeskommunens etterlevelse av grunnprinsippene med tilhørende sikkerhets-tiltak.

2.5.4 Personopplysningsloven og personvernforordningen (GDPR)

Personvernforordningen inneholder en rekke bestemmelser som forutsetter at virksomheter som behandler personopplysninger har etablert god internkontroll. De vurderinger som er gjort av fylkeskommunens styring av informasjonssikkerhet i henhold til ISO 27001 og NSMs grunnprinsipper er derfor også relevant ved vurderingen av om fylkeskommunen har etablert tilstrekkelige mekanismer for å sikre sin behandling av personopplysninger.

Forordningen inneholder også mer detaljerte krav og plikter til den behandlingsansvarlige. Ved utvalg og vurdering av hvilke krav som er de mest sentrale i personvernforordningen, er det særlig sett hen til forordningens bestemmelser om overtredelsesgebyr. KPMG har undersøkt om fylkeskommunen

- ✓ Overholder og kan dokumentere etterlevelse av de grunnleggende prinsippene for behandling av personopplysninger i art. 5
- ✓ Legger til rette for og gir informasjon til de registrerte etter art. 12, 13 og 14
- ✓ Ivaretar sikkerhet ved behandling av personopplysninger, særlig med hensyn til art. 24, 32 og 35
- ✓ Ivaretar prinsippene om innebygd personvern og personvern som standard-innstilling etter art. 25.
- ✓ Overholder sine plikter ved bruk av databehandlere etter art. 28.
- ✓ Har tilstrekkelig oversikt over sin behandling og fører protokoll over behandlings-aktiviteter etter art. 30.
- ✓ Har etablert tilstrekkelig mekanismer for å fange opp avvik og melde til Datatilsynet etter art. 33.
- ✓ Har et personvernombud i tråd med forventningene etter art. 37 til 39.
- ✓ Sikrer at overføring av personopplysninger til tredjeland skjer i tråd med bestemmelsene i forordningens kap. V.

Det er viktig å presisere at KMPG i denne undersøkelsen ikke har kontrollert alle behandlingsaktiviteter i fylkeskommunen opp mot alle de sentrale kravene i forordningen. KPMG har, basert på en risikobasert tilnærming, med utgangspunkt i fylkeskommunens innspill i risikoworkshop, gjort et utvalg av behandlingsaktiviteter der det har vært nødvendig med nærmere undersøkelser. Det har i den forbindelse vært sett på områdene tannhelse, skole og skoleskyss.

3 Analyse

3.1 Internkontrollsystem

Hovedproblemstillingen som adresseres i dette delkapitlet er om fylkeskommunen har etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet og personvern. Utgangspunktet for dette delkapitlet har vært de overordnede krav og forventninger til styringssystem for informasjonssikkerhet etter ISO 27001.

3.1.1 Styringssystemets tilpasning til organisasjonen

Målsetting

Fylkeskommunen har etablert et styringssystem tilpasset interne og eksterne behov og forventninger, og er tilpasset virksomhetens formål.

Observasjoner og vurderinger

Ved vurderingen av om fylkeskommunens styringssystem oppfyller målsettingen, har KPMG sett på om fylkeskommunens styringssystem for personvern og informasjonssikkerhet er tilpasset organisasjonen, og om styringssystemet tar hensyn til interne og eksterne forventninger fra ulike interessenter.

Fylkeskommunen har etablert et styringssystem for informasjonssikkerhet, «Handbok for personvern og informasjonstryggleik», som er basert på «Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren». Normen er utarbeidet av og for virksomheter innenfor helse og omsorgssektoren, og er et rammeverk for internkontroll som på de fleste punkter oppfyller krav og forventninger til hva et styringssystem skal inneholde for å være i tråd med ISO/IEC 27001.

Fylkeskommunen behandler til dels store mengder helseopplysninger, særlig innenfor tannhelsesektoren. Med dette som utgangspunkt fremstår det forsvarlig at fylkeskommunen har basert sitt styringssystem på normen.

Fylkeskommunen har i intervju gitt uttrykk for at de vurderer å revidere «Handbok for informasjonssikkerhet og personvern». I intervju er det også gitt uttrykk for at det ikke er gjennomført særskilte vurderinger av om fylkeskommunens styringssystem bidrar til å understøtte den strategiske retningen i virksomheten.

I lys av fylkeskommunens nye organisasjonsstrategi, og programmet «Nye digitale arbeidsformer», bør fylkeskommunen foreta en vurdering av om styringssystemet i tilstrekkelig grad bidrar til å understøtte strategien og programmet, eller om det er nødvendig å foreta revisjon.

Anbefalinger

- ✓ Fylkeskommunen bør vurdere og revidere styringssystemet sitt for informasjonssikkerhet for å sikre at styringssystemet bidrar til å understøtte organisasjonsstrategien og programmet for nye digitale arbeidsformer. Det bør særlig vurderes om mål og strategi som beskrevet i styringssystemet fortsatt er tilstrekkelige, og om mål

og strategi er i samsvar med og bidrar til å understøtte den nye organisasjons-strategien.

3.1.2 Ledelsesforankring og policy

Målsetting

Ledelsen understøtter arbeidet med informasjonssikkerhet, herunder ved å etablere et styringssystem for informasjonssikkerhet, sørger for at styringssystemet fungerer etter hensikten, har tildelt roller og ansvar, og fremmer kontinuerlig forbedring.

Observasjoner og vurderinger

Ved vurdering av om prinsippet overholdes, har KPMG vurdert om ledelsen har tatt eierskap til, og understøttet arbeidet med implementering av styringssystemet for informasjonssikkerhet, om ledelsen har etablert mekanismer for å sikre at styringssystemet tas i bruk og oppnår tiltenkte resultater, og om ledelsen fremmer kontinuerlig forbedring. Roller og ansvar er behandlet i mer detalj under i pkt. 3.2.

Fylkeskommunens styringssystem for informasjonssikkerhet, «Handbok for personvern og informasjonstryggleik», ble vedtatt av ledelsen 11.05.2020. Styringssystemet inneholder på et overordnet nivå de vesentlige elementer et styringssystem må inneholde, og er inndelt i en styrende, gjennomførende og en kontrollerende del. Det er definert informasjons-sikkerhetsmål og en strategi for å nå disse målene. Styringssystemet er publisert på intranett, og det er gjennomført mer detaljerte gjennomganger av styringssystemet med enkelte grupper ansatte.

Styringssystemet legger også til rette for kontinuerlig forbedring særlig gjennom styrings-systemets kontrollerende del som inneholder rutiner for sikkerhetsrevisjon, risiko-vurdering, avvikshåndtering og ledelsens gjennomgang. Slike sikkerhetsrevisjoner er imidlertid ikke gjennomført, og det er heller ikke ledelsens gjennomgang.

I intervju er det opplyst om at det ikke er etablert noen fast rapportering til ledelsen om informasjonssikkerhet. Det er imidlertid informert om at IT-seksjonen jevnlig oppdaterer hele organisasjonen om viktig informasjon. IT-seksjonen lager også saker til toppleder-gruppen når det er temaer/saker knyttet til informasjonssikkerhet som bør behandles av ledelsen. KPMG har fått oppgitt at slik rapportering til ledelsen har økt i hyppighet den siste tiden.

Ledelsen har også understøttet arbeidet med informasjonssikkerhet og personvern gjennom sin involvering, herunder beslutninger om å etablere og igangsette programmet «Nye digitale arbeidsformer». Inntrykket er at fylkeskommunens ledelse er mer involvert i arbeidet med informasjonssikkerhet og personvern nå enn før, og at involveringen har gått fra å være relativt tilfeldig til mer systematisk. Det gjenstår likevel en del når det kommer til ledelsens involvering og styring, noe fylkeskommunen har pågående prosesser for å forbedre, herunder ved å i større grad integrere informasjonssikkerhet og personvern i virksomhetsstyringen på en systematisk måte.

Det er opplyst om at det utarbeides et årshjul som skal understøtte arbeidet med virksomhetsstyring og internkontroll. Årshjulet spesifiserer hvilke aktiviteter ledelsen planlegger å utføre i løpet av året. Fylkeskommunen bør sikre at sentrale kontrollpunkter for informasjonssikkerhet og personvern inntas og tas hensyn til ved utarbeidelse av årshjulet.

Med hensyn til ledelsesforankring og ledelsens involvering i arbeidet med personvern og informasjonssikkerhet er inntrykket at de fleste initiativer som gjelder informasjonssikkerhet og personvern initieres lenger nede i linjen. KPMG har ikke sett at ledelsen har tatt ansvar for oppfølging av de prinsipper, retningslinjer og rutiner som fremgår av styringssystemet. Det er som tidligere beskrevet ikke etablert fast rapportering til ledelsen, og det gjennomføres heller ikke egenkontroll, revisjoner, øvelser eller ledelsens gjennomgang. Samlet sett tyder dette på at fylkeskommunens ledelse foreløpig ikke har etablert en tilstrekkelig oppfølging av informasjonssikkerhet og personvern.

Anbefalinger

- ✓ Ledelsen i fylkeskommunen bør sikre at styringssystemet for informasjonssikkerhet fungerer, og at det etterleves. Ledelsen bør med jevne mellomrom vurdere om styringssystemet fungerer etter hensikten, og sikre at det gjennomføres egenkontroll, øvelser og revisjoner av styringssystemet.
- ✓ Ledelsen i fylkeskommunen bør etablere faste punkter for rapportering av status for arbeidet med informasjonssikkerhet og personvern for å sikre at ledelsen har tilstrekkelig informasjon om risiko på disse områdene i fylkeskommunen.
- ✓ Fylkeskommunens ledelse bør gjennomføre øvelser for å sikre at tiltak og planer fungerer etter hensikten.
- ✓ For å sikre at styringssystemet også fremstår ledelsesforankret for de ansatte i fylkeskommunen, bør ledelsen jevnlig gi informasjon og retningslinjer for arbeidet med personvern og informasjonssikkerhet for å understøtte og forankre arbeidet som utføres.
- ✓ Ledelsen bør etablere relevante måleparametere for arbeidet med informasjonssikkerhet og personvern som det skal rapporteres på, for å kunne måle utvikling over tid.

3.1.3 Risikostyring

Målsetting

Fylkeskommunen har definert informasjonssikkerhetsmål og har definert en prosess for risikostyring herunder med tanke på håndtering av informasjonssikkerhetsrisiko.

Observasjoner og vurderinger

KPMG har ved vurdering av om dette kravet er oppfylt sett på om fylkeskommunen har etablert en prosess for risikostyring, herunder om det er definert kriterier for risikoaksept, kriterier for når risikovurderinger skal gjennomføres, og definert hvem som kan beslutte tiltak og akseptere restrisiko.

Fylkeskommunen har i sitt styringssystem definert når det skal gjennomføres risikovurderinger. Dette gjelder alltid før en ny behandling av personopplysninger, ved større endringer i eksisterende systemer eller løsninger, ved bytte av leverandører på sentrale tjenester, ved alvorlige avvik og som en del av kontroll og oppfølging. Det er også til en viss grad definert et nivå for akseptabel risiko, ved at risikonivå «rød» krever risikoreduserende tiltak, at det skal vurderes tiltak ved nivå «gul».

Risikovurderinger skal gjennomføres i fylkeskommunens system for risikovurdering og avvikshåndtering «Risk manager». I Risk manager er det lagt inn beskrivelser av de ulike sannsynlighets og konsekvenskategoriene, og det er gitt en tilsvarende beskrivelse av

akseptabelt risikonivå som i styringssystemet. Det er informert om at Risk manager skal byttes ut med et nytt system i løpet av 2022.

Det gjennomføres flere risikovurderinger enn det som fremgår av oversikten i Risk manager. IT-seksjonen gjennomfører forenklede risikovurderinger som et ledd av sin normale drift. Risikovurderinger dokumenteres da i et system som benyttes av ansatte i IT-seksjonen. Dette gjelder særlig ved mindre endringer av eksisterende systemer, slik som oppdateringer, konfigurasjonsendringer, patching etc.

Ut fra oversiktene over gjennomførte risikovurderinger, gjennomfører ikke fylkeskommunen risikovurderinger i alle tilfeller der det i styringssystemet er angitt at slike vurderinger skal skje. Dette gjelder både i forbindelse med endringer av eksisterende systemer, anskaffelse av nye systemer, eller før en ny behandling av personopplysninger. Det er heller ikke dokumentert at gjennomførte risikovurderinger gjennomgås i tråd med de gyldighetsperiodene som er spesifisert i Risk manager, eller ved endringer av for eksempel trusselbilde.

Fylkeskommunen har definert et nivå for akseptabel risiko. Nivå for akseptabel risiko bør imidlertid vurderes med utgangspunkt i hva som utgjør et akseptabelt nivå av risiko for fylkeskommunen. Ut fra klassifiseringen og beskrivelser av kategorier for sannsynlighet og konsekvens, fremstår det ikke klart hvilken risiko fylkeskommunen har definert som akseptabel. Ved vurdering av informasjonssikkerhetsrisiko tas det for eksempel ikke hensyn til hvor høy risiko fylkeskommunen er villig til å akseptere innenfor ulike kategorier slik som økonomi, omdømme, operative evner, liv og helse. En slik kategorisering benyttes ved vurdering av HMS-risiko, men den benyttes ikke ved vurdering av informasjonssikkerhetsrisiko.

I styringssystemet er det ikke definert hvem som kan akseptere informasjonssikkerhetsrisiko eller beslutte tiltak. I intervju er det vist til at dette følger bestemmelser om budsjettdisponeringsmyndighet, og at tiltak kan besluttes i tråd med de økonomiske rammene den enkelte leder må forholde seg til. Investeringer som går ut over den enkelte leders budsjettdisponeringsmyndighet må løftes til ledergruppen, og eventuelt behandles politisk.

De beskrevne prosessene knyttet til beslutning av tiltak, gir ikke veiledning med tanke på hvem som kan akseptere risiko og eventuelt hvor mye risiko den enkelte leder kan akseptere. Slik Risk manager er bygget opp med tanke på arbeidsflyt, er det også bare risikoreduserende tiltak som skal godkjennes av en overordnet. Godkjennende leder får ikke automatisk informasjon om restrisiko ved aksept av tiltak.

I Intervju med fylkeskommunens ledelse ble det uttrykt en forventning om at risikovurderinger er et av temaene som skal løftes for behandling og godkjenning i ledergruppen. Dette skjer imidlertid i praksis utelukkende i tilfeller hvor det anbefales tiltak som av budsjettmessige grunner er påkrevd å løfte til ledelsen.

Fylkeskommunen gjennomførte konsekvensanalyser og overordnet risikovurdering av sin tjenesteportefølje i 2012, men har ikke oppdatert eller gjennomført nye slike vurderinger i etterkant. Verdi/konsekvensvurderinger er viktige å gjennomføre for å forstå hva konsekvensene av eksempelvis bortfall vil være, og for å sikre at sikkerhetsnivået er tilstrekkelig og at tiltak står i sammenheng med konsekvensene for fylkeskommunen eller for brukere av fylkeskommunens tjenester. Det er også viktig for å forstå og kunne sammenligne risiko på tvers av fylkeskommunens tjenesteområder, og av hensyn til prioritering av tiltak. Fylkeskommunen har i intervju oppgitt at de nå er i gang med å gjennomføre verdivurderinger av sin tjeneste- og systemportefølje.

Med utgangspunkt i de risikovurderinger KPMG har undersøkt, er det en viss variasjon i kvalitet. Det oppstilles scenarier, men det er i flere tilfeller ikke vurdert risiko for cyberangrep eller alvorlige digitale hendelser ved vurdering av IT-system. Vurderingene av sannsynlighet og konsekvens er i varierende grad redegjort for, og det fremstår ikke i alle tilfeller klart hvordan risikoreduserende tiltak er egnet til å redusere identifiserte risiko.

Anbefalinger

- ✓ Etablere kontrollmekanismer som sikrer at risikovurderinger gjennomføres i relevante arbeidsprosesser i linjen, for eksempel i tilknytning til anskaffelsesprosesser, hvor det kan inntas i innkjøpsavdelingens rutiner eller sjekklister og kontrolleres at det er gjennomført før konkurranser kunngjøres.
- ✓ Etablere prosesser og rutiner som sikrer at risikovurderinger oppdateres ved større endringer, herunder slik som ved endret/skjerpet trusselbilde og at det sikres at de gjennomgås.
- ✓ Tydeliggjøre og definere hva som utgjør akseptabel risiko for fylkeskommunen.
- ✓ Fylkeskommunen bør gjennomføre verdi/konsekvensvurderinger av sine tjenester, prosesser og systemer, for å vurdere risiko på et overordnet nivå.
- ✓ Fylkeskommunen bør tydeliggjøre hvem som kan akseptere ulike nivå av risiko i organisasjonen, herunder hvem som kan akseptere restrisiko, og hvem som kan beslutte tiltak.

3.1.4 Overvåkning, avvikshåndtering, egenkontroll og ledelsens gjennomgang

Målsetting

Fylkeskommunen har etablerte prosesser for overvåkning, måling, analyse, avviks-håndtering og evaluering, har etablert kontrollmekanismer slik som egenkontroll eller -revisjon, samt definert prosess for ledelsens gjennomgang.

Observasjoner og vurderinger

Undersøkelsen av oppfyllelse av denne målsettingen har særlig tatt for seg hvilke formelle kontrollmekanismer som er etablert, hvordan avvik håndteres og hvordan prosessene etterleves. Når det gjelder teknisk overvåkning og prestasjonsevaluering, er dette adressert under vurderingen av problemstillingen om robusthet mot digitale trusler.

Fylkeskommunen har etablert en prosess for å rapportere inn og vurdere avvik og brudd på informasjonssikkerhet. Avvik skal meldes inn gjennom fylkeskommunens system for avvikshåndtering - Risk manager. Det er oppgitt at ansatte har fått informasjon og opplæring i hva som utgjør avvik og hvordan dette skal håndteres. Fylkeskommunen har dokumentert at det fanges opp og meldes inn avvik og brudd på informasjonssikkerhet. Når avvik meldes inn følges prosessen slik denne er skissert i fylkeskommunens styrings-system.

Etter fylkeskommunens styringssystem skal det gjennomføres revisjon en gang årlig. Fylkeskommunen har utarbeidet et skjema som skal fungere som et utgangspunkt for slike revisjoner. Dette skjemaet tar for seg mange av de samme temaene som er adressert i denne undersøkelsen. Det er ikke gjennomført slik revisjon.

Det er presisert at listen over kontrollpunkter for revisjoner må tilpasses den enkelte sikkerhetsrevisjon. Det fremgår imidlertid ikke av rutinen eller skjemaet som er utarbeidet at tilpasning, og tema for revisjoner, bør velges med utgangspunkt i en vurdering av risiko.

Resultatene fra revisjonen skal etter styringssystemet behandles i ledelsens gjennomgang. Ledelsens gjennomgang skal som et utgangspunkt gjennomføres en gang årlig som en fast ordning, og det er definert hva som skal behandles ved gjennomgangen. Noen slik gjennomgang er ikke gjennomført.

Ut fra foreliggende dokumentasjon, samt informasjon fra intervju, har fylkeskommunen definerte prosesser for overvåkning, måling, analyse og evaluering. Disse etterleves imidlertid foreløpig ikke i praksis. Det gjennomføres ikke revisjoner eller egenkontroll, og det gjennomføres ikke systematisk oppfølging fra ledelsen i form av ledelsens gjennomgang. Etter fylkeskommunens kontinuitetsplan, skal det gjennomføres minst tre tester/øvelser per år, herunder to enkle tester og minst en avansert test. KPMG kan ikke se at dette er gjennomført.

At revisjoner følger en definert sjekkliste, fremstår forsvarlig når fylkeskommunen starter med gjennomføring av sikkerhetsrevisjoner. Slike revisjoner bør imidlertid være risikobaserte og innrettet mot de områdene av virksomheten hvor informasjonssikkerhetsrisikoen er høyest. Uten noen form for kontroll av om styringssystemet fungerer etter hensikten, eller kontroll av om tiltak virker etter hensikten og etterleves, er det vanskelig å si at systemet i praksis ivaretar prinsipper om kontinuerlig forbedring.

Anbefalinger

- ✓ Fylkeskommunen bør gjennomføre årlig revisjon eller egenkontroll for å sikre at implementerte kontroller og sikkerhetsmekanismer fungerer etter hensikten og at fylkeskommunen når målene som er satt for arbeidet med informasjonssikkerhet og personvern. Revisjon og egenkontroll bør være risikobasert og innrettet og fokusert mot områder med høyest risiko. For å tydeliggjøre en slik risikobasert tilnærming, bør beskrivelser av revisjoner i styringssystemet justeres.
- ✓ Fylkeskommunen bør sikre at ledelsens gjennomgang inntas som et fast punkt ved utarbeidelse av årshjul for virksomhetsstyring og internkontroll.
- ✓ Fylkeskommunen bør sette av tilstrekkelig med ressurser til å gjennomføre revisjonene som spesifisert i styringssystemet.
- ✓ Ved oppfølging av risikovurderinger, egenkontroll og revisjon, samt resultater fra ledelsens gjennomgang, bør fylkeskommunen utarbeide handlingsplaner for å sikre at de har tilstrekkelig oversikt og at tiltak prioriteres basert på risiko. Ledelsen i fylkeskommunen bør sikre at slike handlingsplaner følges opp med jevne mellomrom, for eksempel i form av fast statusrapportering, for å sikre at avvik lukkes i tråd med vedtatte frister.

3.1.5 Oppsummering

Hovedproblemstillingen for dette delkapitlet var om fylkeskommunen har etablert et tilfredsstillende internkontrollsystem for informasjonssikkerhet og personvern.

Som beskrevet i de foregående punktene har fylkeskommunen etablert et styringssystem for informasjonssikkerhet. Styringssystemet oppfyller på et overordnet nivå flere av kravene som stilles til internkontrollsystem for informasjonssikkerhet og personvern. Styringssystemet har definert og spesifisert mål, strategi, og rutiner for arbeidet med informasjonssikkerhet i fylkeskommunen.

Ut fra foreliggende dokumentasjon fremstår imidlertid implementeringen og operasjonaliseringen av fylkeskommunens styringssystem for informasjonssikkerhet og personvern som mangelfull. Ledelsen har ikke i tilstrekkelig grad fulgt opp at styringssystemet implementeres og etterleves i fylkeskommunen, blant annet ved å følge opp status på implementering, gjennomføre ledelsens gjennomgang, revisjoner eller øvelser. Det fremstår som det i mindre grad har vært kontrollert at mål, strategier, rutiner og prinsipper som spesifisert i styringssystemet etterleves. Det er imidlertid startet opp flere initiativer i fylkeskommunen som samlet vil kunne bedre ledelsens involvering og eierskap til arbeidet med informasjonssikkerhet og personvern.

Prosess for risikostyring er ikke i tilstrekkelig grad operasjonalisert og implementert i fylkeskommunen. Det gjennomføres risikovurderinger, men ikke i alle tilfeller hvor dette skal gjennomføres etter interne rutiner. Fylkeskommunen har ikke oppdatert sine overordnede verdi- eller konsekvensvurderinger siden 2012, og det er heller ikke etablert vurderinger av nivå for akseptabel risiko. Videre er det heller ikke i tilstrekkelig grad definert hvem som kan akseptere risiko i fylkeskommunen.

3.2 Ansvar og oppgaver

3.2.1 Innledning

For at en virksomhet skal kunne ha et fungerende styringssystem for informasjonssikkerhet, er det avgjørende at ansvar er tydeliggjort, tildelt og forstått. Dette delkapitlet svarer ut problemstilling 2 - «I hvilken grad er ansvar og oppgaver knyttet til informasjonssikkerhet og personvern tydeliggjort, plassert og forstått» i fylkeskommunen.

3.2.2 Ansvar og oppgaver knyttet til informasjonssikkerhet og personvern

Målsetting

Fylkeskommunen har definert roller og tydeliggjort ansvar knyttet til informasjonssikkerhet og personvern. Ansvaret er forstått av rolleinnehavere, som utfører de oppgaver og ivaretar det ansvaret som ligger til rollene.

Observasjoner og vurderinger

Ved vurdering av om forventningene er oppfylt, har KPMG særlig vurdert om sentrale roller er beskrevet, om innholdet i rollen er forstått, og om oppgavene som ligger til rollene utføres.

Ansvar knyttet til informasjonssikkerhet og personvern er beskrevet i fylkeskommunens styringssystem. Fylkeskommunedirektør har det overordnede sikkerhetsansvaret og er behandlingsansvarlig i fylkeskommunen. Behandlingsansvarliges ansvar og oppgaver er definert. Ansvar for utførelsen av oppgavene er delegert til juridiske avdeling og forvaltes av fagleder for informasjonssikkerhet.

Etter fylkeskommunens styringssystem, er leder for hvert fagområde og stabsavdeling sikkerhetsansvarlig («tryggleiksansvarlig») for sin enhet. De har det daglige ansvaret for at enheten sine personopplysninger er tilfredsstillende sikret i tråd med regelverket og handboken. Sikkerhetsansvarlig har videre ansvar for å sette i verk og dokumentere tiltak utover det som er beskrevet i handboken.

Fagleder for informasjonssikkerhet og IT-seksjonen har spesialiserte funksjoner knyttet til informasjonssikkerhet og personvern. Faggruppe informasjonssikkerhet skal koordinere og følge opp oppgavene til sikkerhetsansvarlig. Faggruppen ledes av fagleder for informasjonssikkerhet organisert i juridisk avdeling. Sikkerhetsansvarlig har hver sin representant (personvernkoordinator) i faggruppen. I tillegg deltar lederne for IT-seksjonen og dokumentsenteret. Fylkeskommunen har også utpekt et personvernombud og beskrevet ombudets rolle.

På et overordnet nivå fremstår rollene i arbeidet med informasjonssikkerhet og personvern som definert og tilordnet. Gjennom intervju er det imidlertid gitt uttrykk for at forståelsen av ansvar og roller er uklar i linjen. Dette gjelder særlig med tanke på rollen som sikkerhets-ansvarlig og deltakere i faggruppen for informasjonssikkerhet.

For sikkerhetsansvarlig fremstår ikke innholdet i rolle, ansvar og oppgaver forstått i alle tilfeller. Rollen forveksles tidvis med fagleder informasjonssikkerhet sitt ansvar og oppgaver. Det kommer frem i intervju at ansvar og krav til informasjonssikkerhet og personvern i varierende grad er integrert i oppdragsnotatene i linjen, noe det oppleves at det burde vært. Videre er informasjonssikkerhet og personvern i varierende grad et tema i styringsdialogen i linjen.

Sikkerhetsansvarliges rolle er kortfattet beskrevet, og innebærer ut fra beskrivelsen et hovedansvar innenfor sitt virksomhetsområde til å sikre at personopplysninger er sikret i tråd med styringssystemet og regelverk. Til rollen ligger også ansvar for at sikkerhetstiltak implementeres. Ansvarslinjer, rapportering, kontroll, og godkjenning, fremstår ikke tydelig beskrevet og det gjør heller ikke grensegangen mot andre roller. Tilsvarende gjelder for beskrivelse av oppgavene som ligger til rollen som deltaker i faggruppen for informasjonssikkerhet - personvernkoordinator.

Etter styringssystemet har fylkesutdanningssjefen og fylkestannlegen ansvar for å organisere og etablere rutiner opp mot ytre enheter. Fylkeskommunen har gjennomført en omorganiseringsprosess, noe som gjør at noen funksjoner og beskrivelser i handboken ikke lenger er dekkende. For eksempel har tittelen fylkesutdanningssjef blitt byttet til kompetanse- og næringsdirektør. Dette bør oppdateres for å unngå eventuelle misforståelser.

Faggruppe for informasjonssikkerhet skal koordinere og følge opp oppgavene til sikkerhets-ansvarlig. Det kommer frem i intervju at faggruppen først ble etablert høsten 2021, og at det har blitt gjennomført ett møte i faggruppen der blant annet styringssystemet ble gjennomgått. Ut fra intervju fremstår det som at deltakerne i faggruppe for informasjonssikkerhet opplever uklarhet knyttet til innholdet i rolle og oppgaver. Det er i den forbindelse gitt uttrykk for at ansvaret til koordinatorene for informasjonssikkerhet i faggruppen bør tydeliggjøres.

Det er i liten grad definert prosesser for koordinering, samarbeid og ansvarsfordeling mellom ulike sikkerhetsroller, slik som sikkerhetsansvarlig og personvernkoordinator. Det er også uklart hvordan rollen som personvernkoordinator skal utføres, og hvilken involvering og kapasitet det krever. Faggruppens mandat og ansvarsoppgaver er heller ikke tilstrekkelig spesifisert.

Fylkeskommunen har på et overordnet nivå beskrevet de ulike rollene som skal inngå i det daglige arbeidet med informasjonssikkerhet og personvern, herunder også med tanke på ansvarslinjer. Ut fra foreliggende dokumentasjon og informasjon, er det imidlertid ikke slik at innholdet i rollene nødvendigvis er forstått av rolleinnehavere. Dette gjelder særlig for faggruppe for personvern og informasjonssikkerhet som først nylig ble etablert. Ut fra funnene over i 3.1, er det også en rekke oppgaver som er beskrevet i fylkeskommunens

styringssystem som ikke utføres. Tydelige beskrivelser av roller og ansvar er viktig for å sikre at oppgaver ikke faller mellom to stoler. I tillegg til tydelige beskrivelser, er det også viktig at rolleinnehavere er kjent med og har forstått det ansvaret og de oppgavene som ligger til rollen. På disse punktene har fylkeskommunen forbedringspotensial.

Anbefalinger

- ✓ Fylkeskommunen bør tydeliggjøre ansvar og oppgaver knyttet til de ulike rollene i fylkeskommunen, herunder særlig for sikkerhetsansvarlig og faggruppe for informasjonssikkerhet. Fylkeskommunen bør lage tydelige instrukser, som tydelig beskriver grensegangen mellom ulike rollers ansvar og oppgaver.
- ✓ Fylkeskommunen bør definere et mandat for faggruppen, der målene for faggruppen beskrives. Det bør også etableres faste arenaer for faggruppen, og defineres hva faggruppen skal rapportere på og til hvem.
- ✓ Fylkeskommunen bør etablere mekanismer som sikrer at oppgaver og ansvar som ligger til de ulike rollene følges opp i forbindelse med den daglige driften.

3.2.3 Oppsummering

Hovedproblemstilling 2 var om og i hvilken grad ansvar og oppgaver knyttet til informasjonssikkerhet og personvern er tydeliggjort, plassert og forstått.

Ut fra de gjennomførte undersøkelser, har fylkeskommunen definert sentrale roller i arbeidet med informasjonssikkerhet og personvern. Rollene er plassert, men de fremstår ikke forstått i alle tilfeller. For flere sentrale roller fremstår det uklart hva som konkret ligger til rollene, og hvor grensene mellom ansvarsområder går.

Flere av de sentrale rollene, slik som sikkerhetsansvarliges rolle, er kortfattet beskrevet, og mangler informasjon om ansvarslinjer, rapportering, kontroll, og godkjenning. Tilsvarende gjelder også for beskrivelse av oppgavene som ligger til rollen som deltaker i faggruppen for informasjonssikkerhet – personvernkoordinator, hvor innholdet i rollen fremstår uklart.

Fylkeskommunen bør tydeliggjøre rollebeskrivelser og kommunisere dette til rolleinnehavere på en egnet måte for å redusere risiko for at oppgaver faller mellom to stoler og dermed ikke blir utført. Det bør utarbeides tydelige rollebeskrivelser og instrukser for å sikre at oppgaver, rolle og ansvar i tilstrekkelig grad er forstått av rolleinnehavere.

3.3 Kompetanse og kapasitet

3.3.1 Innledning

I dette delkapitlet behandles problemstilling 3 - «I hvilken grad innehar fylkeskommunen nødvendig kompetanse og kapasitet for en tilstrekkelig internkontroll vedrørende informasjonssikkerhet og personvern».

Både opplæring og kompetanse er helt avgjørende for å ivareta et tilfredsstillende sikkerhetsnivå. En høy andel av digitale angrep er såkalte phising-angrep, som er rettet mot de ansatte i virksomheten. God opplæring vil dermed kunne være avgjørende for å hindre at angripere lykkes med å trenge inn i fylkeskommunens systemer.

3.3.2 Kompetanse

Målsetting

Fylkeskommunen har vurdert sitt behov for kompetanse på ulike nivåer i organisasjonen, har implementert mekanismer, herunder opplæring for å sikre at alle ansatte har tilstrekkelig kompetanse innenfor informasjonssikkerhet og personvern.

Observasjoner og vurderinger

KPMG har ved vurdering av fylkeskommunens arbeid med kompetanse særlig sett på hvilke vurderinger som er gjort av kompetansebehov for ulike roller og på ulike nivå av fylkeskommunen. Det er også undersøkt om og på hvilken måte fylkeskommunen sikrer at alle ansatte har kompetansen de trenger innenfor personvern og informasjonssikkerhet.

Fylkeskommunen har definert et punkt i sin sikkerhetsstrategi, som innebærer at alle medarbeidere skal ha gjennomført et minimum av sikkerhetsopplæring, noe som skal dokumenteres gjennom en opplæringsplan. Det er også laget en liste over hva opplæringen minst skal inneholde.

Fylkeskommunen har oppgitt at det sentrale verktøyet for å vurdere og gi tilgang til opplæring til ansatte er gjennom fylkesakademiet som ledes av HR. Det er akademiet som definerer hvilken kompetanse det er behov for, og hva som blir satsningsområdene. På bakgrunn av nettverkets vurderinger, etableres det en katalog med kurs og lignende som ansatte kan melde seg på. Kurskatalog er tilgjengelig på fylkeskommunens intranett, og omfatter også kurs innenfor personvern og informasjonssikkerhet. Det er imidlertid ikke gjennomført noen kartlegginger av kompetanse i hele organisasjonen.

Ettersom det ikke er gjennomført kompetansekartlegginger av de ansatte sin kompetanse, finnes ingen kompetanseoversikter for ansatte knyttet til informasjonssikkerhet og personvern i dag. Det har imidlertid pågått et arbeid med å samle oversikt over kompetanse i Visma tidligere, men dette arbeidet er ikke fullført.

Med hensyn til kompetansebehov for spesialistroller og tilsvarende, slik som ansatte med definerte roller og ansvar etter styringssystemet, har det ikke vært gjort en kartlegging eller vurdering av kompetansebehovet. Det fremgår likevel at enkelte slike funksjoner, herunder fagleder og sentrale ansatte på IT-seksjonen, så langt det lar seg gjøre forsøker å holder seg faglig oppdatert innenfor sine ansvarsområder. Ifølge IT-seksjonen oppdaterer faggruppene seg på sine respektive områder med jevne mellomrom. Det oppgis imidlertid at faglig oppdatering har vært utfordrende som følge av høy arbeidsbelastning og manglende kapasitet. For disse rollene fremstår kompetansen som god.

For deltakerne i faggruppen, har det ikke blitt gjennomført kompetansehevende tiltak utover en gjennomgang av fylkeskommunens styringssystem og den generelle opplæringen som er gitt til alle ansatte. Et av formålene med faggruppen er at denne skal bidra til å bygge kompetanse i linjen, og bidra til at styringssystemet implementeres og følges opp. Deltakerne skal også fungere som personvernkoordinatorer. For at dette skal være mulig, må de selv inneha tilstrekkelig kompetanse og innsikt innenfor informasjons-sikkerhet og personvern. Det har de ikke i dag, noe som understøttes av informasjon fra intervju.

I fylkeskommunen foregår opplæring innenfor informasjonssikkerhet og personvern på to nivåer – generell opplæring i regi av fylkeskommunen som er felles for alle enheter og intern spesifikk opplæring i den enkelte enhet.

Den generelle opplæringen i regi av fylkeskommunen fremstår ikke tilstrekkelig systematisk. Det gjennomføres opplæring for eksempel i forbindelse med nasjonal sikkerhetsmåned eller gjennom opplæringsopplegg utarbeidet av personvernombud. Det ble sist gjennomført nano-læring høsten 2021, og det er tidligere blitt gjennomført obligatorisk opplæring i avvik og risikovurderinger, samt i bruk av systemer og applikasjoner som for eksempel Windows 10 og Teams. Fylkeskommunen har også tidligere arrangert samlinger for nyansatte og nye ledere, hvor informasjonssikkerhet og personvern var tema. Siste slik samling var i 2019.

Det kommer frem av intervju at det er variasjoner i den spesifikke opplæringen om informasjonssikkerhet og personvern i enhetene, og at det er variasjon i hvilken grad informasjonssikkerhet og personvern inngår ved introduksjon av nyansatte. Det er skjer ingen strukturert oppfølging av at minsteopplæring gjennomføres for ansatte, og slik gjennomføring dokumenteres ikke. Enkelte enheter har utarbeidet egne sjekklister for introduksjon av nye ansatte som inneholder elementer av informasjonssikkerhet og personvern. HR har oppgitt at det arbeides med et introduksjonsprogram for nyansatte. Dette vil gjøre introduksjonen av nyansatte mer systematisk.

I fylkeskommunens IT-sikkerhetsplan er det beskrevet at det gjennomføres sikkerhetsbevissthetshevende kampanjer via e-post årlig. Det informeres videre på intranettet ved spesielle hendelser, eller situasjoner som krever økt bevissthet hos ansatte. I IT-sikkerhetsplanen er det som risikoreduserende tiltak foreslått å opprette et sikkerhetskulturprogram og skape bevissthet rundt sikkerhet og måling av sikkerhetskultur. Det vises i IT-sikkerhetsplanen til at sikkerhetsbevisstheten mangler i deler av organisasjonen. Videre mangler IT-seksjonen tid til å prioritere arbeid med sikkerhetskultur. Arbeidet med sikkerhetskultur i IT-seksjonen er også stykkevis og delt, og det er i tillegg vektlagt at det bør rettes større fokus mot oppfølging av rutiner.

Samlet fremstår ikke fylkeskommunens arbeid med opplæring av ansatte innenfor informasjonssikkerhet og personvern systematisk. Det er fremstår til dels tilfeldig om det gis opplæring, og det virker som om det er variasjon mellom enhetene i fylkeskommunen. Dette gjelder både for alle nyansatte og personer som har vært ansatt i lengre tid. For særskilte roller i fylkeskommunen, slik som deltakere i faggruppen, er det ikke gitt tilstrekkelig opplæring for at de skal fungere på en tilfredsstillende måte i rollene sine. For sikkerhetsroller fremstår kapasitet som en utfordring og begrenser muligheter til å holde seg faglig oppdatert.

Samtidig har fylkeskommunen flere god initiativer på gang som vil kunne bøte på utfordringene med dagens opplæring. I den forbindelse nevnes særskilt prosjektet om kompetansestyring, som inneholder flere konkrete tiltak for å systematisere arbeidet med kompetanse. Det er oppgitt at målet med prosjektet er å få bedre styring, kontroll og oppfølging av kompetanse i fylkeskommunen, og det er definert en rekke mål for prosjektet og tiltak.

<u>Anbefalinger</u>

- ✓ Sikre at informasjonssikkerhet og personvern inkluderes i fylkeskommunens prosjekt for etablering av kompetansestyring.
- ✓ Gjennomføre kartlegginger av kompetansebehov på ulike nivå innenfor informasjons-sikkerhet og personvern.
- ✓ Gjennomføre obligatorisk opplæring for alle ansatte jevnlig gjennom året. Det bør sikres at det etableres mekanismer for oppfølging av ledere og ansatte når det kommer til gjennomføring av obligatorisk opplæringsopplegg.

- ✓ Vurdere kompetansebehov for sikkerhetsroller, og utarbeide kompetanseplaner basert på disses vurdering av kompetansebehov.
- ✓ Bygge opp og vedlikeholde plattform for kurs og opplæring til ansatte på nettsidene.
- ✓ Følge opp IT-sikkerhetsplanens forslag til tiltak som gjelder sikkerhetskultur og sikkerhetsbevissthet for ansatte.

3.3.3 Kapasitet

Målsetting

Fylkeskommunen har vurdert ressursbehovet knyttet til sikkerhetsarbeid, og støtter opp under arbeidet med informasjonssikkerhet og personvern med tilstrekkelige ressurser.

Observasjoner og vurderinger

Ved vurdering av om fylkeskommunen har tilstrekkelig kapasitet har KPMG undersøkt kapasitet til sentrale ressurser i fylkeskommunens arbeid med informasjonssikkerhet og personvern, herunder slik som fagleder for informasjonssikkerhet, nøkkelpersonell ved IT-seksjonen og deltakere i faggruppe for informasjonssikkerhet.

Fra intervju er det oppgitt at fylkeskommunen mangler kapasitet knyttet til informasjons-sikkerhet og personvern. Kapasitetsutfordringer er knyttet til flere roller, herunder eksempelvis fagleder for informasjonssikkerhet. Rollen er omfattende og inkluderer både informasjonssikkerhet, personvern og beredskap. Under pandemien har beredskapsdelen av stillingen tatt mye kapasitet, noe som har påvirket arbeidet med informasjonssikkerhet og personvern. Planlagte oppgaver, eller oppgaver som det ligger til rollen å følge opp, har blitt prioritert ned eller bort.

Når det kommer til faggruppen for informasjonssikkerhet, fremgår det av gjennomførte intervjuer at rolle i faggruppen har kommet i tillegg til de ansattes øvrige oppgaver, og at det ikke er dedikert tid og kapasitet til å ivareta oppgavene som ligger til rollen. Samtidig oppgis det at flere av medlemmene har en viss fleksibilitet i sin øvrige oppgaveportefølje, noe som gjør at arbeid inn mot faggruppen, eller som personvernkoordinator i linjen, kan prioriteres når det er behov. Det gis uttrykk for en forståelse i enhetene om at arbeid med informasjonssikkerhet og personvern er noe som må prioriteres. Det er imidlertid oppgitt at enkelte av medlemmene av faggruppen vil få kapasitetsmessige utfordringer dersom omfanget øker utover dagens nivå. Som beskrevet i foregående punkter, er faggruppen for øyeblikket ikke operativ.

Kapasitetsutfordringer er også beskrevet av IT-seksjonen. Fylkeskommunen har en stor applikasjonsportefølje som er krevende å håndtere. Kapasitetsutfordringer har fått konsekvenser for eksempelvis avdelingens mulighet til å følge opp leverandører og avtaler. For å avhjelpe kapasitetsutfordringer foretar IT-seksjonen en risikobasert prioritering. Det vektlegges at det som brenner mest og er mest nødvendig blir prioritert.

Det er oppgitt at fylkeskommunen arbeider med å øke sin kapasitet, blant annet ved å ansette en kvalitetsleder som vil ha et særskilt ansvar for kvalitetssystem og internkontroll. Videre arbeider flere av fag- og tjenesteområdene i fylkeskommunen med å omdefinere eksisterende eller etablere nye roller som skal arbeide med kvalitetsarbeid og internkontroll i tjenesteområdet. Det skal også etableres et fagnettverk for internkontroll og kvalitetsarbeid på tvers av hele organisasjonen.

Ut fra de gjennomførte undersøkelsene fremstår det som at fylkeskommunen har kapasitetsutfordringer innenfor arbeid med personvern og informasjonssikkerhet. En stor

del av belastningen for oppfølging av styringssystemet har i praksis falt på enkeltpersoner som også har andre ansvarsområder. Kapasitetsutfordringer har særlig kommet til syne ved at sentrale oppgaver prioriteres ned eller bort og ikke utføres. Fylkeskommunen har truffet tiltak for å kompensere for manglende kapasitet hos enkelte nøkkelressurser, herunder ved etablering av faggruppe, og ansettelser. Det må sikres at faggruppen tilføres tilstrekkelig ressurser og kompetanse slik at de kan fungere i tråd med intensjonene.

Anbefalinger

- ✓ Gjennomføre vurderinger av kapasitet til sentrale roller i fylkeskommunen, herunder for fagleder for informasjonssikkerhet, faggruppe for informasjonssikkerhet og personvern, og IT-seksjonen.
- ✓ Bevisstgjøre organisasjonen på at det finnes et personvernombud og informere om ombudets rolle og oppgaver for å redusere belastningen for fagleder for informasjonssikkerhet.

3.3.4 Oppsummering

Hovedproblemstilling 3 var om og i hvilken grad fylkeskommunen innehar nødvendig kompetanse og kapasitet for en tilstrekkelig internkontroll vedrørende informasjonssikkerhet og personvern.

Som gjennomgått i de foregående punktene, har fylkeskommunen etablert rutine som definerer et minimumsnivå for kompetanse innenfor personvern og informasjonssikkerhet. Det fremstår imidlertid uklart om dette etterleves i praksis. Det gjennomføres videre e-læringskurs der tema er informasjonssikkerhet og personvern. Det fremstår imidlertid uklart i hvilken grad det faktisk følges opp at de ansatte gjennomfører slike kurs. Gjennomføring og oppfølging av kompetansehevende tiltak fremstår ikke systematisk i fylkeskommunen.

Innenfor sentrale sikkerhetsfunksjoner er det ikke gjennomført kartlegging av kompetansebehov, og særlig for faggruppe for informasjonssikkerhet fremstår det klart at det vil måtte gis opplæring dersom faggruppen skal fungere i tråd med sin hensikt, herunder som personvernkoordinatorer i linjen. Fylkeskommunen har ikke utarbeidet kompetanseoversikt, men arbeider med en slik kartlegging, og det inngår også i prosjektet om kompetansestyring.

Med hensyn til kapasitet, er det indikasjoner på at fylkeskommunen har dedikert for lite ressurser til arbeidet med informasjonssikkerhet og personvern. En stor andel av belastningen, og også ansvaret for å gjennomføre styringssystemet i fylkeskommunen, har falt på enkeltpersoner som også har annet ansvar. Dette kommer til syne ved at en del oppgaver og aktiviteter som er beskrevet i styringssystemet har blitt nedprioritert.

3.4 Robusthet mot digitale trusler

3.4.1 Innledning

For å kartlegge Møre og Romsdal fylkeskommune sin robusthet mot digitale trusler er de benyttet en tredelt tilnærming: først ble det gjennomført en penetrasjonstest hvor en emulerte hvordan en reell trusselaktør ville forsøke å angripe fylkeskommunens infrastruktur; deretter ble det gjennomført en kartlegging av fylkeskommunens arbeid med

IKT-sikkerhet opp mot myndighetenes anbefalinger (NSMs grunnprinsipper for IKT-sikkerhet); og til slutt ble det gjennomført et simulert phishing-angrep for å vurdere hvor godt forberedt de ansatte er på å håndtere sikkerhetstrusler som potensielt ikke fanges opp av de tekniske systemene.

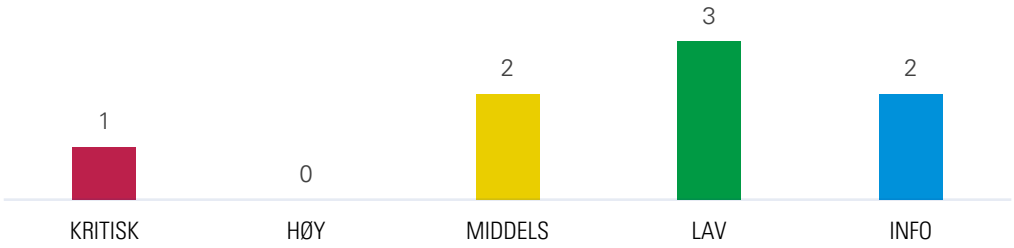
3.4.2 Penetrasjonstest

Målsetting

Virksomheten bør ha en sikker ekstern perimeter som kun er åpen for tillatt trafikk, og som ikke eksponerer sårbare systemer. På innsiden av virksomhetens nettverksperimeter skal ikke en kompromittert bruker kunne øke sine rettighetsnivåer eller få tilgang til informasjon som brukerkontoen i utgangspunktet ikke skal ha tilgang til.

Vurdering

Det ble ikke avdekket noen sårbarheter eller mangler i Møre og Romsdal fylkeskommunes eksterne angrepsflate. Internt i nettverket ble det avdekket totalt 8 sårbarheter fordelt på ulike alvorlighetsgrader. Se figuren nedenfor.



Figur 1: Sårbarheter etter alvorlighetsgrad

Totalt sett så viser ikke resultatene fra penetrasjonstesten at Møre og Romsdal fylkeskommune skiller seg negativt ut fra sammenlignbare virksomheter basert på antallet sårbarheter eller alvorlighetsgraden på disse sårbarhetene. Det er positivt at det ikke ble avdekket noe sårbarheter som var eksponert mot internett og lot seg direkte utnytte av en trusselaktør uten tilgang fra innsiden. Det var også en rekke angrep som vanligvis gir resultater som ikke nådde gjennom hos Møre og Romsdal fylkeskommune. Dette tyder på et over gjennomsnittet sikkerhetsfokus.

Anbefaling

Fylkeskommunen bør (om det ikke allerede er gjort) adressere kritiske og høye observasjoner umiddelbart. Middels, lave og info observasjoner bør vurderes håndtert.

3.4.3 Simulert phishing-angrep

Målsetting

Virksomhetens ansatte er oppmerksomme på forsøk på sosial manipulering og svindel gjennom digitale kanaler, og rapporterer forsøk på dette gjennom etablerte kanaler.

Vurdering

For å kunne gjøre en kvalifisert vurdering av målsettingen er det nødvendig å designe en test som når frem til alle eller et representativt utvalg av alle ansatte. Det ble i forkant av testen avholdt dialog med hovedverneombud og personvernombud for å vurdere den beste måten å gjennomføre det simulerte phishing angrepet på.

Det ble besluttet at testen skulle rettes mot alle med et ansettelsesforhold i fylkeskommunen, og at resultatet ikke skulle deles inn på et lavere avdelingsnivå enn at det var minimum 10 personer i den gruppen for å unngå å identifisere enkeltindivider.

Det ble i forkant av testen gjennomført flere avklaringer med fylkeskommunens for å sørge for at testen skulle forløpe på en måte som ga et realistisk inntrykk av hvordan ansatte ville reagere dersom de ble utsatt for svindel. Det betydde bla. at en for en kort periode måtte koble bort tekniske sikkerhetstiltak for å unngå at disse kan påvirke resultatene

På tross av at oppsettet ble testet i forkant mot et utvalg av fylkeskommunens ansatte for å verifisere at alt fungerte etter hensikten, så viste det seg dessverre at fylkeskommunen ikke hadde lagt inn nødvendig unntak i enkelte sikkerhetsløsninger, som dermed fanget opp og blokkerte nettverkstrafikk kort tid etter at fullskala simulert phishing angrep ble iverksatt.

Fylkeskommunen var informert om at denne typen tester ville medføre en betydelig del ekstraarbeid på førstelinjen på den aktuelle dagen, og hadde vært med på å velge en dato for testen som skulle fungere best mulig med tanke på tilgjengelige ressurser. Fylkeskommunen besluttet også å legge ut en melding om pågående svindelforsøk tidligere på dagen enn avtalt, som også sannsynligvis vil påvirke sammenligningsgrunnlaget KPMG har mot andre virksomheter.

Disse forholdene medfører at verdien av resultatet fra testen er betraktelig svekket som et representativt mål på hvordan en gjennomsnittlig ansatt forholder seg til tilsvarende svindelforsøk. Dette er uheldig da hensikten med denne spesifikke testen ikke var å vurdere om de tekniske sikkerhetstiltakene fungerer etter hensikten, men derimot hvordan de ansatte håndterer svindelforsøk i de tilfellene de sikkerhetstiltak ikke fungerer som planlagt – noe som ofte er måten trusselaktører lurer til seg konfidensiell informasjon som brukernavn og passord.

De ansatte bør anses som den siste og viktigste barrieren i organisasjonens sikkerhetsstrategi. Viktigheten av dette illustreres veldig bra ved at de tekniske sikkerhetstiltakene som ble aktivert mot sin hensikt under testen ikke var i stand til å forhindre flere ansatte fra å legge fra seg brukernavn og passord. Dette skjedde fordi enkelte ansatte leste eposten på mobiltelefonen, og brannmuren til fylkeskommunen ikke omfatter disse. Det viser også at fylkeskommunens varslingskanaler for sikkerhetshendelser ikke når frem til alle ansatte.

Våre systemer registrerte totalt 125 tilfeller av ansatte som ble lurt til å legge fra seg brukernavn og passord etter at brannmuren blokkerte PC-klientene fra å koble til vår server. 101 av disse tilfelle ble registrert etter at fylkeskommunen hadde lagt ut varsel om pågående phishing, og over 30 av forsøkene ble registrert 5 timer etter at varselet var lagt ut.

Anbefaling

- ✓ Fylkeskommunen bør kjøre målrettet opplæring mot alle ansatte for å redusere sannsynligheten for at konfidensiell informasjon kommer på avveie.
- ✓ Fylkeskommunen bør evaluere om varslingskanaler fungerer etter hensikt.

3.4.4 Anbefalt myndighetspraksis

Vurderinger som er gjort i tilknytning til dette delkapittelet baserer seg på informasjon som har kommet frem gjennom intervjuer med nøkkelpersoner i Møre og Romsdal fylkeskommune, samt informasjon som er oversendt i form av dokumentasjon. KPMG legger til grunn at oppgitt informasjon stemmer med virkeligheten, og våre vurderinger og anbefalinger er følgelig knyttet opp mot det bildet som tegnes av denne informasjonen. Vurderingen er basert på myndighetenes anbefalinger iht. NSMs grunnprinsipper for IKT-sikkerhet v. 2.0.

3.4.4.1 Identifisere og kartlegge

Styringsstrukturer, leveranser og understøttende systemer

Målsetting

Virksomheten identifiserer strukturer og prosesser for sikkerhets- og risikostyring for å styre arbeidet med sikring av IKT-systemene. Virksomheten kartlegger leveranser, informasjonssystemer og understøttende funksjoner og vurderer dette opp imot fastsatte toleransegrenser for risiko for å etablere og justere sikkerhetstiltak

Vurdering

Risikovurderinger og sikkerhetsspesifikasjoner gjennomføres ut fra et ad-hoc perspektiv, og det er ikke noen standardisert prosess for å kartlegge og holde oversikt over leveranser og sikkerhetskrav.

Anbefaling

- ✓ Fylkeskommunen bør innføre en standardisert prosess for risikovurdering og sikkerhetsspesifikasjon ved anskaffelser av IKT-løsninger.

Enheter og programvare

Målsetting

Virksomheten har kartlagt enheter og programvare på nettverket, og har oversikt over forvaltede (og ikke-forvaltede) enheter og gjeldene konfigurasjon for disse.

Observasjoner og vurderinger

For maskinvare så er det innkjøpsavtaler som sørger for stor grad av standardisering og en relativt homogen portefølje på de mest brukte utstyrskategoriene. På programvaresiden så sier fylkeskommunen at de har fokus på forvaltning av programvare, og at det jobbes med å få på plass en kontrollert prosess for innføring og forvaltning av programvare.

Det mangler en fullstendig oversikt over alle enheter og programvare i organisasjonens nettverk. Den oversikten som finnes er ikke samlet i et register, men vedlikeholdes manuelt i ulike fragmenterte regneark. Fylkeskommunen har også ulike verktøy som kan hente ut uttrekk over enheter og programvare i deler av infrastrukturen.

Anbefaling

- ✓ Fylkeskommunen bør innføre et sett med verktøy/et register som automatisk holder oversikt over versjoner på utstyr og programvare som befinner seg i organisasjonens

nettverk. Et slikt register bør også inkludere IoT, skytjenester og andre eksterne tjenester som benyttes i fylkeskommunen. Som en del av kartleggingen bør det gjøres en analyse av organisasjonens bruk av «skygge-IT» gjennom f.eks. analyse av aggregert nettverkstrafikk mot kjente tilbydere av skytjenester.

Brukere og tilganger

Målsetting

Virksomheten har oversikt over hvilke brukergrupper, brukere og tilgangsbehov som finnes i virksomheten og har kartlagt ansvar for IKT-sikkerhet.

Vurdering

Fylkeskommunen har en sentral katalogtjeneste som styrer den store majoriteten av brukere, grupper og tilgangsnivåer. Tilgangsstyring og kontroll er integrert med sentrale personalprosesser som ansettelse, permisjon og oppsigelse. Dette betyr at tilganger følger ansettelsesforholdet. Fylkeskommunen opplyser selv at kontrollregimet for innleide og leverandører ikke er like godt integrert.

Alle brukere gis standardrettigheter basert på prinsippet om minste tjenstlige behov. Ytterligere tilganger gis med godkjenning av nærmeste leder. Fylkeskommunen har ikke levert dekkende dokumentasjon på tilgangsnivåer og grupper. Det er gjennom intervjuer kommet frem at håndtering av eleverte og privilegerte rettigheter ikke følger samme kontrollregime som for vanlige rettigheter.

Anbefaling

- ✓ Fylkeskommunen bør dokumentere standardtilganger og alle tilgangsgrupper. Alle tilganger bør gis basert på gruppetilhørighet, og dokumentasjonen bør si noe om hvilke systemer, tjenester og tilgangsnivå gruppetilhørigheten bør medføre.
- ✓ Det bør formaliseres en prosess for håndtering av eleverte tilganger. Unntak fra standardtilganger, herunder eleverte rettigheter, bør dokumenteres, og unntak bør gis for en midlertidig periode med automatisk utløp og behov for godkjenning før fornyelse. All bruk av eleverte tilganger bør i utgangspunktet logges.
- ✓ Prosessen for håndtering av tilganger for innleide og leverandører bør formaliseres. Tilganger settes til å utløpe automatisk basert på varighet til kontrakt e.l., og bør kreve en manuell godkjenning fra ansvarlig bestiller for å fornyes.

3.4.4.2 Beskytte og opprettholde

Ivareta sikkerhet i anskaffelses- og utviklingsprosesser

Målsetting

Sikkerhet er en integrert del av prosessene for anskaffelse og utvikling, og virksomheten minimerer risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter.

Vurdering

I forbindelse med innkjøp av IKT-leveranser vil fylkeskommunen sette en rekke sikkerhetskrav i form av kravspesifikasjonen for den respektive innkjøpsprosessen. Det finnes sett

med sikkerhetskrav som danner grunnlagt for kravspesifikasjonen til fylkeskommunen. Disse standardkravene bør utvides til å dekke bla. integrasjon og kompatibilitet med sentrale komponenter i sikkerhetsarkitekturen til fylkeskommunen.

Programvareutvikling foregår i hovedsak med tredjepartsleverandører og i mindre grad med interne ressurser. Fylkeskommunen vil som oftest lene seg på leverandørenes prosesser for sikker utvikling, og har ikke egne formaliserte prosesser for dette. Det er ikke etablert formaliserte prosesser for vedlikehold av utviklet programvarekode ut over overordnede rutiner for applikasjonsforvaltning.

Det finnes separate miljøer for utvikling, test og produksjon som er logisk separert. Miljøene er ikke adskilt fysisk på maskinvare eller i nettverk. Det opplyses om at det er høyt fokus på å ikke bruke sensitive data fra produksjonsmiljøer i testmiljøer. Fylkeskommunen opplyser at all ny programvare, og programvare med vesentlige endringer, vil bli testet i testmiljøet for det tas i bruk i produksjonsmiljøet.

Fylkeskommunen har etablert Service Level Agreements (SLA) med de mest sentrale IKT-leverandørene, men det er mange mindre leverandører som mangler slike avtaler. Det er ikke noen strukturert prosess for å følge opp sikkerhet eller verifisere leveranser hos leverandører.

Anbefaling

- ✓ Sikkerhetskrav ved anskaffelser bør inneholde konkrete krav til kryptering i ro og under transport sett i forhold til klassifiseringen av informasjon som skal behandles. I tillegg bør sikkerhetskravene dekke alle nødvendige integrasjoner mot fylkes-kommunens sikkerhetsarkitektur, jf. NSMs grunnprinsipper for IKT-sikkerhet pkt. 2.2.1. Det bør også finnes et sett med sikkerhetskrav til bruk ved anskaffelse av maskinvare.
- ✓ Prosesser og retningslinjer for sikker utvikling bør utarbeides og formaliseres. For å unngå å vedlikeholde en rekke mer eller mindre teknologiavhengige retningslinjer bør disse basere seg på anerkjente rammeverk for sikker utvikling. Fylkeskommunens prosesser bør også omfatte sikkerhetsoppdateringer av komponenter som åpne biblioteker e.l. etter at programvaren er ansett som funksjonelt ferdigutviklet.
- ✓ Fylkeskommunen bør ha prosesser som sikrer at en følger opp sikkerhet og leveranser ved tjenesteutsettelse, f.eks. gjennom krav om sikker utvikling, SLA-rapporter og forventninger til innsyn i og oppfølging av sikkerhetsrevisjoner eller attestasjoner fra sentrale leverandører.

Etabler en sikker IKT-infrastruktur

Målsetting

Virksomheten har etablert en helhetlig sikkerhetsarkitektur som ivaretar ønsket sikkerhets-nivå gjennom gode sikkerhetsfunksjoner og sikkerhetsstrukturer med mulighet for etterprøvbarhet.

Vurdering

Fylkeskommunen har etablert en IKT-infrastruktur som baserer seg på god praksis for sikkerhet, med bla. sentrale katalogtjenester for brukeradministrasjon, segmentering (og pågående mikrosegmentering) av nettverk, eget administrasjonsnettverk og nettverk for sikker sone, overvåkning av nettverkstrafikk (IDS og IPS), overvåkning av hendelser på endepunkter, gode løsninger for sikkerhetskopiering, mv.

Flere fagsystemer benytter seg av applikasjonsspesifikke identiteter og er dermed ikke er koblet opp mot katalogtjenestene. Fylkeskommunen har ikke rullet ut all tilgjengelig sikkerhetsfunksjonalitet enda.

Selv om fylkeskommunen har implementert gode tiltak for å forvalte en sikker IKT-infrastruktur, så har ikke KPMG fått forelagt dokumentasjon på at det er gjennomført en helhetlig risikovurdering av IKT-virksomheten. Dette kan føre til at fylkeskommunen ikke har mulighet til å avdekke og adressere større systematiske risikoer som naturkatastrofer, bortfall av strøm eller nettforbindelse, omfattende hackerangrep mv.

Anbefaling

- ✓ Fylkeskommunen bør gjennomføre en årlig helhetlig risikovurdering av hele IKT-virksomheten for å fange opp systematiske risikoer mot hele eller store deler av IKT-infrastrukturen.
- ✓ Det er flere sikkerhetskomponenter og muligheter i teknologien til fylkeskommunen som kan rulles ut eller allerede er rullet ut. Det er viktig at arbeidet med dette fortsetter å holde tritt med den teknologiske utviklingen. Bla. endringen fra stedlig IT-tjenester til skybaserte løsninger gjør at en bør tenke nytt rundt ting som perimeter-sikring osv.

Ivareta en sikker konfigurasjon

Målsetting

Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Vurdering

Fylkeskommunen gjennomfører jevnlig utrulling av sikkerhetsoppdateringer på tvers av porteføljen, blant annet gjennom en månedlig planlagt «patchedag» hvor IT-seksjonen går gjennom og oppdaterer programvare til siste anbefalte versjon. Selv om det benyttes sentraliserte løsninger for utrulling av oppdateringer for deler av infrastrukturen finnes det en del systemer som krever en manuell håndtering. Fylkeskommunen opplyser at det er noe teknisk gjeld i porteføljen, men at dette er planlagt faset ut.

Drift og vedlikehold foregår i hovedsak over et eget driftsnett som er skjermet fra øvrig nettverk. For å koble til må en innom en eller flere jump-servere. Det er ikke forelagt noen dokumenterte prosesser for hvordan prosessene for bla. sikkerhetsoppdateringer gjennomføres.

Standardpassord oppgis å bli deaktivert når nye systemer eller utstyr innlemmes i fylkeskommunens nettverk, men denne prosessen er ikke dokumentert. MRFK kan heller ikke vise til at det er noen øvrig systematisk tilnærming til herding av klienter, tjenere og sky-tjenester, og det er ikke gjennomført noen grundig vurdering av hvilken standard-funksjonalitet som kan deaktiveres uten at det medfører tap av nødvendige funksjoner. «Hvitelisting» av programvare er også et svært effektivt risikoreduserende tiltak som det anbefales å benytte i de fleste større organisasjoner.

Fylkeskommunen benytter forhåndsdefinerte oppsett for å tanke operativsystem og standard programvare på klientplattformen. Tilsvarende så benyttes det forhåndsdefinerte oppsett for å installere ulike typer tjenere. Det fremstår likevel som det er en god del utstyr

og installasjoner som mangler forhåndsdefinerte installasjonsoppsett. Det er ikke mottatt noen informasjon om at det gjennomføres verifikasjoner eller sikkerhetstesting av forhåndsdefinerte oppsett.

IoT-enheter benyttes på ulike lokasjoner innad i organisasjonen, og har foreløpig blitt plassert i det tekniske nettet for å i noen grad isolere IoT-enheter fra øvrig utstyr. Det er en plan om at IoT-enheter skal over på en mikrosegmentert nettverksinfrastruktur etter hvert. MRFK opplyser at det ikke er noen fullstendig oversikt over slike enheter i organisasjonen, og at det ikke er noen prosess for å sikre at bruk av ulike IoT-løsninger gjennomgår en hensiktsmessig risikovurdering før det tas i bruk i organisasjonen.

Anbefaling

- ✓ Det bør utarbeides dokumentasjon som beskriver hvordan de ulike systemene holdes oppdatert, enten det er gjennom et sentralisert og automatisk system eller om det er avhengig av manuelle prosesser (og i så tilfelle hvordan dette gjennomføres). Dokumentasjonen bør omfatte hele infrastrukturen, inkl. maskinvare, fastvare og programvare på både klientplattform, nettverksutstyr, tjenere og andre enheter (skrivere, AV-utstyr, mv).
- ✓ Fylkeskommunen bør prioritere å få på plass dokumentasjon som beskriver hvordan utstyr og programvare er sikret med en sikker konfigurasjon. Det bør være en forhåndsdefinert konfigurasjon for alle enheter som benyttes i organisasjonen, og det bør jevnlig gjennomføres verifikasjon/test av disse opp mot anbefalt praksis. Dette bør sees i sammenheng med en vurdering av hvordan programvare og utstyr best mulig kan herdes ved bla. å deaktivere funksjonalitet som ikke er i bruk.
- ✓ Hvitelisting av tillat programvare på klientplattformen bør implementeres. Dette vil høyst sannsynlig medføre en del merarbeid i innkjøringsfasen, men vil også gi en høy reduksjon i risiko for angrep gjennom klientplattformen. Fylkeskommunen opplyser allerede å ha funksjonalitet for å rulle ut et regime for hvitelisting av programvare på klienter gjennom Microsoft 365.
- ✓ Selv om mesteparten av drift og administrasjon må gå gjennom eget driftsnettverk, får KPMG opplyst at det finnes enkelte administrasjonsgrensesnitt som er offentlig tilgjengelig over internett. Fylkeskommunen er klar over dette, og arbeider med å håndtere disse. Dette arbeidet bør fullføres.
- ✓ Alle IoT-enheter og løsninger bør gjennomgå en grundig risikovurdering fra et informasjonssikkerhets- og personvernperspektiv før de tas i bruk. IoT-enheter representerer ofte en kategorisk utfordring på å sikre sikkerhet i integrasjoner og dataflyt. Mangel på grundige risikovurderinger representerer en stor risiko for at data kommer på avveie.

Beskytt virksomhetens nettverk

Målsetting

Virksomheten kontrollerer og beskytter nettverkene sine mot interne og eksterne trusler.

Vurdering

Nettverket i organisasjonen er konfigurert slik at forvaltende enheter logger på nettverket med et sertifikat og blir plassert i et VLAN som gir tilgang til ulike interne tjenester. Ikke-forvaltede enheter som logger på uten sertifikat vil bli plassert i et eget VLAN som ikke har tilgang til disse interne tjenestene.

Fylkeskommunen har ansvar for å drifte nettverk på et stort antall lokasjoner. Det opplyses om at det er god kontroll på den fysiske sikkerheten til infrastrukturen på hovedkontoret, men at det er mindre oversikt over den fysiske sikkerheten til infrastruktur på satellitt-lokasjoner.

Nettverket er beskyttet av brannmurer og IDS/IPS på kant, dvs. i sonen mellom interne nettverk og eksterne nettverk (internett). Nettverket er videre segregert i ulike soner (VLAN) som også er skjermet mot hverandre innad. Klientplattformen har videre brannmur i operativsystemet. Fylkeskommunen har automatiserte løsninger for å overvåke og analysere nettverkstrafikk i sanntid.

Anbefaling

- ✓ Fylkeskommunen bør gjøre en kartlegging av den fysiske sikkerheten til nettverket ut til satellittlokasjoner. Kartleggingen bør ta stilling til om sentralt nettverksutstyr er tilstrekkelig skjermet fra publikum.

Kontroller dataflyt

Målsetting

Virksomheten har kontroll på informasjonsflyten mellom ulike deler av systemer slik at enheter kun kan kommunisere sammen etter vedtatte regler. Virksomheten har også kontroll på informasjonsflyten inn og ut av virksomheten.

Vurdering

Ved å benytte seg av en sentralisert brannmurløsning kontrollerer fylkeskommunen data-flyten mellom de forskjellige sonene i nettverket. Ikke-forvaltede enheter som mobil-telefoner eller andre enheter med «lav tillit» vil bli plassert i en egen nettverkssone for utstyr med «lav tillit» når de logger på nettverket. Skrivere, AV-utstyr, byggeteknisk IT-utstyr osv., vil også bli plassert i egne soner. Det er også egne sikre soner for sensitive data som helseopplysninger mv.

I utgangspunktet må all pålogging på interne tjenester gå gjennom forvaltede enheter som er pålogget fylkeskommunens nettverk, enten lokalt eller gjennom en VPN fra en ekstern lokasjon. Enkelte tjenester er eksponert mot internett, men disse er plassert i en egen DMZ-sone og sikret på ulike måter.

Fylkeskommunen er i gang med å implementere mikrosegmentering i nettverket. Når dette er ferdigstilt vil det gi en enda bedre og mer granulert inndeling og skjerming av ulike soner i nettverket, og ytterligere begrense muligheten for «peer-to-peer» trafikk i nettverket.

Anbefaling

- ✓ Fylkeskommunen opplyser at det finnes løsninger med teknisk gjeld i infra-strukturen, men at det er en plan for å avvike disse systemene. Det anbefales iht. til god praksis å skjerme løsninger med teknisk gjeld som medfører at det f.eks. ikke er mulig å installere sikkerhetsoppdateringer i egne nettverk for å redusere risiko.
- ✓ Fylkeskommunen bør se på muligheten til å styre all nettverkstrafikk fra forvaltede enheter gjennom fylkeskommunens infrastruktur for å enklere kunne avdekke avvik og sikkerhetsbrudd i nettverkstrafikken.

- ✓ Alle enheter som mobiltelefoner, nettbrett, ol. som gis tilgang til organisasjonens data (e-post, nettverk, systemer, el.) bør underlegges forvaltning for å sørge for at tilgangen gis betinget på et grunnleggende sikkerhetsnivå.

Ha kontroll på identiteter og tilganger

Målsetting

Virksomheten har oversikt over identiteter og kontoer i informasjonssystemene og styrer tilgang til ressurser effektivt og i henhold til virksomhetens retningslinjer.

Vurdering

MRFK har en sentral katalogtjeneste som styrer den store majoriteten av brukere, grupper og tilgangsnivåer. Tilgangsstyring og kontroll er integrert med sentrale personalprosesser som ansettelse, permisjon og oppsigelse. Dette betyr at tilganger følger ansettelses-forholdet. Fylkeskommunen opplyser selv at kontrollregimet for innleide og leverandører ikke er like godt integrert.

Alle brukere gis standardrettigheter basert på prinsippet om minste tjenstlige behov. Ytterligere tilganger gis med godkjenning av nærmeste leder. Fylkeskommunen har ikke levert dekkende dokumentasjon på tilgangsnivåer og grupper.

Fylkeskommunen skiller mellom vanlige brukerkontoer og administrative brukerkontoer. Sistnevnte blir markert «adm_brukernavn». Det er gjennom intervjuer kommet frem at håndtering av eleverte og privilegerte rettigheter ikke følger samme kontrollregime som for vanlige rettigheter, bla. gjennom at eleverte rettigheter følgelig kan bli værende etter at behovet ikke lenger er til stede.

To-faktor autentisering er implementert for de systemene som støtter dette. Det er likevel noen systemer som ikke har støtte for to-faktor autentisering. Det samme gleder for SSO, hvor enkelte eldre systemer ikke har støtte. Det er også avdekket en varierende passord-policy på tvers av ulike systemer.

Anbefaling

- ✓ Fylkeskommunen bør dokumentere hva som inngår i ulike tilgangsnivåer og grupper, og hvordan disse korresponderer med tjenstlige behov hos ansatte, elever og innleide.
- ✓ Det bør være en prosess som sørger for årlig revisjon av brukernes tilganger. Denne revisjonen bør også se på om tilgangene som gis ved gruppetilhørighet er iht. prinsippet om minste tjenstlige behov. Prosessen bør også avdekke brukerkontoer som ikke lenger er i bruk.
- ✓ Prosessen for håndtering av tilganger for innleide og leverandører bør formaliseres. Tilganger settes til å utløpe automatisk basert på varighet til kontrakt e.l., og bør kreve en manuell godkjenning fra ansvarlig bestiller for å fornyes.
- ✓ Fylkeskommunen bør vurdere praksisen med å dele ut administrative rettigheter til sluttbrukere. Dette kan redusere støttebehovet fra IT-seksjonen på kort sikt, men er ikke i henhold til god praksis. Fylkeskommunen bør bla. se på om det finnes løsninger for å f.eks. levere ut programvarepakker gjennom ulike distribusjonskanaler som ikke krever at sluttbrukere har administratortilganger.

Beskytt data i ro og i transitt

Målsetting

Virksomheten beskytter data som ligger på ulike lagringsmedium og når den formidles over ulike informasjonskanaler.

Vurdering

Fylkeskommunen opplyser at det er implementert kryptografi på de delene av infrastrukturen som støtter dette. Det mangler likevel en formalisert strategi og kravspesifikasjon for håndtering av kryptografi i virksomheten. Fylkeskommunen mangler generelt dokumentasjon på hvordan kryptografi er benyttet i virksomheten.

Anbefaling

- ✓ Fylkeskommunen bør utvikle en dokumentert strategi og kravspesifikasjon for håndtering av kryptografi. Strategien bør inneholde valg av kryptografiske verktøy, håndtering av sertifikater, hvordan utøve sikker nøkkelgenerering, hvordan nøkler/passord oppbevares, sikkerhetskopiering av nøkler, fornyelse av nøkler og hvordan håndtere kompromittering av nøkler.
- ✓ Som et ledd i en overordnet risikovurdering bør det identifiseres hvilke data i infrastrukturen som bør krypteres under transport og i ro. Som et minimum bør kommunikasjon som foregår over kommunikasjonskanaler med lav tillit krypteres (f.eks. eksterne nettverk og internett). Data på klientmaskiner, mobiltelefoner, mv. bør krypteres for å unngå at data havner på avveie.

Beskytt e-post og nettleser

Målsetting

Virksomheten minimerer angriperes mulighet til å manipulere menneskelig oppførsel i forbindelse med bruk av epostklienter og nettlesere.

Vurdering

Fylkeskommunen har aktivert SPF, men opplyser at det mangler andre sikkerhetsmekanismer som DMARC, DKIM og DNSSEC for å sikre virksomheten mot phishing og angrep over epost.

Det er som tidligere nevnt tidligere ikke implementert hvitelisting av programvare eller programvaretillegg i nettlesere el. på klientplattformen til fylkeskommunen.

Anbefaling

- ✓ Aktiver DMARC, DKIM og DNSSEC for å sikre epost bedre.
- ✓ Innfør hvitelisting av programvaretillegg i nettlesere osv. for å unngå at usikker programvare kjøres via disse kanalene.

Etabler evne til gjenoppretting av data

Målsetting

Etabler en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap.

Vurdering

Fylkeskommunen har etablert en policy for sikkerhetskopiering av deres IKT-systemer. Her fastsettes blant annet organisasjonens generelle retningslinjer rundt sikkerhetskopiering samt prosedyrene som understøtter dette. Policyen beskriver at alle servere knyttet til IT-tjenester som IT-seksjonen har driftsansvar for eller som står i avdelingens datarom (fysiske og virtuelle) skal inkluderes i sikkerhetskopipolicyen. Servere hos andre enheter (f.eks. videregående skoler) avtales særskilt for hver enkelt sak.

Fylkeskommunen har et nytt system for sikkerhetskopiering som støtter «immutable storage». Dette er en teknologi som sikrer at data ikke skal kunne manipuleres eller ødelegges etter at det er tatt sikkerhetskopi. Det blir fastsatt regelmessighet på sikkerhets-kopiering for hvert enkelt system (e.g., database server, filservere, osv.) mens det for andre tjenester som har lovpålagte krav på denne fronten er opp til tjeneste- eller systemeier å kartlegge og avtale med IT-drift.

Standard oppbevaringsperiode for sikkerhetskopier er 32 dager. Policyen lister relevante lovpålagte lagringskrav samt kartlegger prosedyrene for hvordan sikkerhetskopieringen utføres. Utover dette er det ikke listet interne logiske og fysiske krav til sikring av sikkerhetskopier.

Det foreligger ikke noen konkrete mål på gjenopprettingstid for virksomhetens ulike systemer, og det er ikke gjennomført noen større øvelser for å se og analysere hvordan et større gjenopprettingsscenario vil fungere i praksis.

Anbefaling

- ✓ Fylkeskommunen bør gjennomføre en årlig storskala test/øvelse for gjenoppretting av kritiske verdikjeder og sentrale IT-systemer og infrastruktur. Det bør som en del av dette etableres måltall for hvor raskt det vil ta å få på plass kritiske verdikjeder og sentrale IT-systemer og infrastruktur.

Integrer sikkerhet i prosess for endringshåndtering

Målsetting

Opprettholde virksomhetens etablerte sikkerhetstilstand ved planlagte endringer.

Vurdering

Fylkeskommunen har utarbeidet en policy for endringshåndtering som forklarer hvordan en bruker deres interne verktøy til å dokumentere endringer og få disse godkjent. Endringer vil bli dokumentert gjennom bruken av dette verktøyet. Det er ingen tydelige krav til testing av endringer før og etter idriftsetting, men håndboken krever test som sikrer at forventede funksjoner er ivaretatt i forbindelse med konfigurasjonsendringer på nettverket eller i datautstyr.

Anbefaling

- ✓ Policy og prosess for endringshåndtering bør omfatte testing og dokumentasjon av at sikkerhetstiltak fungerer før og etter driftssetting.

3.4.4.3 Oppdage

Oppdag og fjern kjente sårbarheter og trusler

Målsetting

Virksomheten oppdager og fjerner kjente sårbarheter og kjent skadelig kode i virksomhetens IKT-systemer.

Vurdering

Fylkeskommunen har gjennomført sårbarhetsskanning ved bruk at av tredjeparter, men det mangler prosesser for gjennomføring av jevnlig sårbarhetskartlegging. Her bør også rutiner for prioritering av funn og verifisering av oppdagede sårbarheter utformes.

Fylkeskommunen har uformelle rutiner for innsamling av trusseletterretning ved å benytte åpne kilder som Reddit, BleepingComputer og CVE feeds. Bortsett fra dette har fylkeskommunen ingen kommersielle verktøy eller strukturerte rutiner for innsamling av trusselinformasjon.

Det benyttes antivirus på klientmaskiner og på servere. Fylkeskommunen har også abonnement på trusseletterretning som inngår i brannmurløsningen for å avdekke pågående hendelser i nettverket.

Anbefaling

- ✓ Opprette rutiner for jevnlig (automatisert) sårbarhetsskanning av infrastrukturen. Her anbefales tjenester som for eksempel Qualys, Tenable Nessus eller Rapid7 Nexpose.
- ✓ Vurdere behovet for en mer strukturert innsamling av trusseletterretning som kan tilpasses og skreddersys basert på IKT-porteføljen til fylkeskommunen.

Etabler sikkerhetsovervåkning

Målsetting

Virksomheten overvåker sine IKT-systemer og samler inn relevante data for å oppdage sikkerhetshendelser og legge et grunnlag for analyse av data.

Vurdering

Fylkeskommunen har ikke etablert tydelige målsettinger for sikkerhetsovervåkning. I «IT Sikkerhetsplan» er det beskrevet at fylkeskommunen har til hensikt å sikre data gjennom å avdekke eventuelle avvik og brudd i informasjonssikkerhet og personvern, samt å ha kapasitet til å etterforske hendelser og sikkerhetsbrudd.

Fylkeskommunen har ikke dedikerte verktøy eller plattformer som understøtter slik sikkerhetsovervåkning p.t., men bruker en sammensatt løsning med ulike komponenter som samlet gir god innsikt i hva som foregår i IKT-infrastrukturen, herunder servere, brannmur, rutere og klienter. Det opplyses om at det er enkelte begrensninger i informasjonen som kan hentes ut fra klienter ved sikkerhetshendelser.

Det opplyses om at dataene lagres i 2 år for å kunne sikre sporbarhet ved en hendelse, men det kan ikke dokumenteres at det er gjort noen konkrete vurderinger av hva som er lovpålagt og evt. begrensninger for oppbevaring av loggdata. Fylkeskommunen har ikke beskrevet hvordan loggdataene sikres mot manipulering.

Anbefaling

- ✓ Fylkeskommunen bør gjøre en vurdering av hvilke lovpålagte plikter som kan påvirke oppbevaringstid (lengre/kortere) for loggdata, samt om loggdata oppbevares på en trygg nok måte for å unngå manipulering av evt. trusselaktør.
- ✓ God synlighet i hva som har skjedd på klienter er av stor verdi ved etterforskning av sikkerhetsbrudd. Fylkeskommunen bør derfor vurdere om de henter inn nok sikkerhetslogger fra klientene til å kunne understøtte en granskning ved en reell sikkerhetshendelse.

Analyser data fra sikkerhetsovervåkning

Målsetting

Virksomheten oppdager skadelige aktiviteter som påvirker informasjonssystemer, data og tjenester gjennom analyse av sikkerhetsrelevante data.

Vurdering

Logging av systemer på tvers av IKT-infrastrukturen til fylkeskommunen blir i dag brukt for å overvåke systemenes ytelse og tilgjengelighet, mens det også blir brukt for feilsøking. Til tross for at loggene blir samlet, og til dels sentralisert, finnes det ingen plan for analyse av data for sikkerhetsovervåkning i fylkeskommunen i dag. Fylkeskommunen har ingen konkrete eskaleringsrutiner eller rutiner for håndtering av sikkerhetshendelser.

I forbindelse med herding mot trusselen for løsepengevirus har fylkeskommunen opprettet varsling dersom store mengder filer blir skrevet på systemene. Bortsett fra dette har ikke fylkeskommunen dokumentert eller rapportert noen form for kartlegging eller etablering av forståelse for normaltilstanden i virksomhetens systemer.

Anbefaling

- ✓ Fylkeskommunen bør implementere et system som er i stand til å analysere de store mengdene loggdata og alarmere ved avvik fra normaltilstanden.
- ✓ Det bør utarbeides en rutine for eskalering og håndtering av alarmer fra avvik i normaltilstand.

Gjennomfør inntrengningstester

Målsetting

Virksomheten tester elementer i egne forsvarsmekanismer (teknologi, prosesser og personell) ved å simulere målene og handlingene til en angriper.

Vurdering

Fylkeskommunen har rapportert at det har blitt utført inntrengingstester med sporadiske intervaller når kapasiteten og budsjettet tillater det. Fylkeskommunen har god kjennskap til de viktige delene av informasjonssystemet som bør vektlegges i testingen, og hva som

bør unngås. Det gjennomføres en inntrengningstest som en del av prosjektet bak denne rapporten.

Anbefaling

- ✓ Fylkeskommunen bør planlegge jevnlige sikkerhetstester, og sørge for at det settes av budsjett for dette. Det finnes ulike typer tester, hvorav noen vil være spesifikt rettet mot enkeltsystemer eller komponenter. Fylkeskommunen bør sørge for at det som et minimum utføres en test for utsiden av nettverksbarriere (for å simulere en ekstern angriper) og en test fra innsiden av nettverksbarrieren (for å simulere kompromittert klient) ca. årlig.

3.4.4.4 Håndtere og gjenopprette

Forbered virksomheten på håndtering av hendelser

Målsetting

Virksomheten har implementert effektive prosesser for hendelseshåndtering slik at hendelser oppdages hurtig, kontrolleres, skaden minimeres og hendelsesårsaken fjernes effektivt. Dette inkluderer gjenopprettelse av integriteten til systemer og nettverk.

Vurdering

Fylkeskommunen har utarbeidet en kontinuitetsplan som beskriver prosedyrer dersom viktige forretningsfunksjoner ikke fungerer på en tilfredsstillende måte. Denne inneholder en tydelig beskrivelse av ansvaret for de relevante rollene ved en krisehåndtering.

Kontinuitetsplanen fremstår ikke som oppdatert, og mangler blant annet sentral og viktig informasjon om nødprosedyrer, midlertidige prosedyrer og gjenopprettingsprosedyrer.

Kontinuitetsplanen setter krav om at det skal utføres to enkle og minst en avansert test hvert år. Det er ikke oversendt dokumentasjon på at det er utført øvelser.

Anbefaling

- ✓ Kontinuitetsplanen bør oppdateres og fullføres.
- ✓ KPMG har ikke fått oversendt noe dokumentasjon på at det er gjennomført øvelser. Dette bør gjennomføres iht. egne rutiner og god praksis.
- ✓ Planverk for testing av krise- og kontinuitetsplanverket bør utvides til å omfatte sentrale leverandører som vil kunne påvirkes ved en hendelse.
- ✓ Det bør foreligge en oppdatert oversikt over alle sentrale kontaktpersoner hos samarbeidspartnere og leverandører. Dette kan være IT-spesialister innen ulike fagfelt, leverandører av utstyr og programvare, ledelsen, sluttbrukere, media mm.

Vurder og klassifiser hendelser

Målsetting

Virksomheten vurderer og klassifiserer hendelser korrekt og hurtig slik at hendelsene blir håndtert effektivt, med riktig prioritet, og involverer nødvendige ressurser og personell.

Vurdering

Fylkeskommunen har tilgang til en rekke loggdata som kan tilføre viktig informasjon under håndtering av en sikkerhetshendelse. Det er p.t. ikke noen dokumentert prosess for hvordan fylkeskommunen skal utnytte potensialet som ligger i dette.

Anbefaling

- ✓ Det bør utarbeides en prosessbeskrivelse som detaljerer hvordan fylkeskommunens omfattende tilgang på loggdata kan benyttes til å håndtere en reell hendelse.

Kontroller og håndter hendelser

Målsetting

Virksomheten håndterer hendelser korrekt og med riktige ressurser slik at spredning og konsekvenser minimeres og normaltilstand opprettholdes eller gjenopprettes effektivt.

Vurdering

Fylkeskommunen har gjennomført en ROS-analyse av konsekvenser dersom de største IKT-plattformene og mest brukte programvarene i organisasjonen skulle falle bort. Denne ROS-analysen er 10 år gammel og bør oppdateres.

Anbefaling

- ✓ Det bør gjennomføres en ny ROS-analyse som tar for seg håndtering av de mest relevante scenarioene en ser for seg kan oppstå. Eksempler på dette kan være bortfall av datasenter, løsepengeangrep, tjenestenektangrep, naturkatastrofer, utro tjenere, mv.

Evaluer og lær av hendelser

Målsetting

Virksomheten lærer av hendelser og forbedrer sikkerhetstiltak, hendelsesprosesser, opplæring av personell og oppdatering av gjeldende prosedyrer.

Vurdering

Fylkeskommunen har ikke en prosess for hendelseshåndtering som beskriver hvordan lærdommer og observasjoner fra hendelser skal innarbeides i eksisterende drift og planverk.

Anbefaling

- ✓ Metodeverket for håndtering av hendelser og avvik bør inneholde konkrete punkter om hvordan fylkeskommunen skal evaluere og lære av hendelser og avvik.

3.4.5 Sammendrag

Det er etablert et godt basisnivå iht. NSMs grunnprinsipper for IKT-sikkerhet. Det er enkelte tiltak fylkeskommunen bør se på som er nevnt i kapitelene ovenfor. På den tekniske siden trekkes det spesielt frem at fylkeskommunen med fordel vurdere utvalgte tiltak for å herde

klientplattformen, f.eks. hvitelisting av tillatt programvare og fjerning av ikke-essensiell programvare og funksjonalitet på standardplattformen.

Det er også en rekke anbefalinger som går på manglende risikostyring og mangel av dokumentasjon som bør adresseres. Spesielt er det identifisert mangler i planverk for krise og kontinuitetsberedskap som kan ha potensielt store konsekvenser ved håndtering av en sikkerhetshendelse.

I takt med at utviklingen går i retning av flere enheter og deling av data på tvers av disse, så bør fylkeskommunen se på hvordan det i fremtiden best mulig kan sikres dataflyt mellom enheter og redusere risikoen for utnyttelse av angrepsvektorer som best håndteres ved blant annet herding av endepunkter og god forvaltning av mobile enheter med tilgang til organisasjonens data.

3.5 Personvern

3.5.1 Innledning

Hovedproblemstillingen er i dette delkapitlet om og i hvilken grad fylkeskommunen etterlever sentrale krav i personvernlovgivningen. KPMG har vurdert de sentrale kravene som stilles i personopplysningsloven og personvernforordningen (GDPR) når det kommer til fylkeskommunens behandling av personopplysninger.

Rapporten er i fortsettelsen tematisk inndelt i samsvar med rekkefølgen i personvern-forordningen.

3.5.2 Etterlevelse av grunnleggende prinsipper for behandling av person-opplysninger

De grunnleggende prinsippene for behandling av personopplysninger er listet opp i GDPR art. 5 nr. 1. De fleste av personvernforordningens øvrige bestemmelser må leses og forstås i lys av disse prinsippene, og de kan dermed forstås som et sett med helt grunnleggende krav for å behandle personopplysninger. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at prinsippene overholdes etter GDPR art. 5 nr. 2. Det siste omtales ofte som prinsippet om ansvarlighet, og innebærer at den behandlingsansvarlige må kunne dokumentere at prinsippene overholdes.

3.5.2.1 Prinsippet om lovlighet, rettferdighet og åpenhet

Målsetting

Alle behandlingsaktiviteter skjer på en lovlig måte, herunder at de har et behandlings-grunnlag, og at behandling skjer på en tilstrekkelig rettferdig og åpen måte overfor den registrerte.

Observasjoner og vurderinger

KPMG har ved vurdering av om prinsippet overholdes særlig sett på om all behandling har et behandlingsgrunnlag, og om behandling skjer på en tilstrekkelig åpen måte overfor den registrerte, herunder om det gis tilstrekkelig informasjon om behandlingen. Informasjon til de registrerte er også omtalt mer detaljert under i pkt. 3.5.3. Med hensyn til informasjon

til de registrerte, har det for vurderingen under dette punktet vært sentralt om fylkeskommunen kan dokumentere at slik informasjon er gitt i tråd med prinsippet om ansvarlighet i personvernforordningen art. 5 nr. 2.

I protokollen over behandlingsaktiviteter er det ikke angitt et behandlingsgrunnlag for alle behandlingsaktiviteter. Angivelse av behandlingsgrunnlag er for ordens skyld ikke et krav som stilles til protokollen, men fylkeskommunen er som nevnt pålagt å kunne dokumentere overholdelse av de grunnleggende prinsippene, noe som det i fylkeskommunens tilfelle er lagt opp til at skal skje gjennom protokollen.

Med hensyn til situasjoner hvor behandling av personopplysninger er basert på den registrertes samtykke, er det i intervju gitt informasjon om at det ved innføringen av personvernforordningen ikke ble foretatt en gjennomgang av om tidligere innsamlede samtykker var lovlig, herunder om det var gitt informasjon. Når behandling av personopplysninger baseres på samtykke, skal den behandlingsansvarlige kunne påvise at den registrerte har samtykket. For at et samtykke skal være gyldig må den registrerte ha fått tilstrekkelig informasjon, herunder om retten til å trekke tilbake sitt samtykke. Ettersom fylkeskommunen ikke har hatt en gjennomgang av sine behandlinger som er basert på samtykke, er det risiko for at fylkeskommunen behandler personopplysninger basert på ugyldige samtykker.

Fylkeskommunens styringssystem inneholder beskrivelser av hvilken informasjon som skal gis til de registrerte ved innsamling av personopplysninger. Denne beskrivelsen er i tråd med kravene som stilles i personvernforordningen.

Når det kommer til behandling basert på samtykke har KPMG også gjort undersøkelser av informasjon som gis i forbindelse med samtykker på fylkeskommunens nettsider, og har funnet eksempler der fylkeskommunen behandler personopplysninger basert på samtykke, men der informasjon ikke gis i forbindelse med samtykket. Behandling av personopplysninger vil i et slikt tilfelle mangle behandlingsgrunnlag, noe som er et alvorlig brudd på personvernforordningen.

Fylkeskommunen har for enkelte behandlinger angitt berettiget interesse, jf. GDPR art. 6 nr. 1 bokstav f), som behandlingsgrunnlag. I tilfeller hvor dette grunnlaget benyttes skal det foretas en interesseavveining mellom den behandlingsansvarliges og den registrertes interesse tilknyttet behandlingen. Ut fra foreliggende dokumentasjon og informasjon fra intervju kan KPMG ikke se at fylkeskommunen har foretatt dokumenterte interesseavveininger.

Personvernerklæringen er fylkeskommunens hovedkilde til informasjon til de registrerte. Mangler knyttet til personvernerklæringen har tidligere blitt påpekt av personvernombud i ombudets revisjon fra 2020. De påpekte forholdene er ikke rettet. Fylkeskommunen har heller ikke en personvernerklæring for egne ansatte, og det er begrenset informasjon som gis om behandling av personopplysninger til egne ansatte utover informasjon fra enkelte av systemene som benyttes i virksomheten.

I intervju informeres det om at fylkeskommunen skal utbedre personvernerklæringen, men at dette arbeidet har blitt forsinket som følge av pandemien.

<u>Anbefalinger</u>

- ✓ Fylkeskommunen bør gjennomgå og kvalitetssikre at det gis informasjon til de registrerte i de tilfeller hvor behandling er basert på den registrertes samtykke. Det bør kvalitetssikres at informasjonen som gis er i tråd med personvernforordningens krav, og at det er etablert mekanismer som sikrer at registrerte kan trekke tilbake sitt samtykke like enkelt som det ble gitt.

- ✓ Fylkeskommunen bør revidere personvernerklæringen sin, og rette opp i de avvik som tidligere er påpekt av personvernombudet.
- ✓ Fylkeskommunen bør oppdatere protokollen i de tilfeller hvor det ikke er angitt et behandlingsgrunnlag for behandlingsaktiviteter.
- ✓ Fylkeskommunen bør foreta dokumenterte interesseavveininger i de tilfeller behandling av personopplysninger er basert på behandlingsgrunnlaget berettiget interesse. Vurderingene bør inkludere de elementer som fremheves av Datatilsynet i deres veileder om behandlingsgrunnlag.

3.5.2.2 Prinsippet om formålsbegrensning

Målsetting

Fylkeskommunen samler personopplysninger inn til spesifikke, uttrykkelig angitte og berettigede formål, og viderebehandler ikke opplysningene på en måte som er uforenlig med formålene for innsamling.

Observasjoner og vurderinger

Ved vurdering av om fylkeskommunen oppfyller dette prinsippet, har KPMG særlig sett på om formål er tilstrekkelig spesifikt og uttrykkelig angitt, og om det foregår viderebehandling til andre formål.

Fylkeskommunen har spesifisert i styringssystemet at all behandling av personopplysninger skal ha et formål. Ut fra undersøkelser av blant annet protokoll, fremstår imidlertid ikke fylkeskommunens angivelse av formål som tilstrekkelig spesifisert. Dette gjelder særlig med hensyn til behandling av personopplysninger innenfor tannhelse og ved behandling av personopplysninger om fylkeskommunens ansatte.

I disse tilfellene bærer formålsangivelsen preg av å være sekkeposter som inneholder behandling til flere ulike formål med forskjellige behandlingsgrunnlag. Slik bruk av sekkeposter er ikke i tråd med prinsippet om formålsbegrensning. Det er imidlertid viktig å merke seg at dette ikke i seg selv innebærer at behandling ikke skjer til berettigede formål eller at de mangler behandlingsgrunnlag. Manglende spesifisering av formål vanskeliggjør derimot overholdelse av fylkeskommunens informasjonsplikt og gjør det utfordrende å vurdere om personopplysninger behandles til uforenlige formål. Med sekkepostangivelse av formål vil det også være vanskelig for fylkeskommunen å dokumentere at det ikke samles inn mer personopplysninger enn nødvendig for de ulike formålene.

Anbefalinger

- ✓ Fylkeskommunen bør sikre at formålene ved behandling av personopplysninger er tilstrekkelig spesifikt og uttrykkelig angitt. Fylkeskommunen bør gjennomgå og revidere protokollen over behandlingsaktiviteter for å sikre at formål ved behandling av personopplysninger er tilstrekkelig spesifikt og uttrykkelig angitt.

3.5.2.3 Prinsippet om dataminimering

Målsetting

Fylkeskommunen samler ikke inn mer personopplysninger enn det som er nødvendig for formålene de behandles for, såkalt overskuddsinformasjon.

Observasjoner og vurderinger

KPMG har særlig sett på om det er gjort vurderinger av dataminimering, om disse er dokumenterte, og om det finnes mekanismer som sikrer at det blir vurdert.

Av intervju fremgår det at det ikke er gjort noen helhetlig vurdering av fylkeskommunens innsamling og behandling av personopplysninger opp mot dataminimeringsprinsippet. Det er heller ikke etablert mekanismer for å vurdere overholdelse av prinsippet i forkant av nye behandlingsaktiviteter. Det er imidlertid oppgitt at det er gjennomført vurderinger forbundet med enkelte skjema som benyttes i fylkeskommunen.

Fylkeskommunen har svært mange papirbaserte søknadsskjema liggende på nettsidene til fylkeskommunen. I de tilfeller hvor skjema er utarbeidet før innføringen av personvern-forordningen i norsk rett, er det en risiko for at det samles inn mer personopplysninger enn nødvendig. KPMG har gjort stikkprøveundersøkelser av skjema fra fylkeskommunens nettsider, uten å ha funnet noen tilfeller hvor det klart samles inn mer personopplysninger enn det som er nødvendig for formålene de samles inn for.

Anbefalinger

- ✓ Fylkeskommunen bør vurdere om det samles inn mer personopplysninger enn det som er nødvendig for formålene opplysningene samles inn for. Dette gjelder spesielt i de tilfeller hvor fylkeskommunen samler inn særlige kategorier personopplysninger, slik som helseopplysninger. Arbeidet med vurdering av dataminimering kan gjøres som et ledd av fylkeskommunens prosjekt om prosesskartlegging.
- ✓ Fylkeskommunen bør digitalisere papirbaserte skjema, og i den forbindelse foreta en gjennomgang av hvilke personopplysninger som er nødvendig å samle inn til de ulike formålene.

3.5.2.4 Prinsippet om riktighet

Målsetting

Fylkeskommunen har mekanismer for å sikre at personopplysninger er korrekte og nødvendig oppdaterte, og treffer ethvert rimelig tiltak for å sikre at uriktige opplysninger rettes eller slettes.

Observasjoner og vurderinger

KPMG har undersøkt om det finnes mekanismer for å sikre at opplysninger er riktig, og om det finnes rutiner for å håndtere at feilaktige opplysninger blir rettet eller slettet.

Fylkeskommunen har etablerte rutiner som tar sikte på å sikre at personopplysninger er riktige, og det er også inntatt som et av fylkeskommunens «Tryggleiksmål». Fra intervju fremgår det likevel at det er uklart om det faktisk gjennomføres kontroller av opplysningers riktighet.

Anbefalinger

- ✓ Fylkeskommunen bør gjennomgå sine tiltak for å sikre personopplysningers riktighet, herunder for eksempel ved dokumentasjon av logiske kontroller i IT-systemer, og beskrivelser av mekanismer for å fange opp og rette feil.

3.5.2.5 Prinsippet om lagringsbegrensning

Målsetting

Fylkeskommunen lagrer ikke personopplysninger lenger enn det som er nødvendig for formålene de samles inn for.

Observasjoner og vurderinger

Ved vurdering av overholdelse har KPMG undersøkt om fylkeskommunen har etablert sletterutiner, om slettefrister er definert, og om det gjennomføres kontroll av om personopplysninger lagres lengre enn nødvendig for formålene de er innsamlet for.

For en stor andel av behandlingsaktivitetene i fylkeskommunen, vil det være nødvendig å behandle personopplysninger til arkivformål, og dermed oppbevare opplysningene lenger enn det formålet med innsamlingen ellers skulle tilsi. Slik lagring av personopplysninger er også tillatt etter forordningen. Når det kommer til slik behandling til arkivformål, er det imidlertid viktig å være oppmerksom på at opplysningene må oppbevares i fylkeskommunens arkiv, og slettes fra de ulike fagsystemene de er innhentet fra når det ikke lenger er nødvendig å behandle dem i slike system for formålene de ble innsamlet for.

Fylkeskommunen har i sitt styringssystem angitt at det for hver enkelt IT-system eller register skal etableres en sletterutine eller rutine for oppbevaring av opplysningene. I protokollen er det for en rekke behandlingsaktiviteter beskrevet at det finnes interne sletterutiner for personopplysninger. Det er imidlertid også en del behandlingsaktiviteter som ikke har noen angivelse av lagringstid eller slettefrister.

I intervju er det informert om at det ikke foreligger sletterutiner i alle tilfeller hvor det etter styringssystemet skulle vært etablert rutiner, men at dette har vært et fokusområde for fylkeskommunen og at det arbeides for å få slike rutiner på plass. Manglende sletterutiner medfører stor risiko for at opplysninger lagres lenger enn det som er nødvendig for formålene de er innsamlet for.

Anbefalinger

- ✓ Fylkeskommunen bør kartlegge hvor det mangler sletterutiner, og etablere slike rutiner basert på vurderinger av behovet for lagring, for å forhindre at personopplysninger ikke lagres lenger enn det som er nødvendig for å etterleve prinsippet om lagringsbegrensning.

3.5.2.6 Prinsippet om integritet og konfidensialitet

Målsetting

Fylkeskommunen behandler personopplysninger på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak.

Observasjoner og vurderinger

KPMG har ved vurderingen av overholdelse av dette prinsippet særlig undersøkt om sikkerhetsnivået og tekniske og organisatoriske tiltak er basert på gjennomførte og dokumenterte risikovurderinger.

Fylkeskommunens risikostyring er nærmere kommentert og adressert over i pkt. 3.1.3. KPMG kan ikke se at det er gjennomført dokumenterte risikovurderinger i alle tilfeller der det behandles personopplysninger. Manglende risikovurderinger gjør det vanskelig for fylkeskommunen å dokumentere at personopplysninger oppnår et tilstrekkelig sikkerhetsnivå.

Til tross for manglende dokumentasjon av risikovurderinger, har fylkeskommunen etablert flere tiltak for behandling av personopplysninger som tar hensyn til risikoen forbundet med behandlingene. For behandling av særlige kategorier personopplysninger (tidligere «sensitive personopplysninger») har fylkeskommunen gjennomført særskilte tekniske tiltak, og det er også gjennomført en rekke organisatoriske tiltak slik som opplæring, utarbeidelse av definerte rutiner og retningslinjer. Innenfor de områdene KPMG har undersøkt, herunder tannhelse, skole og samferdsel, er det høy bevissthet rundt behandling av sensitive personopplysninger.

Fylkeskommunen har definert og etablert tilgangsstyring hvor utgangspunktet for tilgang til opplysninger er tjenstlig behov. Fylkeskommunen har også etablert effektive tekniske sikkerhetstiltak, noe som er adressert over under vurdering av hovedproblemstilling 4 om robusthet mot digitale trusler.

Anbefalinger

- ✓ Fylkeskommunen bør sikre at det gjennomføres risikovurderinger i tilfeller hvor det behandles personopplysninger, i tråd med anbefalingene over under pkt. 3.1.3, og gjennomføre vurderinger av personvernkonsekvenser slik som nevnt under pkt. 3.5.4.

3.5.3 Informasjon til de registrerte

Målsetting

Fylkeskommunen har truffet egnede tiltak for å fremlegge informasjon når informasjon samles inn fra den registrerte eller når den samles inn fra andre enn den registrerte etter artikkel 12, 13 og 14. Informasjonen gis på tidspunktet for innsamling når personopplysninger innsamles fra den det gjelder, eller innen rimelig tid etter at de ble samlet inn når de er samlet inn fra andre enn den registrerte.

Observasjoner og vurderinger

KPMG har særlig vurdert om det gis informasjon til de registrerte i tråd med bestemmelsene i forordningen. Det er i tillegg særlig sett på om fylkeskommunen har etablert et personvernerklæring som oppfyller kravene til informasjon.

Fylkeskommunen har en personvernerklæring som er publisert på fylkeskommunens nettsider. Erklæringen er overordnet, og personvernombudet har tidligere påpekt svakheter ved personvernerklæringen som ikke er rettet. Dette er særlig knyttet til beskrivelser av formålene for behandling, som i liten grad er omtalt i erklæringen.

I styringssystemet for informasjonssikkerhet og personvern er det oppstilt krav til hvilken informasjon som skal gis til de registrerte. Utgangspunktet som skisseres i handboka er i tråd med forventningene i personvernforordningen.

Fylkeskommunen benytter papirbaserte skjema til en stor del av sin innsamling av personopplysninger. De fleste skjemaene som er kontrollert, inneholder ikke informasjon om behandling av personopplysninger. En del av skjemaene inneholder en henvisning til

personvernerklæring, men denne vil ikke alene oppfylle informasjonsplikten, blant annet som følge av manglene formålsangivelse som påpekt av personvernombudet.

Med hensyn til informasjon i digitale tjenester og løsninger som leveres av fylkeskommunen, er det varierende hvilken informasjon som gis. I enkelte av de undersøkte tjenestene er det utarbeidet egne personvernerklæringer som oppfyller informasjonsplikten, mens det for andre tjenester slik som nyhetsbrev eller rekruttering ikke gis tilstrekkelig informasjon.

Fylkeskommunen har ikke utarbeidet en egen personvernerklæring for ansatte i fylkeskommunen. I intervju fremgår det likevel at enkelte av de interne systemene har informasjon om de konkrete behandlingene. Det fremgår også informasjon av interne rutiner og retningslinjer, slik som retningslinjer for bruk av e-post, hvor det beskrives vilkår for arbeidsgivers innsyn i e-postboks. Fylkeskommunen har et behandlingsansvar for personopplysninger om egne ansatte, og det er viktig at det gis informasjon også til denne gruppen om hvordan og til hvilke formål det behandles personopplysninger om dem.

I intervju er det presisert at informasjon til de registrerte vil inntas i fylkeskommunens årshjul for å sikre at erklæringer og informasjon oppdateres jevnlig og ved behov. Ut fra de undersøkelser som er gjort, og den informasjonen som er innhentet, oppfylles ikke informasjonsplikten overfor registrerte i dag.

Anbefalinger

- ✓ Fylkeskommunen bør revidere personvernerklæringen sin i tråd med anbefalingene fra personvernombudets revisjon fra 2020.
- ✓ Fylkeskommunen bør utarbeide en personvernerklæring til sine egne ansatte for å sikre at ansatte mottar den informasjonen de har rett på.
- ✓ Fylkeskommunen bør inkludere informasjon om behandling av personopplysninger i de skjema som ligger tilgjengelig på fylkeskommunens nettsider, eller henvise til hvor de registrerte kan finne slik informasjon.
- ✓ Fylkeskommunen bør særlig gjennomgå informasjon som gis der behandling av personopplysninger er basert på de registrertes samtykke.

3.5.4 Behandlingsansvarliges ansvar og sikkerhet ved behandling

Målsetting

Fylkeskommunen har implementert egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandling av personopplysninger skjer i tråd med bestemmelsene i forordningen, herunder art. 24 og 32. Tiltak, som skal ta hensyn til risiko, oppdateres ved behov. Det er gjennomført vurderinger av personvernkonsekvenser (DPIA) i de tilfeller hvor en behandling kan innebære høy risiko for personvernet, jf. Art. 35.

Observasjoner og vurderinger

Ved vurdering av etterlevelse av bestemmelsene om ansvar og sikkerhet ved behandling har KPMG særlig vurdert om tiltak er basert på risikovurderinger, og om det finnes rutiner og prosesser for å sikre at tiltak gjennomgås og oppdateres ved behov.

Etter handbok for personvern og informasjonssikkerhet skal det gjennomføres risikovurderinger ved behandling av personopplysninger. Det skal alltid gjennomføres risikovurdering før en ny behandling gjennomføres, og i forbindelse med avvikshåndtering.

Fylkeskommunen kan ikke dokumentere at det er gjennomført risikovurderinger for alle sine behandlinger av personopplysninger. Dette understøttes også av informasjon fra intervju. Der det er gjennomført risikovurderinger kan det heller ikke dokumenteres at disse oppdateres ved behov.

I forbindelse med anskaffelser av nye systemer, har fylkeskommunen utarbeidet et sett med standardkrav som stilles i kravspesifikasjoner. Disse kravene er imidlertid generelle og tilpasses ikke til den enkelte anskaffelse. Kravene som stilles fremstår ikke egnet for å skille ut hvilke digitale løsninger og systemer som best ivaretar personvern, og tilbydere vurderes heller ikke på sine besvarelser av kravene.

Når det kommer til tekniske sikkerhetstiltak gjennomfører fylkeskommunen vurderinger av sikkerheten løpende, og tiltak oppdateres ved behov. For de organisatoriske tiltakene kan ikke fylkeskommunen dokumentere at tiltak er basert på risikovurderinger, og at tiltak oppdateres ved behov. Dette gjelder særlig med tanke på rutiner, avtaler og opplæring til ansatte. Fylkeskommunen har imidlertid et prosjekt som går på kompetanse-styringssystem, hvor et av formålene er ivaretakelse av regulatoriske krav herunder knyttet til behandling av personopplysninger.

Fra intervju fremgår det at fylkeskommunen gir informasjon til sine ansatte om endringer av trusselbildet som de må forholde seg til gjennom informasjon på intranett. Det er imidlertid ikke gjennom dokumentasjon eller intervju mottatt informasjon om at endringer av eksempelvis trusselbilde også innebærer vurdering og eventuelt justering av rutiner og avtaler.

I personvernerklæringen er det for en rekke behandlingsaktiviteter oppgitt at behandling kan innebære høy risiko for personvernet. I slike tilfeller skal det gjennomføres en vurdering av personvernkonsekvenser. Dette er imidlertid ikke gjort i fylkeskommunen. Det mangler også definerte kriterier for å vurdere om det kan foreligge høy risiko for personvernet, og støtteverktøy slik som maler for å gjennomføre vurderingen. Manglende gjennomføring av DPIA i de tilfeller hvor det kan foreligge høy risiko for personvern innebærer brudd på bestemmelsen i personvernforordningen art. 35.

Anbefalinger

- ✓ Fylkeskommunen bør gjennomføre risikovurderinger for sine behandlinger av person-opplysninger, og sikre at slike vurderinger gjennomføres for nye behandlinger, herunder slik som anskaffelse av nytt sak- og arkivsystem.
- ✓ Fylkeskommunen bør basere krav i sine anskaffelser på gjennomførte risiko-vurderinger.
- ✓ Fylkeskommunen bør gjennomføre vurderinger av personvernkonsekvenser i de tilfeller der det er identifisert at behandling kan innebære høy risiko for personvernet. Fylkeskommunen bør gjennomføre en kartlegging for å identifisere behandlings-aktiviteter som kan innebære høy risiko, og utarbeide maler for å gjennomføre vurderingen.

3.5.5 Innebygd personvern og personvern som standardinnstilling

Målsetting

Fylkeskommunen har definert og implementert prinsippene om innebygd personvern og personvern som standardinnstilling prosesser der det er relevant, herunder særlig ved utvikling av IT-systemer og i forbindelse med anskaffelser.

Observasjoner og vurderinger

Ved vurdering av om prinsippet overholdes, har KPMG særlig sett på fylkeskommunens rutiner for ivaretakelse av innebygd personvern og personvern som standardinnstilling.

Av intervju har det fremgått at fylkeskommunen i svært liten grad utvikler egne digitale løsninger. Det finnes ikke rutiner som er ment å sikre prinsippene ved slik utvikling. Innebygd personvern og personvern som standardinnstilling er ikke nevnt i styringssystemet, eller i rutiner som gjelder for anskaffelser av nye IT-systemer. Fylkeskommunen har etablert et sett med standardiserte krav for ivaretakelse av personvern ved anskaffelse av informasjonssystemer, men disse inneholder heller ikke referanser til de omtalte prinsippene.

Fra intervju har det kommet frem at innebygd personvern og personvern som standardinnstilling ikke har vært et fokusområde i fylkeskommunen. Det har imidlertid fått økt fokus nå, og det er blant annet tatt inn som en forventning til nytt sak- og arkivsystem i «D. Prosjektgjennomføringsdokument med alle vedlegg Sak og Arkiv».

Anbefalinger

- ✓ Fylkeskommunen bør inkludere prinsipper om innebygd personvern og personvern som standardinnstilling i rutinene i styringssystemet sitt.
- ✓ Fylkeskommunen bør inkludere krav til innebygd personvern og personvern som standardinnstilling ved innkjøp av IT-systemer hvor det skal behandles personopplysninger.

3.5.6 Databehandlere

Målsetting

Fylkeskommunen benytter bare databehandlere som gir tilstrekkelige garantier for oppfyllelse av krav og forventninger i forordningen, og det er inngått databehandleravtale som regulerer behandlingen. Fylkeskommunen gjennomfører kontroll av sine databehandlere for å sikre at de overholder avtalens bestemmelser i hele avtaleperioden.

Observasjoner og vurderinger

KPMG har ved undersøkelse av om dette kravet oppfylles sett på hvilke krav som stilles til databehandlere før avtaleinngåelse, om det inngås databehandleravtaler, og om databehandlere følges opp i avtaleperioden.

I forbindelse med anskaffelsesprosesser stilles det krav til at leverandører skal dokumentere sin behandling av personopplysninger og sikkerheten rundt slik behandling. Slike krav er inntatt i de standardkravene som fylkeskommunen stiller i sine konkurransegrunnlag. Fylkeskommunen krever blant annet at databehandlere før avtaleinngåelse beskriver og dokumenterer de tekniske og organisatoriske sikkerhetstiltak som er på plass, og har oppstilt mer detaljerte krav innenfor enkelte sentrale områder. Databehandlere må også bekrefte at de har tilstrekkelige menneskelige og tekniske ressurser til å oppfylle betingelsene i kontrakten og sikre etterlevelse av personvernforordningen.

At fylkeskommunen har utarbeidet et sett med standardkrav, bidrar til å sikre at det stilles krav til behandling av personopplysninger i anskaffelser, noe som er positivt. Kravene som stilles i anskaffelser er imidlertid ikke basert på dokumenterte risikovurderinger og tilpasses i liten grad risiko forbundet med behandling. Tilbyderne evalueres heller ikke på sine besvarelser av kravene.

Fylkeskommunen har etablert egen mal for databehandleravtaler som oppfyller de kravene som stilles i personvernforordningen art. 28. Fra intervju fremgår det også at fylkeskommunen har inngått databehandleravtale med sine databehandlere. Ved gjennomføring av anskaffelser oppstilles det absolutte krav om at det skal inngås databehandleravtale i de tilfeller hvor det foreligger en databehandlerrelasjon. Dette bidrar til å sikre at fylkeskommunen har slike avtaler på plass.

I plikten til å bare benytte databehandlere som gir tilstrekkelig garantier for oppfyllelse av forordningen ligger det også et kontrollelement. Den behandlingsansvarlige skal føre kontroll med at databehandlerne overholder sine forpliktelser gjennom hele avtaleperioden. Hvor hyppig og grundig slike kontroller bør være, avhenger av risikoen forbundet med behandlingen. Ut fra intervju, fremgår det at fylkeskommunen gjennomfører enkelte slike kontroller av sine databehandlere, i tråd med beskrivelsene om oppfølging av databehandlere slik disse er beskrevet i styringssystemet. Kontrollerne fremstår imidlertid ikke systematisk, og i stedet tilfeldig. I intervju er det oppgitt at kontroll av leverandører har blitt nedprioritert som følge av kapasitetsutfordringer.

Anbefalinger

- ✓ Fylkeskommunen bør tilpasse krav som stilles til sine databehandlere basert på risikovurderinger. Standardkrav kan fungere som et godt utgangspunkt, men bør tilpasses. Slik tilpasning av standardkrav krav bør ses i sammenheng med fylkeskommunens arbeid med informasjonsklassifisering, slik at klassifisering avgjør hvilket sett med standardkrav som fungerer som et utgangspunkt.
- ✓ Fylkeskommunen bør systematisere sitt arbeid med oppfølging av databehandlere. Det danske Datatilsynet har laget en veileder som kan benyttes som utgangspunkt i forbindelse med vurdering av kontrollers hyppighet og intensitet.

3.5.7 Protokoll over behandlingsaktiviteter

Målsetting

Fylkeskommunen holder oversikt over sine behandlinger av personopplysninger i en protokoll over behandlingsaktiviteter. Protokollen oppfyller innholdsmessig kravene som fremgår av forordningens art. 30 nr. 1.

Observasjoner og vurderinger

For å undersøke forordningens protokollkrav, har KPMG vurdert om det er etablert en protokoll over behandlingsaktiviteter, om protokollen er riktig utfylt og inneholder påkrevd informasjon, og i tillegg om fylkeskommunen har etablert systemer for å sikre at protokollen holdes oppdatert.

Fylkeskommunen har rutiner for føring av protokoll over behandlingsaktiviteter i styringssystemet, og det er etablert en protokoll over behandlingsaktiviteter. Denne protokollen er basert på Datatilsynets mal, og inneholder flere informasjonselementer enn det som er påkrevd etter forordningens art. 30. Innenfor utdanning er det i tillegg til hovedprotokollen etablert en egen protokoll over behandlingsaktiviteter basert på den samme malen fra Datatilsynet.

Når det kommer til utfylling av protokollen har protokollen enkelte mangler, noe som også er omtalt over under behandlingen av vurderingen av de grunnleggende prinsippene. Personvernombudet påpekte mangler knyttet til protokollen i sin revisjon fra 2020, og en del av funnene fra revisjonen er rettet opp i ettertid.

Etter fylkeskommunens styringssystem, er det sikkerhetsansvarlig som har ansvaret for sine områder for etterlevelse av krav i handboka og regelverket. Basert på intervjuer, fremstår det imidlertid ikke som om denne plikten nødvendigvis er forstått når det kommer til protokollen. Selv om fylkeskommunen har tildelt ansvaret for å holde protokollen oppdatert og riktig utfylt, etterleves ikke dette i praksis i alle sammenhenger. I intervju er det informert om at faggruppen fremover kommer til å spille en sentral rolle i arbeidet med å oppdatere og holde protokollen oppdatert.

Anbefalinger

- ✓ Fylkeskommunen bør revidere protokoll over behandlingsaktiviteter for å sikre at den er dekkende med hensyn til fylkeskommunens behandling av personopplysninger.
- ✓ Fylkeskommunen bør sikre at protokollen holdes oppdatert, blant annet ved å etablere faste rapporterings/kontrollpunkter gjennom året, sørge for at faggruppen har tilstrekkelig innsikt i protokollen, og ved å inkludere oppdatering av protokoll i sjekklister eller tilsvarende i linjen.

3.5.8 Melding til tilsynsmyndighet

Målsetting

Fylkeskommunen har mekanismer for å fange opp brudd på personopplysnings-sikkerheten, og rutiner for å vurdere avvik og eventuelt melde avvik til Datatilsynet og de registrerte.

Observasjoner og vurderinger

Ved vurdering av etterlevelse har KPMG særlig sett på om fylkeskommunen har etablerte rutiner og prosesser for å fange opp, vurdere og melde inn brudd på personopplysnings-sikkerheten, og om disse rutinene fungerer i praksis.

Fylkeskommunen har etablert tydelige og detaljerte rutiner når det kommer til sin avviks-håndtering. Avvik skal meldes inn via systemet Risk Manager, der det gjennomføres en vurdering av de innmeldte avvik. I tilfeller avvik skal meldes til Datatilsynet konsulteres personvernombudet.

Når det kommer til mekanismer for å fange opp avvik, har fylkeskommunen oppgitt at det er gjennomført opplæring i avvik og avvikshåndtering for ansatte i fylkeskommunen. Det finnes tydelige rutiner, og det er dokumentert at det meldes inn avvik i avvikssystemet.

Fylkeskommunen har oversikt over innmeldte avvik, og kan dokumentere at det er gjort vurderinger av personvernrisiko forbundet med de innmeldte avvikene. I de tilfeller hvor et avvik innebærer risiko for de registrerte, har personvernombudet blitt involvert, og det har blitt meldt avvik til Datatilsynet i tråd med fylkeskommunens rutiner.

Anbefalinger

- ✓ Fylkeskommunen bør med jevne mellomrom sikre at ansatte informeres og bevisst-gjøres om hva som utgjør et brudd på personopplysningssikkerheten, hvordan det skal meldes og hvordan slike avvik behandles.

3.5.9 Personvernombud

Målsetting

Personvernombudets rolle og oppgaver er beskrevet i personvernforordningens artikkel 37-39, som blant annet regulerer hvilke oppgaver ombudet minst skal utføre, når ombudet skal involveres, og bestemmelser om ombudets uavhengighet.

Observasjoner og vurderinger

For å vurdere personvernombudsrollen, har KPMG særlig sett på om fylkeskommunen har et personvernombud, om det er tilstrekkelig uavhengig, om det har tilgang på ledelsen, om oppgavene og rollen er spesifisert, om ombudet utfører sine oppgaver, og om ombudet har tilstrekkelige ressurser for å utføre de oppgavene som ligger til rollen.

Fylkeskommunen har et personvernombud som er ansatt ved Interkommunalt Arkiv for Møre og Romsdal (IKAMR). Plassering utenfor organisasjonen bidrar til å sikre uavhengighet og manglende konflikt med øvrige oppgaver. I tillegg til å være personvern-ombud for fylkeskommunen, er ombudet også personvernombud for seks andre kommuner i fylket.

KPMG gjennomførte i 2019 en evaluering av ordningen med personvernombudstjenesten som leveres fra IKAMR. I evalueringen ble det særlig trukket frem følgende forbedrings-punkter:

- ✓ Rapportering til øverste leder. Det er indikasjoner på at ombudet i praksis ikke rapporterer til virksomhetens øverste leder hos enkelte av prosjektdeltakerne (POL Artikkel 38 (3)).
- ✓ Kapasitet. Det vurderes som sannsynlig at personvernombudet pt. Ikke har tilstrekkelig tid til å gjennomføre alle sine forpliktelser iht. regelverket på betryggende vis (POL Artikkel 38 (2))
- ✓ Risikovurdering. Personvernombudene har ikke i tilstrekkelig grad vurdert om risikoen er forbundet med behandlingsaktivitetene prosjektdeltakerne utfører (POL Artikkel 39 (2))
- ✓ Etterlevelseskontroll. Ombudet utfører i begrenset grad kontroll av virksomhetens etterlevelse av personopplysningsloven (POL Artikkel 39 (1, b))

Personvernombudets oppgaver er beskrevet i styringssystemet. IKAMR har også beskrivelser av personvernombudets oppgaver på sine nettside. De to beskrivelsene er ikke helt sammenfallende, og listen over oppgaver i handboka inneholder flere elementer, eksempelvis knyttet til ansvar for å samle inn og identifisere behandlingsaktiviteter og bidra til å få oversikt over behandlingene i fylkeskommunen. I styringssystemet er det angitt at personvernombudet skal delta under leiingas gjennomgang slike denne er beskrevet i styringssystemets pkt. 3.3.4. Fylkeskommunens ledelse har imidlertid ikke gjennomført en slik gjennomgang, og dette har derfor foreløpig ikke vært aktuelt.

Ut fra intervju og den dokumentasjon KPMG har fått oversendt, bidrar personvernombudet med sporadisk rådgivning til fylkeskommunen i spørsmål om personvern. Det opplyses om at det særlig er gitt bistand i forbindelse med en ny behandlingsaktivitet innenfor tannhelse i 2021. Spørsmål kanaliseres i hovedsak via fagleder for informasjonssikkerhet som i intervju er oppgitt som ombudets hovedkontaktpunkt i fylkeskommunen. I tillegg har ombudet gjennomført en revisjon av protokoll og personvernerklæring i 2020, deltatt i avvikshåndtering/innmelding, og delt et opplæringsopplegg med fylkeskommunen innenfor personvern høsten 2021.

Personvernombudet utarbeider årlig en årsrapport som har blitt sendt til ledelsen i fylkeskommunen og fagleder informasjonssikkerhet. Årsrapporten inneholder informasjon om gjennomførte og planlagte leveranser, og beskriver ombudets involvering i arbeidet med personvern i fylkeskommunen. Med hensyn til funn fra KPMGs tidligere evaluering av ordningen kan det se ut som om at det er truffet enkelte tiltak for å kompensere for funn knyttet til ledelsesrapportering. Den aktuelle rapporteringen til ledelsen fremstår imidlertid overfladisk, og gir ikke et dekkende bilde av status for arbeidet med personvern eller risiko for personvernet i fylkeskommunen. Ombudet har ikke kontakt med fylkeskommunens ledelse utover oversendelsen av den aktuelle årsrapporten.

Når det kommer til personvernombudets kapasitet, er dette nylig noe forbedret sammenlignet med utgangspunktet for KPMGs forrige undersøkelse. Ombudet har nå ansvaret for seks kommuner i tillegg til fylkeskommunen, i motsetning til utgangspunktet ved forrige evaluering der ombudet hadde ansvaret for 13 og 14 virksomheter. Til tross for forbedringer på dette punktet, fremstår det fortsatt som et høyt antall virksomheter dersom ombudet skal ivareta alle sine oppgaver på en tilfredsstillende måte for alle virksomhetene. Dette understøttes også av informasjon fra intervju, hvor det fremgår at antallet ville vært for høyt dersom alle virksomhetene skulle følges opp i tråd med kravene i forordningen.

Et av hovedfunnene fra forrige undersøkelse var at ombudene i IKAMR ikke i tilstrekkelig grad har vurdert risiko forbundet med behandlingsaktivitetene i virksomhetene de er ombud for. Ut fra beskrivelser i intervju er dette fortsatt situasjonen. Ut fra de tilganger ombudet har til informasjon vil det også være vanskelig å foreta en dekkende risikovurdering av status for personvern i fylkeskommunen. Ombudet har ikke tilgang til fylkeskommunens systemer, og det er heller ikke noen faste møtepunkter mellom fylkeskommunen og ombudet der ombudet kan få informasjon om fylkeskommunens arbeid med personvern. Tilgang til informasjon er en forutsetning for at ombudet skal kunne arbeide risikobasert.

Med hensyn til ombudets arbeid med kontroll av etterlevelse, ble det gjennomført en gjennomgang av protokoll over behandlingsaktiviteter og personvernerklæring i 2020. Fra ombudets side ble det bedt om dokumentasjon for å gjennomføre en planlagt og varslet kontroll av fylkeskommunen i 2021 rettet mot databehandleravtaler og samtykkeskjema, men dette ble ikke gjennomført fordi ombudet ikke mottok dokumentasjon.

Ut fra den foreliggende dokumentasjon og informasjon fra intervju, utføres ikke alle oppgaver som ombudet skal utføre i tråd med bestemmelsene i personvernforordningen eller i styringssystemet. Personombudets kontroll av etterlevelse har vært begrenset, og KPMG har fått dokumentasjon på at det er gjennomført én slik kontroll etter at personvernforordningen trådte i kraft.

En del av oppgavene er det ut fra dagens organisering også vanskelig å se at ombudet kan utføre på en effektiv måte som følge av manglende tilgang på informasjon. Med utgangspunkt i gjennomførte intervju, fremstår det også tilfeldig om og eventuelt når personvernombudet involveres i prosesser av betydning for personvernet i fylkeskommunen.

Anbefalinger

- ✓ Fylkeskommunen bør etablere faste og hyppige møtepunkter mellom fylkeskommunen og personvernombud, og gi tilgang til relevante informasjonssystemer slik som intranett og Risk Manager, for å sikre at personvernombudet har tilstrekkelig tilgang til informasjon.

- ✓ Personvernombudet bør jevnlig, og minst årlig rapportere til ledelsen på ombudets vurdering av personvernrisiko i fylkeskommunen.
- ✓ Fylkeskommunen bør jevnlig informere alle ansatte om personvernombudet og dets oppgaver, for å sikre at ombudet er tilstrekkelig kjent i organisasjonen.
- ✓ Fylkeskommunen bør tydeliggjøre sine retningslinjer med tanke på når personvernombudet skal involveres.
- ✓ Fylkeskommunen bør sikre at personvernombudet har mulighet til å gjennomføre sine kontrollaktiviteter. Personvernombudets kontroller bør baseres på vurderinger av personvernrisiko i fylkeskommunen.
- ✓ Fylkeskommunen bør involvere personvernombudet i sentrale prosjekter og prosesser i fylkeskommunen slik som ved anskaffelse av et nytt sak- og arkivsystem, prosjekt for prosesskartlegging, og prosjekt om kompetansestyring.

3.5.10 Overføring av personopplysninger til tredjeland

Målsetting

Fylkeskommunen har kartlagt sine overføringer av personopplysninger til tredjeland, har identifisert overføringsgrunnlag etter personvernforordningen kapittel V, og har implementert tiltak for sin overføring som sikrer at overførte personopplysninger oppnår et tilsvarende beskyttelsesnivå som innenfor EU/EØS.

Observasjoner og vurderinger

Etter EU-domstolens dom i sak C-311/181 (Schrems ii-dommen), har adgangen til å overføre personopplysninger til land utenfor EU/EØS, såkalte tredjeland, blitt innskjerpet sammenlignet med tidligere. I Schrems ii-dommen konstaterte EU-domstolen for det første at overføringer til USA basert på Privacy Shield-avtalen mellom EU og USA ikke lenger var et lovlig. For det andre presiserte domstolen at det heller ikke alltid vil være tilstrekkelig å basere en overføring av personopplysninger til tredjeland på avtalemekanismer slik som standard personvernbestemmelser (SCC) eller bindende virksomhetsregler (BCR), fordi slike avtalemekanismer ikke er bindende for myndighetene i landene det overføres til. Kjernen i dommen er at virksomheter som ønsker å overføre personopplysninger ut av EU/EØS må sikre at opplysningene oppnår et tilsvarende beskyttelsesnivå som innenfor EU/EØS.

I etterkant av dommen har European Data Protection Board (EDPB) og Datatilsynet kommet med veiledere som beskriver hva virksomheter må gjøre for å sørge for at eventuelle overføringer skal skje i tråd med personvernforordningen. Ved vurdering av om fylkeskommunen overholder forpliktelser ved overføring av personopplysninger, har KPMG vurdert om fylkeskommunen har gjennomført en kartlegging av sine overføringer til tredjeland, om overføringsgrunnlagene overføringene er basert på er identifisert, om fylkeskommunen har vurdert regelverk og praksis i tredjelandet det overføres personopplysninger til, og om det er implementert tiltak for å sikre at beskyttelsesnivået er i tråd med nivået innenfor EU/EØS.

I fylkeskommunens protokoll over behandlingsaktiviteter er det ikke angitt at det skjer overføringer til tredjeland. Tilsvarende er beskrevet i fylkeskommunens personvernerklæring. Fylkeskommunen benytter imidlertid tjenester som kan innebære slik overføring, herunder eksempelvis tjenester fra store skyleverandører som Google og

Microsoft. I intervju er det oppgitt at det ikke er gjennomført vurderinger av fylkeskommunens eventuelle overføringer til tredjeland. Det er imidlertid oppgitt at det er fokus på problematikken ved inngåelse av nye avtaler, og at det også er stanset et prosjekt med leverandør i tredjeland.

Anbefalinger

- ✓ Fylkeskommunen bør gjennomføre kartlegging rettet mot sine databehandlere for å identifisere eventuelle overføringer av personopplysninger til tredjeland. I den grad slike overføringer identifiseres, bør fylkeskommunen identifisere hvilket overføringsgrunnlag overføringen baserer seg på, og om det er behov for å implementere ytterligere tekniske eller organisatoriske tiltak for å sikre at de overførte opplysningene oppnår et tilsvarende beskyttelsesnivå som innenfor EU/EØS.

3.5.11 Oppsummering

Hovedproblemstillingen i dette delkapitlet var om fylkeskommunen oppfyller sentrale krav i personvernforordningen. Som gjennomgått i de foregående punktene, har fylkeskommunen på et overordnet nivå etablert rutiner som er ment å sikre ivaretakelse av forordningen. Ut fra undersøkelsen er inntrykket at disse rutinene ikke i tilstrekkelig grad er operasjonalisert og gjennomført i organisasjonen.

Fylkeskommunen kan ikke i tilstrekkelig grad dokumentere etterlevelse av de grunnleggende prinsippene. Dette gjelder på flere punkter, der det mest alvorlige er manglende behandlingsgrunnlag ved behandling av personopplysninger på grunnlag av de registrertes samtykke.

Fylkeskommunen gir ikke tilstrekkelig informasjon til de registrerte om sine behandlinger. Det er kjente mangler ved personvernerklæringen som ikke er rettet, og det gis generelt for lite informasjon om fylkeskommunens behandling av personopplysninger på innsamlingstidspunktet. I tillegg gis det i liten grad informasjon til de ansatte om behandling av personopplysninger om dem.

Fylkeskommunen har ikke gjennomført risikovurderinger for alle sine behandlinger, og det er ikke gjennomført vurderinger av personvernkonsekvenser (DPIA) selv om fylkeskommunen har identifisert behandlingsaktiviteter som kan innebære høy risiko for personvernet. Databehandlere følges bare opp i varierende utstrekning.

Fylkeskommunen har etablert et personvernombud, men det er gjennom undersøkelsen avdekket at personvernombudet ikke har tilstrekkelig tilgang på ledelsen, at ombudet ikke har tilgang til informasjon, at det ikke involveres i tilstrekkelig grad i de tilfeller hvor ombudet burde vært involvert, at det ikke utfører alle oppgavene som ligger til rollen og at ombudet ikke i tilstrekkelig grad arbeider risikobasert opp mot fylkeskommunen.

Fylkeskommunen har ikke gjennomført kartlegginger av sine potensielle overføringer av personopplysninger til tredjeland, og dermed heller ikke identifisert overføringsgrunnlag, eller gjennomført tiltak i de tilfellene der det kan være behov for dette for å sikre et tilsvarende beskyttelsesnivå som innenfor EU/EØS.

4 Anbefalinger

KPMG har i dette oppdraget vurdert og undersøkt om fylkeskommunen oppfyller sentrale krav og forventninger knyttet til fem definerte hovedproblemstillinger. Ved gjennomgangen av fylkeskommunens arbeid med informasjonssikkerhet og personvern, har KPMG benyttet standardene ISO/IEC 27001, NSMs grunnprinsipper for IKT-sikkerhet v. 2.0, og personvernforordningen (GDPR) som vurderingskriterier. Det er en viss overlapp mellom forventninger i de tre ramme- og regelverkene, noe som gjenspeiles i både i funn og i anbefaleringer innenfor de enkelte problemstillinger. På et overordnet nivå har fylkeskommunen etablert et styringssystem for informasjonssikkerhet og personvern, samt implementert tilstrekkelige kontroller som sikrer et godt teknisk sikkerhetsnivå. Det finnes likevel en del forbedringspunkter innenfor de ulike områdene som er vurdert i denne undersøkelsen. I fortsettelsen vil de mest sentrale funn fra undersøkelsen gjengis, sammen med en vurdering av hvordan fylkeskommunen bør prioritere sine ressurser for å lukke dem.

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
1		Internkontroll - Ledelsesforankring Fylkeskommunen har ikke i tilstrekkelig grad sikret at styringssystemet for informasjonssikkerhet og personvern fungerer etter hensikten. Det skjer ingen fast rapportering til ledelsen for informasjonssikkerhet og personvern, det gjennomføres ikke egenkontroller, revisjoner, øvelser eller ledelsens gjennomgang. Ut fra funnene i denne undersøkelser fremstår ikke fylkeskommunens styringssystem tilstrekkelig operasjonalisert i organisasjonen og det er ikke i tilstrekkelig grad fulgt opp fra ledelsen.	✓ Ledelsen i fylkeskommunen bør sikre at styringssystemet for informasjonssikkerhet fungerer, og at det etterleves. Ledelsen bør med jevne mellomrom vurdere om styringssystemet fungerer etter hensikten, og følge opp status på arbeid med informasjonssikkerhet og personvern. ✓ Det bør etableres faste punkter for rapportering på definerte måleparametere til fylkeskommunens ledelse.

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
2	●	**Internkontroll - Risikostyring** Fylkeskommunen har ikke gjennomført risikovurderinger i alle tilfeller hvor dette etter styringssystemet eller eksterne krav er påkrevd, herunder ved behandling av personopplysninger. Risikovurderinger oppdateres heller ikke i tråd med sine gyldighetsperioder, eller ved eksterne endringer slik som endringer av trusselbilde. Fylkeskommunen har ikke i tilstrekkelig grad definert et nivå for akseptabel risiko for fylkeskommunen, og det fremstår også uklart hvem som kan akseptere risiko i fylkeskommunen. Det er ikke i tilstrekkelig grad gjennomført verdi- eller konsekvens-vurderinger av fylkeskommunens system- og tjenesteportefølje. Det er kvalitetsmessig variasjon på det de risikovurderinger som er gjennomført. Risikovurderinger behandler ikke alltid aktuelle scenarier, det er i varierende grad redegjort for vurderinger av sannsynlighet og konsekvens, og det er ikke alltid klart hvordan risikoreduserende tiltak er egnet til å redusere identifisert risiko.	✓ Fylkeskommunen bør etablere kontroll-mekanismer som sikrer at risikovurderinger gjennomføres i relevante arbeidsprosesser i linjen. ✓ Etablere prosesser og rutiner som sikrer at risikovurderinger oppdateres ved større endringer, herunder slik som ved endret/skjerpet trusselbilde og at det sikres at de gjennomgås . ✓ Tydeliggjøre og definere hva som utgjør akseptabel risiko for fylkeskommunen. ✓ Fylkeskommunen bør gjennomføre verdi/konsekvensvurderinger av sine tjenester, prosesser og systemer, for å vurdere risiko på et overordnet nivå. ✓ Fylkeskommunen bør tydeliggjøre hvem som kan akseptere ulike nivå av risiko i organisasjonen, herunder hvem som kan akseptere restrisiko, og hvem som kan beslutte tiltak.
3	●	**Internkontroll - Overvåkning og kontroll** Fylkeskommunen har definerte prosesser for overvåkning, måling, analyse og evaluering. Disse etterleves imidlertid ikke i praksis. Det gjennomføres ikke revisjoner eller egenkontroll, og det gjennomføres ikke systematisk oppfølging fra ledelsen i form av ledelsens gjennomgang.	✓ Fylkeskommunen bør gjennomføre årlig revisjon eller egenkontroll for å sikre at implementerte kontroller og sikkerhetsmekanismer fungerer etter hensikten og at fylkeskommunen når målene som er satt for arbeidet med informasjonssikkerhet og personvern. Revisjon og egenkontroll bør være risikobasert og innrettet og fokusert mot de områdene med

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
		Etter fylkeskommunens kontinuitetsplan, skal det gjennomføres minst tre tester/øvelser per år, herunder to enkle tester og minst en avansert test. KPMG kan ikke se at dette er gjennomført.	høyest risiko. For å tydeliggjøre en slik risiko-basert tilnærming, bør beskrivelser av revisjoner i styringssystemet justeres. ✓ Ved oppfølging av risikovurderinger, egenkontroll og revisjon, samt resultater fra ledelsens gjennomgang, bør fylkeskommunen utarbeide handlingsplaner for å sikre at de har tilstrekkelig oversikt og at tiltak prioriteres basert på risiko. Ledelsen i fylkeskommunen bør sikre at slike handlingsplaner følges opp med jevne mellomrom, for eksempel i form av fast status-rapportering, for å sikre at avvik lukkes i tråd med vedtatte handlingsplaner. ✓ Fylkeskommunen bør sikre at det settes av tilstrekkelig med ressurser til å gjennomføre revisjonene som spesifisert i styringssystemet.
4	●	**Ansvar og oppgaver** Fylkeskommunen har på et overordnet nivå beskrevet de ulike rollene som skal inngå i det daglige arbeidet med informasjonssikkerhet og personvern. Ut fra foreliggende dokumentasjon og informasjon, fremstår ikke innholdet i rollene forstått av alle rolleinnehavere. Dette gjelder særlig for faggruppe for personvern og informasjonssikkerhet som først nylig ble etablert. Ut fra funnene i undersøkelsen, er det også en rekke oppgaver som er beskrevet i fylkeskommunens styringssystem som ikke utføres.	✓ Fylkeskommunen bør tydeliggjøre ansvar og oppgaver knyttet til de ulike rollene i fylkes-kommunen, herunder særlig for sikkerhets-ansvarlig og faggruppe for informasjons-sikkerhet. Fylkeskommunen bør lage tydelige instrukser, som tydelig beskriver grensegangen mellom ulike rollers ansvar og oppgaver. ✓ Fylkeskommunen bør definere et mandat for faggruppen, der målene for faggruppen beskrives. Det bør også etableres faste arenaer

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
			for faggruppen, og defineres hva faggruppen skal rapportere på og til hvem. ✓ Fylkeskommunen bør etablere mekanismer som sikrer at oppgaver og ansvar som ligger til de ulike rollene følges opp i forbindelse med den daglige driften.
5		**Kompetanse og kapasitet** Fylkeskommunen arbeider ikke systematisk med opplæring innenfor personvern og informasjonssikkerhet. Det mangler kartlegginger av kompetansebehov på ulike nivå i organisasjonen, og det ressurser med sentrale roller i arbeidet med informasjonssikkerhet og personvern mangler tilstrekkelig opplæring og kompetanse til å kunne utføre oppgavene som ligger til rollen.	✓ Sikre at informasjonssikkerhet og personvern inkluderes i fylkeskommunens prosjekt for etablering av kompetansestyring. ✓ Gjennomføre kartlegginger av kompetansebehov på ulike nivå innenfor informasjonssikkerhet og personvern. ✓ Vurdere kompetansebehov for sikkerhetsroller, og utarbeide kompetanseplaner basert på disse vurdering av kompetansebehov. ✓ Gjennomføre obligatorisk opplæring for alle ansatte jevnlig gjennom året. Det bør sikres at det etableres mekanismer for oppfølging av ledere og ansatte når det kommer til gjennomføring av obligatorisk opplæringsopplegg.

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
			✓ Gjennomføre vurderinger av kapasitet til sentrale roller i fylkeskommunen, herunder for fagleder for informasjonssikkerhet, faggruppe for informasjonssikkerhet og personvern, og IT-seksjonen.
6		**Robusthet mot digitale trusler** Det er etablert et godt basisnivå iht. NSMs grunnprinsipper for IKT-sikkerhet. Det er enkelte tiltak fylkeskommunen bør se på som er nevnt i kapitelene ovenfor. På den tekniske siden trekkes det spesielt frem at fylkeskommunen med fordel vurdere utvalgte tiltak for å herde klient-plattformen, f.eks. hvitelisting av tillatt programvare og fjerning av ikke-essensiell programvare og funksjonalitet på standardplattformen. Det er også en rekke anbefalinger som går på manglende risikostyring og mangel av dokumentasjon som bør adresseres. Spesielt er det identifisert mangler i planverk for krise og kontinuitetsberedskap som kan ha potensielt store konsekvenser ved håndtering av en sikkerhetshendelse. I takt med at utviklingen går i retning av flere enheter og deling av data på tvers av disse, så bør fylkeskommunen se på hvordan det i fremtiden best mulig kan sikres dataflyt mellom enheter og redusere risikoen for utnyttelse av angrepsvektorer som best håndteres ved blant annet herding av endepunkter og god forvaltning av mobile enheter med tilgang til organisasjonens data.	✓ Fylkeskommunen bør gjennomføre ytterligere herding og implementere hvitelisting av programvare på klientplattformen. ✓ Planverk for krise- og kontinuitetsberedskap bør revideres og fullføres. Dette arbeidet bør ha høyeste prioritet. ✓ Eksisterende dokumentasjon bør revideres, og manglende dokumentasjon av bla. sentrale IT-prosesser bør lages.

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
		Personvern – Grunnleggende prinsipper Fylkeskommunen kan ikke dokumentere overholdelse av de grunnleggende prinsippene for behandling av personopplysninger for alle behandlingsaktiviteter. Dette kan utgjøre et brudd på ansvarlighets-prinsippet etter art. 5 nr. 2. Det er ikke gjennomført kontroller av at samtykker er gyldig innhentet og KPMG har funnet tilfeller der det samtykket ikke vil være gyldig. I tillegg mangler det i flere tilfeller sletterutiner, og formålsangivelse er ikke tilstrekkelig spesifikk.	✓ Fylkeskommunen bør gjennomgå og kvalitetssikre at det gis informasjon til de registrerte i de tilfeller hvor behandling er basert på den registrertes samtykke. Det bør kvalitets-sikres at informasjonen som gis er i tråd med personvernforordningens krav, og at det er etablert mekanismer som sikrer at registrerte kan trekke tilbake sitt samtykke like enkelt som det ble gitt. ✓ Fylkeskommunen bør gjennomgå og revidere protokollen over behandlingsaktiviteter for å sikre at formål ved behandling av person-opplysninger er tilstrekkelig spesifikt og uttrykkelig angitt. ✓ Fylkeskommunen bør etablere sletterutiner i tilfeller hvor dette mangler.
		Personvern – Informasjon til de registrerte Fylkeskommunen gir ikke tilstrekkelig informasjon ved innsamling av personopplysninger. Det gjelder i de fleste tilfeller fylkeskommunen samler inn personopplysninger, og er tidligere påpekt av personvernombud.	✓ Fylkeskommunen bør revidere sin personvern-erklæringen på nettsidene sine. ✓ Det bør etableres en personvernerklæring for ansatte som sikrer at også denne kategorien registrerte får informasjon om behandling. ✓ Fylkeskommunen bør inkludere informasjon om behandling av personopplysninger i skjema på sine nettsider, eller informasjon om hvor de registrerte kan finne mer opplysninger.

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
	🟡	**Personvern – Ansvar og sikkerhet** Fylkeskommunen har ikke gjennomført risikovurderinger tilknyttet alle sine behandlinger av personopplysninger. Det er heller ikke gjennomført vurdering av personvernkonsekvenser, selv i tilfeller hvor det er identifisert at det sannsynligvis foreligger høy risiko for personvernet.	✓ Fylkeskommunen bør gjennomføre risiko-vurderinger for sine behandlinger av person-opplysninger, og sikre at slike vurderinger gjennomføres for nye behandlinger, herunder slik som anskaffelse av nytt sak- og arkivsystem. ✓ Fylkeskommunen bør gjennomføre vurderinger av personvernkonsekvenser i de tilfeller der det er identifisert at behandling kan innebære høy risiko for personvernet.
	🟢	**Personvern – Innebygd personvern og personvern som standardinnstilling** Det finnes ikke rutiner som er ment å sikre prinsippene ved utvikling av IT-systemer. Innebygd personvern og personvern som standardinnstilling er ikke nevnt i styringssystemet, eller i rutiner som gjelder for anskaffelser av nye IT-systemer.	✓ Fylkeskommunen bør etablere inkludere prinsipper om innebygd personvern og personvern som standardinnstilling i rutinene i styringssystemet sitt. ✓ Fylkeskommunen bør inkludere krav til innebygd personvern og personvern som standard-innstilling ved innkjøp av IT-systemer hvor det skal behandles personopplysninger.
	🟡	**Personvern – Databehandlere** Fylkeskommunen baserer i liten grad krav til sine databehandlere på vurderinger av risiko knyttet til behandlingen. Kravene som stilles i konkurranser er standardkrav som i liten grad tilpasses avhengig av risiko. Fylkeskommunen gjennomfører i liten grad kontroll av databehandlerne som benyttes. Kontroller fremstår tilfeldig, og er ikke risikobasert.	✓ Fylkeskommunen bør tilpasse krav som stilles til sine databehandlere basert på risikovurderinger. Standardkrav kan fungere som et godt utgangs-punkt, men bør tilpasses. Slik tilpasning av standardkrav krav ses i sammenheng med fylkeskommunens arbeid med informasjons-klassifisering, slik at klassifisering avgjør hvilket sett med standardkrav som fungerer som et utgangspunkt.

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
			✓ Fylkeskommunen bør systematisere sitt arbeid med oppfølging av databehandlere. Det danske datatilsynet har laget en veileder som kan benyttes som utgangspunkt i forbindelse med vurdering av kontrollers hyppighet og intensitet.
		Personvern – Protokoll over behandlingsaktiviteter Fylkeskommunens protokoll over behandlingsaktiviteter er ikke i tilstrekkelig grad utfylt, og lider av enkelte mangler. Det fremstår ikke som om protokollen er tilstrekkelig kjent i organisasjonen, i likhet med ansvaret for utfylling og oppdatering av den.	✓ Fylkeskommunen bør revidere protokoll over behandlingsaktiviteter for å sikre at den er dekkende med hensyn til fylkeskommunens behandling av personopplysninger. ✓ Fylkeskommunen bør sikre at protokollen holdes oppdatert, blant annet ved å etablere faste rapporterings/kontrollpunkter gjennom året, sørge for at faggruppen har tilstrekkelig innsikt i protokollen, og ved å inkludere oppdatering av protokoll i sjekklister eller tilsvarende i linjen.
		Personvern – personvernombud Ut fra dokumentasjon og informasjon fra intervju, utføres ikke alle oppgaver som ombudet skal utføre i tråd med bestemmelsene i personvern-forordningen eller i styringssystemet. Personombudets kontroll av etterlevelse har vært begrenset. En del av oppgavene er det ut fra dagens organisering også vanskelig å se at ombudet kan utføre på en effektiv måte som følge av manglende tilgang på informasjon. Med utgangspunkt i gjennomførte intervju, fremstår det også tilfeldig om og eventuelt når personvernombudet involveres i prosesser av betydning for personvernet i fylkeskommunen.	✓ Fylkeskommunen bør etablere faste og hyppige møtepunkter mellom fylkeskommunen og personvernombud, og gi tilgang til relevante informasjonssystemer slik som intranett og risk manager, for å sikre at personvernombudet har tilstrekkelig tilgang til informasjon. ✓ Personvernombudet bør jevnlig, og minst årlig rapportere til ledelsen på ombudets vurdering av personvernrisiko i fylkeskommunen.

Hovedanbefalinger fra gjennomgangen			
ID	Prioritet	Avvik	Anbefaling
			✓ Fylkeskommunen bør jevnlig informere alle ansatte om personvernombudet og dets oppgaver, for å sikre at ombudet er tilstrekkelig kjent i organisasjonen. ✓ Fylkeskommunen bør tydeliggjøre sine retningslinjer med tanke på når personvern-ombudet skal involveres. ✓ Fylkeskommunen bør sikre at personvern-ombudet har mulighet til å gjennomføre sine kontrollaktiviteter. Personvernombudets kontroller bør baseres på vurderinger av personvernrisiko i fylkeskommunen.
	●	**Personvern – overføring av personopplysninger til tredjeland** I fylkeskommunens protokoll over behandlingsaktiviteter er det ikke angitt at det skjer overføringer til tredjeland. Tilsvarende er beskrevet i fylkes-kommunens personvernerklæring. Fylkeskommunen benytter imidlertid tjenester som kan innebære slik overføring, herunder eksempelvis tjenester fra store skyleverandører som Google og Microsoft. I intervju er det oppgitt at det ikke er gjennomført vurderinger av fylkeskommunens eventuelle overføringer til tredjeland.	✓ Fylkeskommunen bør gjennomføre kartlegging rettet mot sine databehandlere for å identifisere eventuelle overføringer av personopplysninger til tredjeland. I den grad slike overføringer identifiseres, bør fylkeskommunen identifisere hvilket overføringsgrunnlag overføringen baserer seg på, og om det er behov for å implementere ytterligere tekniske eller organisatoriske tiltak for å sikre at de overførte opplysningene oppnår et tilsvarende beskyttelsesnivå som innenfor EU/EØS.

5 Uttalelse fra fylkeskommunedirektør

Fylkeskommunedirektøren har gitt følgende uttalelse til rapporten:

«Fylkeskommunedirektøren sin samlede vurdering er at rapporten gir et riktig bilde av situasjonen. Rapportens anbefalinger gir også et godt grunnlag for å følge opp de ulike forbedringspunktene innenfor disse områdene. Fylkeskommunedirektøren har satt i gang arbeidet med oppfølging og det vil blant annet bli laget en plan for oppfølging så raskt som mulig.

Vi vil likevel knytte noen kommentarer til enkelte deler av rapporten. Den første er knyttet til kapittel 3.4.3 om gjennomføring av phishingangrepet. Som det fremgår av beskrivelsen i rapporten var det ikke en optimal gjennomføring. Vi vil understreke at testen ble planlagt sammen med teamet fra KPMG, og det var ikke slik at alle på it-seksjonen var informert om alle detaljene rundt dette. Dette er blant annet med å forklare bakgrunnen for at tiltak ble satt i verk tidligere enn planlagt. Måten IT-seksjonen reagerte på kan også ses på som et uttrykk for at interne rutiner fungerer og at det reageres raskt når potensielt angrep blir avdekket.

Videre vil vi kommentere forholdet knyttet til overføring av personopplysninger til tredjeland i kapittel 3.5.10. Det er riktig at det ikke er gjennomført en selvstendig kartlegging av alle overføringer. Det er likevel slik at vi i avtalene med leverandører der de store skyleverandørene er en part, presiserer at behandling av personopplysninger skal skje i Europa (EU/EØS), selv om dette i seg selv ikke er en tilstrekkelig garanti mot overføring til tredjeland. Når vi skal inngå nye avtaler med databehandlere er det rutine at lokasjon for behandling av personopplysninger blir vurdert, også for underleverandører.

I det videre arbeidet med oppfølging av forbedringspunktene vil Fylkeskommunedirektøren samtidig vise til oppfølgingen som skjer i forbindelse med fylkestingets sak T-67/21 om kontrollutvalgets undersøkelse av helhetlig virksomhetsstyring og internkontroll, samt program for nye digitale arbeidsformer. Det pågår her allerede arbeid og prosesser som har en direkte påvirkning for flere av forbedringspunktene det blir vist til i denne undersøkelsen. Flere av tiltakene som anbefales vil innebære en utfordring for organisasjonen på kapasitet og kompetanse, i tillegg til at det vil være direkte økonomiske kostnader knyttet til enkelte av tiltakene. Fylkeskommunedirektøren vil så langt som mulig løse det innenfor dagens rammer, men vil komme nærmere inn på behov i den årlige strategi- og rammesaken og i det etterfølgende arbeidet med økonomiplan og årsbudsjett. Behovet for å styrke kapasiteten innenfor virksomhetsstyring og internkontroll, herunder også informasjonssikkerhet og personvern, er allerede adressert til politisk nivå i forbindelse med økonomiplanseminar for fylkestinget den 9. mai. Her ble det også vist til de to omtalte undersøkelsene».

6 Oversikt sentrale dokumenter

Dokumentbestillinger

- ✓ Dokumentbestilling 27.10.2021

Styrende dokumentasjon

- ✓ Handbok for personvern og informasjonstryggleik i Møre og Romsdal fylkeskommune
- ✓ IT-sikkerhetsplan for MRFK oppdatert oktober 2021
- ✓ Økonomiplan med handlingsprogram 2021-2024 – Sak T-95/20
- ✓ Passordpolicy MRFK
- ✓ Policy for sikkerhetskopiering av IT-systemer i Møre og Romsdal fylkeskommune
- ✓ Forvaltning av Microsoft 365 i Møre og Romsdal fylkeskommune
- ✓ Klassifisering av data i Microsoft 365 versjon 1.2 17.07.2020
- ✓ Rettighetsstruktur tannhelsesystemer
- ✓ Prosessbeskrivelse og rutiner for bestillingsskjema for skole og sentraladministrasjonen
- ✓ Retningslinjer skytenester
- ✓ Retningslinjer for bruk av epost i Møre og Romsdal fylkeskommune versjon 1.0 25.01.2016
- ✓ Retningslinjer for datalagring i Møre og Romsdal fylkeskommune versjon 1.0 25.01.2016
- ✓ Retningslinjer for fjernarbeid i Møre og Romsdal fylkeskommune
- ✓ Fjernarbeidsløsning med 2-faktor
- ✓ Retningslinjer for utlevering av elektronisk utstyr til tilsette i Møre og Romsdal fylkeskommune
- ✓ IKT-reglement for dei vidaregåande skolane 1.8.2021
- ✓ Reglar for IKT-bruk i Møre og Romsdal fylekskommune gyldig frå 01.05.2012
- ✓ Reglement for mobil tenestetelefon for tilsette i Møre og Romsdal fylkeskommune
- ✓ Avtale om mobil tenestetelefon
- ✓ Avtale om regelmessig fjernarbeid
- ✓ Bruksavtale for utvida tilgang til fylkesnettet

Applikasjonsforvaltning

- ✓ Applikasjonsforvaltning i MRFK oppdatert 15.06.2021
- ✓ Applikasjonsforvaltning – implementering av applikasjonsforvaltning i MRFK
- ✓ Applikasjoner og roller i applikasjonsforvaltning
- ✓ Vurderinger av nye applikasjoner i Microsoft 365
- ✓ Fagsystemer Møre og Romsdal fylkeskommune
- ✓ Forenklet nettverkskart
- ✓ Wiki Nettverk

Tilgangsstyring

- ✓ Tilgangskontroll Active Directory on-prem MRFK
- ✓ Bestilling av tilganger i Visma Økonomi
- ✓ Endringshåndtering IT-miljø – Møre og Romsdal fylkeskommune
- ✓ Rutiner for tilgangskoder til Ephortebrukere
- ✓ Tilgangskontroll i Microsoft 265 og Azure
- ✓ Tilgangsstyring i Visma Enterprise oppdatert 21.01.2021

Risikovurderinger og avvik

- ✓ Avviksoversikt september 2019 – november 2021
- ✓ Oversikt risikovurderinger september 2019 – november 2021
- ✓ Risikovurdering Office 365
- ✓ Risikovurdering psykologjournal
- ✓ Risikovurdering handtering av konfidensiell informasjon
- ✓ Risikovurdering klassetrivsel
- ✓ Risikovurdering Vigo Opplæring 2018
- ✓ Risikovurdering Vigo Opplæring 2020
- ✓ Risikovurdering av uønska hendingar

Informasjonssikkerhet

- ✓ Foranalyse trinn 1 – identifiser oppgaver og informasjonstyper
- ✓ Sjekkliste for eksterne IKT-tjenester/skytjenester

Innkjøp og anskaffelser

- ✓ Anskaffelsesstrategi for Møre og Romsdal fylkeskommune 17.12.2018
- ✓ Anskaffelsesprosedyre for Møre og Romsdal fylkeskommune mai 2021
- ✓ Rutine kjøp over kroner 100 000
- ✓ Rutine kjøp under kroner 100 000
- ✓ Prosedyre avtaleoppfølging
- ✓ Avtaleoppfølging i fylkeskommunen
- ✓ Mal kontraktsevaluering ved prolongering / avtaleslutt
- ✓ Mal referat oppfølgingsmøte
- ✓ Opprettelse av behovsmelding i Mercell – revidert juli 2021
- ✓ Maler konkurransegrunnlag
- ✓ Mal avtale om varekjøp
- ✓ Mal rammeavtale varekjøp
- ✓ Mal databehandleravtale
- ✓ Mal bilag til databehandleravtalen
- ✓ Eksempler kravspesifikasjoner IT-systemer
- ✓ Interne rutiner / prosedyrer for anskaffelser / innkjøp ved de videregående skolene
- ✓ Anskaffingsansvar – roller, ansvar og fullmakter
- ✓ Anskaffingsansvar
- ✓ Sikkerhetskrav ved anskaffelser

Kontinuitetsplan

- ✓ Enkel konsekvens analyse for 14 systemer og applikasjoner
- ✓ Risiko- og sårbarhetsanalyse for Møre og Romsdal fylkeskommune 30.03.2012
- ✓ MRFK kontinuitetsplan versjon 1.2

Samferdsel

- ✓ Risikomatrise 2021/2022
- ✓ Styrings- og oppdragsnotat for 2022 sektor

Tannhelse

- ✓ Mailkorrespondanse med tannhelse
- ✓ Powerpointpresentasjon om tannhelsetjenesten
- ✓ Klinikkleiarfunksjonen ansvar og oppgaver
- ✓ Introduksjonsprogram for tannhelsetenesta
- ✓ Skjermbilder intranett
- ✓ Veiledning og instruksjoner i bruk av Opus versjon 2.0 05.10.2017
- ✓ Vilkår for medlemskap i Helsenettet
- ✓ Møre og Romsdal Revisjon IKS – uavhengig attestasjonsoppdrag for Møre og Romsdal fylkeskommune om internkontroll innenfor tannhelsetjenester i fylkeskommunen

Opplæring

- ✓ Mailkorrespondanse med HR
- ✓ Skjermbilder intranett
- ✓ Mal med sjekkliste for introduksjonsprogram nytilsette med prøvetid
- ✓ Mal arbeidsavtale
- ✓ Rapporter program «nye digitale arbeidsformer»
- ✓ Program nye digitale arbeidsformer rapport fase 1 desember 2021
- ✓ Prosjektgjennomføringsdokument prosjekt retningslinjer for informasjonsforvaltning og lagring
- ✓ Retningslinjer for informasjonsforvaltning og lagring
- ✓ Prosjektgjennomføringsdokument prosjekt revisjon kommunikasjons- og kanalstrategi
- ✓ Prosjektgjennomføringsdokument prosjekt nytt intranett og nettsideutvikling
- ✓ Prosjektgjennomføringsdokument prosjekt sak- og arkivsystem
- ✓ Styringsdokument prosjekt verksemdstyringsverktøy i Møre og Romsdal fylkeskommune
- ✓ Prosjektgjennomføringsdokument prosjekt kvalitetssystem
- ✓ Prosjektgjennomføringsdokument prosjekt kompetansestyring
- ✓ Kommunikasjonsstrategi per 01.12.2021

Personvern

- ✓ Rutine for innsyn i personopplysninger
- ✓ Revisjonsrapport Møre og Romsdal fylkeskommune 2020 – Interkommunalt arkiv for Møre og Romsdal
- ✓ Evaluering av prosjektet personvernombud Interkommunalt arkiv for Møre og Romsdal
- ✓ Årsrapport personvernombudet 2020
- ✓ Protokoll art 30 GDPR med menyer
- ✓ Protokoll art 30 GDPR Utdanning
- ✓ Avvik Datatilsynet 1
- ✓ Avvik Datatilsynet 2
- ✓ Avvik Datatilsynet 3