Vestfold og Telemark revisjon

Informasjonssikkerhet og personvern

Forvaltningsrevisjon | Nome kommune

22: 3816 402

Innhold

Sammendrag

I denne forvaltningsrevisjonen har vi sett på hvordan Nome kommune arbeider for å ivareta informasjonssikkerheten i kommunen og innbyggernes personvern. Rapporten omtaler ulike tiltak og rutiner på informasjonssikkerhetsområdet, både organisatoriske og tekniske, men er først og fremst konsentrert rundt kommunens tiltak for å ivareta kravene som stilles i personopplysningsloven. Det er utarbeidet flere revisjonskriterier som vil bli redegjort for og gjennomgått i rapportens kapitler. Overordnet sett har vi operert med to problemstillinger, hvor den ene er på et generelt nivå og handler om kommunens tiltak med tanke på personopplysningsloven, mens den andre problemstillingen handler om den praktiske oppfølgingen på dette området i kommunens enheter.

I dette sammendraget presenteres de sentrale funnene og vurderingene i rapporten, sortert under de to problemstillingene.

Har Nome kommune etablert tiltak for å ivareta kravene i personopplysningsloven?
Vi finner at kommunen i stor grad har etablert gode tiltak for å ivareta kravene i personopplysningsloven, slik dette er beskrevet i styrende dokumenter på området og andre rutinebeskrivelser.

Samtidig mener vi at kommunen samlet sett har potensiale for forbedring. Noen rutiner som beskrives i styrende dokumenter på området følges ikke opp på alle punkter. For eksempel har det ikke vært gjennomført en årlig «ledelsens gjennomgang» med rapportering på informasjonssikkerhet og personvern, inkludert avvik, til kommunedirektøren. Det er likevel slik at informasjonssikkerhet, personvern og avvik har vært oppe som tema på møter i kommunens ledergruppe.

Kommunen har ikke gjennomført risikovurderinger for alle sine systemer som behandler personopplysninger.

Styrende dokumenter på området informasjonssikkerhet inneholder noen punkter som fremstår som uavklarte, eller under arbeid. Det er behov for å oppdatere de styrende dokumentene.

Det er noen svakheter i kommunens oversikt over systemer og tilhørende dokumenter. Databehandleravtaler er ikke lenket til systemet i Digiorden, noe som gjør personvernombudets kontrollfunksjon mer utfordrende. For flere systemer i behandlingsprotokollen i Digiorden er det uklart hvilket behandlingsgrunnlag som ligger til grunn for kommunens behandling av personopplysninger, da flere behandlingsgrunnlag er registrert samtidig. Det er en særlig utfordring at samtykke registreres som behandlingsgrunnlag sammen med en rettslig forpliktelse eller andre behandlingsgrunnlag som ikke krever samtykke.

Hvordan blir personopplysningsloven og kommunens egne tiltak fulgt opp i praksis i kommunens enheter?

For å svare på denne problemstillingen har vi undersøkt to utvalgte enheter i kommunen, en skole og hjemmetjenesten, gjennom intervjuer med ledelsen ved enhetene.

På et overordnet nivå fikk vi et godt inntrykk av hvordan det tenkes rundt, og jobbes med, informasjonssikkerhet og personvern i disse enhetene. I denne oppsummeringen vil vi ta utgangspunkt i prinsippene om fortrolighet og tilgjengelighet, som er to viktige prinsipper innenfor området informasjonssikkerhet.

Når det gjelder fortrolighet, er vårt inntrykk at begge enhetene er bevisste på å behandle personopplysninger om elever og pasienter/brukere i godkjente fagsystemer så langt det lar seg gjøre, og de er bevisste på å bruke andre sikre kanaler når det er behov for å utveksle personopplysninger utenom fagsystemene. Det er rutiner for kontroll av fullmakt ved innsynsforespørsler, og gode rutiner for utsendelse av personopplysninger til rett mottaker.

Tilgjengeligheten på personopplysninger er godt ivaretatt i enhetene. Begge enhetene har gode systemer og gode rutiner som sørger for at ansatte har tilgang til de opplysningene som er nødvendige ut fra deres rolle og ansvarsområde. Enhetene har, i samarbeid med kommunen og IKT-drift, gode rutiner for tilgangsstyring. Hjemmetjenesten har en papirbasert sikkerhetskopi av viktige opplysninger for beredskapssituasjoner, slik at nødvendig hjelp kan ytes til brukerne ved en hendelse som gjør det digitale systemet utilgjengelig. Medisinlister behandles på papir i den vanlige driften, men det er gode rutiner for sikkerhet/tilgang på disse dokumentene. Når det gjelder skolen er bruken av papirkopier noe mer omfattende, ved at elevmappene kopieres til et papirarkiv i tillegg til det digitale arkivet. Vår vurdering er at man kunne redusert risikoen for at personopplysninger kommer på avveie dersom lærerne fikk tilgang til det digitale arkivet. Skolen har imidlertid gode rutiner for tilgang til, og bruk av, opplysningene i papirarkivet. Disse rutinene bidrar til å redusere risikoen som et papirarkiv innebærer.

Anbefalinger

Vi anbefaler at Nome kommune:

- oppdaterer informasjonssikkerhetshåndboken og andre styrende dokumenter på området informasjonssikkerhet og personvern, eventuelt utarbeider nye overordnede styringsdokumenter på området
- sikrer en formalisering av rapporteringen på området og sørger for at praksis samsvarer med rutiner som beskrives i styrende dokumenter,
- gjennomgår rutinene for registreringer i behandlingsprotokollen, og sørger for at behandlingsgrunnlaget for de ulike formålene blir presist angitt

- gjennomfører risikovurderinger og DPIA i samsvar med lovkravene og egne rutiner
- vurderer om rutiner og saksbehandling knyttet til krav om innsyn i personopplysninger ivaretar de registrertes rettigheter
- vurderer om bruken av papirbaserte systemer helt eller delvis kan erstattes med digitale løsninger når kommunens enheter behandler personopplysninger

1. Innledning

1.1. Kontrollutvalgets bestilling

Forvaltningsrevisjonen er bestilt av kontrollutvalget i Nome kommune i sak 28/21. Informasjonssikkerhet er en del av kommunens vedtatte plan for forvaltningsrevisjon i perioden.

Reglene om forvaltningsrevisjon står i kommuneloven § 23-2 første ledd bokstav c, jf. § 23-3 og § 24-2 og i forskrift om kontrollutvalg og revisjon.

1.2. Problemstilling og revisjonskriterier

Rapporten handler om følgende problemstillinger:

1. Har Nome kommune etablert tiltak for å ivareta kravene i personopplysningsloven?
2. Hvordan blir personopplysningsloven og kommunens egne tiltak fulgt opp i praksis i kommunens enheter?

Revisjonskriteriene[1] i denne forvaltningsrevisjonen er hentet fra personopplysningsloven og relevante veiledere fra Datatilsynet. Kriteriene framgår under hver problemstilling nedenfor, og er nærmere omtalt i vedlegg 2 til rapporten.

1.3. Avgrensning

Rapporten omfatter ikke behandling av personopplysninger knyttet til folkevalgte og kommunens egne arbeidstakere.

1.4. Metode og kvalitetssikring

Denne forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Lars Pedersen, med Kirsti Torbjørnson som oppdragsansvarlig.

Rapporten bygger på informasjon fra kommunens relevante dokumenter på området, samt informasjon hentet direkte fra systemet Digiorden (behandlingsprotokoll). Vi har også gjennomført intervjuer med to utvalgte enheter i kommunen. De utvalgte enhetene var en grunnskole og kommunens hjemmetjeneste. Vi har gjennomført en stikkprøvekontroll av opplysninger om utvalgte systemer i kommunens behandlingsprotokoll (Digiorden).

Det står mer om metode og tiltak for kvalitetssikring i vedlegg 3 til rapporten.

[1] Det skal alltid etableres revisjonskriterier i forvaltningsrevisjon, jf. forskrift om kontrollutvalg og revisjon § 15. Revisjonskriterier er de regler og normer som gjelder innenfor det området vi skal undersøke. Revisjonskriteriene er grunnlaget for revisors analyser, vurderinger og konklusjoner.

1.5. Om personopplysningsloven og sentrale begreper på området

Gjeldende personopplysningslov trådte i kraft juli 2018. Loven gjennomfører EUs personvernforordning (ofte kjent som GDPR) i norsk lov. Forordningsteksten er tatt inn som vedlegg til loven, og har inndeling i artikler, mens loven ellers er inndelt i paragrafer.

Personopplysningsloven bruker noen begreper som det er relevant å ha kjennskap til:

- Behandling – dette er enhver operasjon som gjøres med personopplysninger.
- Behandlingsansvarlig – er den som beslutter at personopplysninger skal samles og hvordan dette skal gjøres. I de fleste tilfeller er kommunen behandlingsansvarlig.
- Behandlingsgrunnlag – hjemmel som er nødvendig for å kunne behandle personopplysninger, hjemlene står i artikkel 6 nr. 1.
- Databehandler – er den som på oppdrag av en behandlingsansvarlig behandler data. Dette er gjerne IKT-leverandører som enten behandler personopplysninger direkte eller får tilgang til disse eks. ved vedlikehold og support av kommunens systemer. Databehandlere har ofte underleverandører og disse omtales som underdatabehandler.
- Databehandleravtale – lovpålagt avtale mellom behandlingsansvarlig og databehandler som regulerer behandlingen av personopplysninger som databehandler skal gjøre på vegne av behandlingsansvarlig og skal sikre at databehandler har egnede tekniske og organisatoriske tiltak for å oppfylle personopplysningslovens krav. Databehandleravtaler er regulert i artikkel 28 nr. 3.
- Personopplysning – definert i personvernforordningen artikkel 4 nr. 1 som: «enhver opplysning om en identifisert eller identifiserbar fysisk person».
- Den registrerte – en fysisk person som kommunen behandler personopplysninger om.
- Særlige kategorier av personopplysninger (sensitive personopplysninger) – er definert i personvernforordningen artikkel 9 nr. 1. Det er ikke tillatt å behandle disse opplysningene med mindre man har hjemmel i artikkel 9 nr. 2.

1.6. Kommunedirektørens uttalelse

Rapporten ble sendt til uttalelse 12.05.22, jf. forskrift om kontrollutvalg og revisjon § 14. Kommunedirektørens uttalelse ligger i vedlegg 1.

2. Informasjonssikkerhet og personvern

Problemstilling 1:
Har Nome kommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Problemstilling 2:
Hvordan blir personopplysningsloven og kommunens egne tiltak fulgt opp i praksis i kommunens enheter?

Til disse problemstillingene har vi utledet følgende revisjonskriterier:

Nome kommune skal ha

- **en organisasjon med klar plassering av ansvar og myndighet, samt rutiner for rapportering**
- **personvernombud, organisert i samsvar med personopplysningsloven**
- **protokoll over hvilke personopplysninger kommunen behandler**
- **risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA)**
- **tekniske og organisatoriske tiltak for å sikre personopplysningene**
- **rutiner for å håndtere brudd på personopplysningssikkerheten**
- **tiltak for å ivareta innsynsretten til de registrerte**
- **system for å sikre at kommunen har databehandleravtale med alle databehandlere**
- **system for å sikre at databehandleravtalene ivaretar kommunens behov**

Se vedlegg 2 for en nærmere redegjørelse av bakgrunnen for revisjonskriteriene.

2.1. Organisering, ansvar og rapportering

Nome kommune skal ha en organisasjon med klar plassering av ansvar og myndighet, samt rutiner for rapportering.

2.1.1. Fakta om organisering, ansvar og rapportering

Organisering og ansvar
Nome kommune har en informasjonssikkerhetshåndbok som beskriver regler, retningslinjer og rutiner på informasjonssikkerhetsfeltet i kommunen. Formålet med håndboken er å beskytte informasjon og informasjonssystemer, sike at behandlingen av informasjon fyller lovpålagte krav og andre forpliktelser, samt at slik behandling dekker behovet for personvern og etisk ansvar. Sammen med andre styrende, gjennomførende og kontrollerende dokumenter utgjør informasjonssikkerhetshåndboken kommunens plan for informasjonssikkerhet.

Informasjonssikkerhetshåndboken beskriver regler og retningslinjer for behandling av informasjon. Det står at alle som benytter kommunens systemer er forpliktet til å kjenne til og følge håndboken. Ansvaret følger linjeledelsen i kommunen.

Ledere er tillagt et særskilt ansvar på flere områder. Særlig legger håndboken vekt på lederes ansvar for å gi ansatte tilstrekkelig opplæring innenfor aktiviteter som handler om informasjonssikkerhet, behandling av informasjon, personvern og avvikshåndtering. Videre står det at ledere har ansvaret for at formålet med behandlingen av informasjon (behandlingsprotokollen) skal registreres i Digiorden[2] og arkiveres i WebSak (kommunens arkivsystem). Ledere har også ansvar for at IT-utstyret som brukes, anskaffes i henhold til kommunens standarder og innkjøpsrutiner.

Håndboken inneholder rollebeskrivelser for personvernombudet ledere, informasjonssikkerhetsansvarlig, behandlingsansvarlig, it-drift, systemeier og systemansvarlig.

Den enkelte virksomhetsleder er systemeier for de systemene som naturlig hører inn under området man er virksomhetsleder for. Systemeieren har ansvaret for å ivareta informasjonssikkerheten i disse systemene. Systemeieren delegerer den daglige oppfølgingen av dette til en systemansvarlig. Den systemansvarlige har da det operative ansvaret for systemet, hvilket også inkluderer opplæring av ansatte, samt utarbeidelse av risikoanalyser. IT-drift er tillagt det tekniske ansvaret for at systemene er tilgjengelige for kommunens ansatte.

Selv om plassering av ansvar og myndighet på dette området i all vesentlighet er beskrevet i kommunens styrende dokument på området er det flere punkter som ikke er formelt avklart i dokumentet. Dette gjelder blant annet fagansvarlig for informasjonssikkerhet, samt faste fora med roller i internkontroll- og sikkerhetsarbeidet.

Rapportering

Rådmannens ledergruppe skal minst årlig avholde et møte (ledelsens gjennomgang) om internkontrollen på informasjonssikkerhet i kommunen. Det framgår av håndboken at det er kommunedirektøren som skal initiere denne gjennomgangen. I dette møtet skal ledelsen avdekke om sikkerheten ivaretas mht. mål, strategier og prosedyrer, og det skal besluttes tiltak for det videre sikkerhetsarbeidet. Håndboken nevner flere konkrete punkter som skal dekkes, blant annet rapportering på avvik, endringer i trusselbildet på området, endringer i personopplysninger som kommunen behandler og organisatoriske endringer.

[2] Digiorden er et styringsverktøy. Digiorden er utviklet av kommunene i Kongsbergregionen og Telemark. Løsningen skal gi oversikt over kommunenes systemer og datasettene i systemene. Digiorden gir også støtte for GDPR-protokoll og noe styringsdata for kommunens ledelse. Løsningen ble overført til KS i 2021, for å bli en nasjonal løsning for alle kommuner.

Vi har fått opplyst fra kommunen at ledelsens gjennomgang ikke er gjennomført årlig slik det er beskrevet i kommunens egne dokumenter på området. Kommunedirektøren opplyser at ledergruppen følger opp relevant tema innenfor informasjonssikkerhet og personvern i sine møter, og at det har vært avholdt et møte i utvidet ledergruppe med deltakelse fra personvernombudet.

Personvernombudet opplyser at hun samarbeidet godt med ledelsen i kommunen. Personvernombudet opplyser samtidig at hun deltar sporadisk på ledermøter. Hun opplyser også at det ikke har vært noen rutiner for rapportering på avvik til kommunedirektøren. Personvernombudet opplyser at kommunen har jobbet med en ny informasjonssikkerhetsplan hvor samarbeid og rapportering mellom personvernombudet og ledelsen vil få en mer formalisert form, noe personvernombudet anser som positivt. Arbeidet med ny informasjonssikkerhetsplan er også bekreftet av kommunedirektøren.

2.1.2. Revisors vurdering av organisering og ansvar

Nome kommune har dokumentasjon som beskriver en organisasjon med klar plassering av ansvar og myndighet knyttet til ivaretakelse av informasjonssikkerhet og personvern. Som en hovedregel er ansvaret på dette området organisert etter kommunens ordinære linjeledelse og det er beskrevet hvordan ansvaret er delegert på de ulike ledelsesnivåene.

Både informasjonssikkerhetshåndboken og dokumentet «roller og ansvar i internkontroll- og sikkerhetsarbeidet» er sentrale, styrende dokumenter på området informasjonssikkerhet og personvern. Vi anbefaler at kommunen tar en gjennomgang av både disse og andre styrende dokumenter på området informasjonssikkerhet og personvern. Målet med en slik gjennomgang bør være at relevante dokumenter er oppdatert i tråd med gjeldende rutiner i kommunen, enten det gjelder roller og ansvar, myndighet og delegering, rapportering, fora og møtepunkter, eller annet. En slik gjennomgang kan også benyttes til å endre eller oppdatere rutiner ved behov. Vi har fått opplyst at kommunen har kommet langt i arbeidet med en ny plan for informasjonssikkerhet, hvor flere rutiner, roller og funksjoner får oppdaterte beskrivelser. Her vil også ulike rapporteringsrutiner og fora bli mer formalisert. Her bør særlig rapportering til kommunedirektør og ledermøter hvor informasjonssikkerhet er tema formaliseres slik at det er samsvar mellom kommunens styrende dokumenter og praksis på området.

2.2. Personvernombud

Nome kommune skal ha personvernombud, organisert i samsvar med personopplysningsloven.

Datatilsynet har utarbeidet en veileder hvor det er beskrevet hvilke oppgaver personvernombudet har. Her fremgår det at personvernombudet skal informere om forpliktelsene som kommunen har

etter personopplysningsloven, både til behandlingsansvarlig og andre ansatte. Videre skal personvernombudet:

- kontrollere kommunens overholdelse av personvernregelverket og interne rutiner og regler,
- på forespørsel gi råd om vurdering av personvernkonsekvenser (DPIA),
- samarbeide og være kontaktpunkt for Datatilsynet og samarbeide med dem.

Videre skriver Datatilsynet at personvernombudet skal fokusere sin innsats på de områdene hvor risikoen er høyest. Datatilsynet skriver også at personvernombudet kan få andre oppgaver så lenge det ikke oppstår en interessekonflikt.

Det fremgår av personvernforordningen art. 38 nr. 3 at personvernombudet skal være uavhengig, det vil si at man ikke kan instrueres i utførelsen av oppgavene og heller ikke kan avsettes eller straffes for utførelsen av oppgavene. Videre fremgår det av personvernforordningen art. 37nr. 5 at personvernombudet skal være faglig kvalifisert og ha kunnskap på området som er tilstrekkelig for å kunne utføre arbeidet.

2.2.1. Fakta om personvernombudet

Nome kommune har personvernombud sammen med Midt-Telemark kommune. Personvernombudet er ansatt i Midt-Telemark kommune som juridisk rådgiver, og dette utgjør 60 prosent av stillingen. De resterende 40 prosentene er satt av til rollen som personvernombud for de to kommunene. Personvernombudet har hatt stillingen siden 2018. Hun er jurist, og har arbeidserfaring som skatteoppkrever og fra NAV. Hun har holdt seg oppdatert om personvernregelverk gjennom informasjon og kurs, særlig fra Datatilsynet.

Personvernombudets rolle og ansvar er beskrevet i informasjonssikkerhetshåndboken. Ifølge denne skal kommunens personvernombud bistå ved spørsmål om personvern, gi råd ved utredninger, og kontrollere kommunens overholdelse av regelverket. Videre slås det fast at personvernombudet rapporterer til kommunedirektørens ledergruppe, og at personvernombudet ikke skal motta instruksjoner i forbindelse med utførelsen av sine oppgaver. I intervjuet bekreftet personvernombudet disse oppgavene, og opplyste at det går mest tid til rådgivning, og mindre tid til kontroll. Hun opplyser at hun bidrar til DPIA, og bruker mye tid på databehandleravtaler, både oppfølging og resignering av eksisterende avtaler, og utarbeidelse av kommunens egen avtale. Mange ledere tar kontakt og rådfører seg angående databehandleravtaler.

Personvernombudets rolle og ansvar er også beskrevet i håndbokens del om rutiner for behandling av avviksmeldinger, samt i dokumentet «rutine for sikkerhetsbrudd på personvern», som mer utfyllende beskriver kommunens rutiner rundt behandling av sikkerhetsbrudd og avvik. Gjennom intervjuet opplyste personvernombudet å ha vært involvert i en sak i Nome kommune som omhandlet avvik med påfølgende varsling til Datatilsynet. Kommunedirektøren var også involvert i håndteringen av denne hendelsen. Personvernombudet får en melding om avvik som registreres i Compilo. Personvernombudet leser disse avvikene før de lukkes av leder, men er i

liten grad involvert i oppfølgingen av mindre alvorlige avvik. Dersom et avvik er alvorlig, blir personvernombudet også varslet direkte.

2.2.2. Revisors vurdering av kommunens ordning med personvernombud

Personvernombudets rolle og ansvar er tydelig beskrevet. Dokumentasjonen viser at personvernombudet har en uavhengig rolle, ved at personvernombudet rapporterer til kommuneledelsen, men ikke instrueres i utførelsen av sine oppgaver. Personvernombudets faglige kvalifikasjoner er ivaretatt gjennom utdanningsbakgrunnen som jurist samt faglige oppdateringer gjennom kurs fra blant annet Datatilsynet.

Innenfor den tiden personvernombudet har til sine oppgaver, går det mest tid til rådgivning. Det er dermed mindre tid til den delen av rollen som handler om å kontrollere kommunens overholdelse av personvernloven og egne rutiner på området. Det har ikke vært noen systematisk rapportering fra personvernombudet til kommuneledelsen når det gjelder avvik.

Det er vår vurdering at kommunen har et personvernombud som er organisert i samsvar med personopplysningsloven.

2.3. Behandlingsprotokoll

Nome kommune skal ha en protokoll over hvilke personopplysninger kommunen behandler.

En protokoll skal vise formålet med behandlingene, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Hvis det er aktuelt, skal også eventuelle databehandlere stå oppført i protokollen. I tillegg anbefaler Datatilsynet at blant annet funksjonsområde (hvilken del av kommunen som bruker opplysningene) og kilde for opplysningene framgår.

2.3.1. Rutiner og system for behandlingsprotokoll

Ifølge informasjonssikkerhetshåndboka har systemeier ansvar for de systemene som benyttes innenfor de områdene vedkommende er virksomhetsleder for. Systemeier skal oppnevne en systemansvarlig. Systemansvarlig skal registrere kommunens systemer i behandlingsprotokollen. Systemet kommunen bruker til behandlingsprotokoll heter Digiorden. Systemeier har ansvar for at Digiorden oppdateres med nye opplysninger om systemene. Informasjonssikkerhetsansvarlig skal sørge for at Digiorden oppdateres etter årlig informasjonssikkerhetsgjennomgang.

I intervjuet opplyser personvernombudet å ha vært involvert i kommunens arbeid med behandlingsprotokollen i en rådgivende rolle, blant annet for å orientere om hvordan regelverket skal forstås.

2.3.2. Registreringer i protokollen

Det er registrert 41 systemer i kommunens behandlingsprotokoll (Digiorden). Alle systemene har status «utført» i Digiorden, hvilket indikerer at registreringen av systemet er fullført.

For alle systemene er det lagt ved en personvernerklæring som retter seg mot brukerne av systemet. Denne informerer om rettigheter som innsyn, retting, sletting og andre relevante rettigheter etter personvernloven. I erklæringen står det at brukeren skal ta kontakt dersom man ønsker å benytte seg av disse rettighetene, men det er ikke oppgitt noen spesiell kontaktinformasjon for dette formålet.

Personopplysningslovens artikkel 30 regulerer hvilken informasjon en behandlingsprotokoll skal inneholde. For eksempel skal en behandlingsprotokoll blant annet inneholde informasjon om behandlingsansvarlig, formål med behandlingen, kategorier av registrerte, kategorier av personopplysninger, beskrivelse av tekniske og organisatoriske tiltak og tidsfrister for sletting. Datatilsynet har utarbeidet en mal for behandlingsprotokoll som både viser obligatorisk informasjon og annen informasjon som Datatilsynet anbefaler at inkluderes i protokollen[3].

Vi har plukket ut følgende systemer i kommunens behandlingsprotokoll til en stikkprøvekontroll:

- Komtek (grunnlagsdata ifm. kommunale avgifter)
- CGM (elektronisk pasientjournal)
- Visma Fakturering (distribusjon av fakturaer via ulike kanaler)
- Compilo (melding og behandling av avvik)
- Visma Familia (journalføring og arkivering, barnevern)

Stikkprøvekontrollen viser at tre av systemene har den nødvendige informasjonen registrert, mens det for Komtek og Visma Familia ikke er registrert hvem som er behandlingsansvarlig.

I en behandlingsprotokoll er det sentralt å registrere et behandlingsgrunnlag. Behandlingsgrunnlaget angir det rettslige grunnlaget for behandlingen av personopplysninger. For mange systemer kan to eller flere behandlingsgrunnlag være relevante, eller treffende. I slike tilfeller skal virksomheten velge ett behandlingsgrunnlag[4]. Vi ser at flere av systemene i stikkprøvekontrollen er registrert med flere behandlingsgrunnlag, i to tilfeller er fire ulike behandlingsgrunnlag registrert. Her er samtykke (personvernforordningen art. 6 nr. 1.a) oppgitt som behandlingsgrunnlag sammen med andre behandlingsgrunnlag, blant annet personvernforordningen art. 6 nr. 1.c (at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse).

[3] Malen (excel-dokument) kan lastes ned her: https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/forordningen/artikkel-30_protokoll-behandlingsansvarlig.xlsx
[4] Datatilsynet har en veiledning til behandlingsgrunnlag her: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/ hvor det blant annet presiseres at virksomheten må bestemme seg for ett behandlingsgrunnlag per formål.

2.3.3. Revisors vurdering av behandlingsprotokoll

Kommunen har en behandlingsprotokoll som viser hvilke opplysninger kommunen behandler i de ulike systemene. Vår vurdering er at kommunen ikke oppfyller revisjonskriteriet på dette området, da noen av de undersøkte systemene ikke er registrert med en behandlingsansvarlig.

Vi vil også bemerke at protokollen har en mangel ved at det i flere tilfeller er oppgitt flere behandlingsgrunnlag for samme formål/system. Dette kan medføre uklarhet om hvilket rettsgrunnlag kommunen har for behandlingen av personopplysninger. Som nevnt er det flere systemer i behandlingsprotokollen hvor samtykke (6.1.a) er oppgitt som behandlingsgrunnlag i kombinasjon med andre behandlingsgrunnlag, for eksempel at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse (6.1.c). De ulike behandlingsgrunnlagene i personvernlovens artikkel 6 er likestilte. Med andre ord er det ikke slik at man må be om samtykke dersom man har et annet behandlingsgrunnlag. Det er heller ikke slik at samtykke nødvendigvis er å foretrekke som behandlingsgrunnlag.

I tilfeller hvor det er innhentet samtykke fra de registrerte, og samtykke er oppgitt som behandlingsgrunnlag i kombinasjon med andre behandlingsgrunnlag, vil det være vanskelig å endre behandlingsgrunnlaget i ettertid. Hvis man for eksempel oppdager en svakhet ved hvordan samtykke er innhentet og dermed endrer behandlingsgrunnlaget til å kun bygge på en rettslig forpliktelse, vil det medføre at de registrerte kan ha fått et feilaktig inntrykk av at samtykke kan trekkes tilbake.

Videre er det viktig å være klar over at et samtykke må være frivillig for å være lovlig (Jarbekk og Sommerfeldt 2019: 63). Det betyr at myndigheter vanskelig kan bruke samtykke som grunnlag for myndighetsutøvelse[5] ettersom det ofte vil være en skjevhet i maktforholdet mellom den som avgir samtykke og den som ber om det. Frivillighet innebærer også at et samtykke når som helst kan trekkes tilbake.

Vi anbefaler at kommunen tar en gjennomgang av sine rutiner for registreringer i behandlingsprotokollen, særlig med hensyn til en mer tydelig presisering av behandlingsgrunnlaget for de ulike formålene. Kommunen bør vurdere hva som eventuelt skal gjøres med de registreringene som allerede ligger inne i protokollen. Videre bør det registreres en behandlingsansvarlig for alle systemene som inngår i protokollen.

[5] Myndigheter kan bruke samtykke som grunnlag for andre aktiviteter enn myndighetsutøvelse. Ett eksempel kan være utsendelse av informasjon.

2.4. Risikovurderinger og DPIA

Nome kommune skal ha risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA).[6]

2.4.1. Fakta om risikovurderinger og DPIA

Risikovurderinger
Kommunens informasjonssikkerhetshåndbok omtaler risikovurderinger og rutiner for dette på ulike steder i dokumentet. Oppsummert beskriver håndboken at risikovurderinger skal gjennomføres ved anskaffelse av nye IT-systemer. I den prosessen skal det også vurderes om det er behov for å utarbeide en DPIA. Videre skal risikovurderinger også gjennomføres ved endringer i systemer eller ved endringer i trusselbildet. Risikovurderinger skal oppdateres i forbindelse med en årlig gjennomgang av informasjonssikkerheten. Systemeier er ansvarlig for den årlige gjennomgangen. I tillegg til systemeier, skal informasjonssikkerhetsansvarlig og/eller personvernombud samt representanter fra IT-drift delta. Dette skal dokumenteres og oppdateres i kommunens system Digiorden.

Kommunen har utarbeidet en generell mal for risikoanalyser med tilhørende støttedokumenter. Malen med tilhørende støttedokumenter beskriver hvordan man går frem for å identifisere, analysere og evaluere risiko. Malen inneholder matriser for hendelsesvurderinger og konsekvensvurderinger.

Vi har mottatt risikovurderinger for flere av kommunens systemer. Flere av risikovurderingene omhandler Fiks-plattformens ulike elementer/systemer (smittesporing, prøvesvar, vaksinestatus, folkeregister). Det foreligger også en DPIA for Fiks smittesporing. Videre har kommunen risikovurderinger for Pasientnett og Klinikermelding. Basert på innsendt dokumentasjon, samt bekreftet i dialog med kommunen, mangler det risikovurderinger for flere av kommunens systemer.

2.4.2. Revisors vurdering av risikovurderinger og DPIA

Kommunen har dokumenter som beskriver rutiner på dette området. Kommunen har også maler og støttedokumenter som inneholder de vesentlige momentene i en risikovurdering. Det følger av personvernforordningen art. 24 at kommunen må gjennomføre risikovurderinger for alle systemer som behandler personopplysninger. Artikkel 35 definerer når det i tillegg skal utføres DPIA. Basert på den innsendte dokumentasjonen og vår dialog med kommunen er det vår vurdering at kommunen ikke i tilstrekkelig grad etterlever egne rutiner og lovkrav på dette området, ettersom det mangler risikovurderinger for flere av kommunens systemer.

[6] DPIA står for Data Protection Impact Assessment

2.5. Tekniske og organisatoriske tiltak

Nome kommune skal ha tekniske og organisatoriske tiltak for å sikre personopplysningene

Denne delen av rapporten tar for seg ulike tekniske og organisatoriske tiltak som Nome kommune har gjennomført for å sikre opplysningene de behandler, utover de tiltakene[7] som utgjør egne kapitler i rapporten. For noen tiltak og rutiner kan det allikevel være noe overlapp med beskrivelsene i de andre kapitlene.

2.5.1. Felles tekniske og organisatoriske tiltak

Nome og Midt-Telemark IKT (NMT IKT) har flere dokumenter med rutinebeskrivelser som inneholder både organisatoriske og tekniske tiltak som skal ivareta sikkerhet og personvern i driften av kommunens løsninger. Disse rutinebeskrivelsene tar for seg områder som tilgang og brukerkontroll, passord, lagring av data, bruk av epost, bruk av it-utstyr, programvare og nettverk, oppstart og avslutning av arbeidsforhold, avhending av datautstyr, samt id-kort. Hvert dokument beskriver formålet med rutinen og hvem rutinen gjelder for, i tillegg til en beskrivelse av selve rutinen. Under følger en kort oppsummering av noen sentrale punkter fra disse dokumentene.

Tilgang og brukerkontroll

- Hver bruker skal tildeles en unik og personlig brukerkonto/ID. Det skal ikke brukes felles brukerprofiler i fagsystemer.
- To-faktor autentisering skal brukes på alle tjenester som er publisert mot internett og levert av en tredjepart (eksempler er Office-pakken og webmail).
- Bruker skal være logget på kun én arbeidsstasjon, og man skal logge ut når man forlater arbeidsstasjonen. Kolleger kan ikke benytte hverandres innlogging.
- Systemeier er ansvarlig for at det gjennomføres en årlig kontroll for å sikre at kun autoriserte brukere har tilgang til fagsystemet.

Passord

- Manuelt tildelte passord skal endres av brukeren til et passord kun brukeren selv kjenner.
- Passord skal lages på en ikke-gjenkjennbar måte.
- Passord skal endres regelmessig.
- Rutinen inneholder flere råd for hvordan en bruker bør konstruere et passord.

Lagring og behandling av data

- Fysiske dokumenter og lagringsmedium (cd, minnepinne, osv.) skal behandles i henhold til aktuelle lovbestemmelser.
- Lagringsmedium skal kasseres i henhold til kommunens rutiner for avhending og kassering.

[7] Organisering, personvernombud, behandlingsprotokoll, risikovurderinger, håndtering av brudd/avvik, innsynsrett og databehandleravtaler.

- Alle data relatert til arbeidet som ikke håndteres av et fagsystem eller arkivet skal lagres på en filserver. Ikke-sensitiv informasjon kan lagres i skyen (Office 365, Teams). Det skal ikke lagres slike data lokalt på PCen.

Bruk av epost

- All jobbrelatert epost skal gå via kommunens epost-løsning (driftes av Nome og Midt-Telemark IKT).
- Dersom beskyttelsesverdig informasjon må sendes via epost skal denne informasjonen sendes som et kryptert vedlegg. Krypteringen skal gjøres med godkjent krypteringsprogram.
- Ved bruk av epost på mobile enheter (mobiltelefon, nettbrett) kan vedlegg leses, men ikke lagres på enheten.
- Telefoner låses etter 3 minutters inaktivitet. Ved aktivering av epost på enheten må brukeren legge inn en 6-sifret kode eller et passord.

Bruk av IT-utstyr, programvare og nettverk

- Ansatte skal få nødvendig opplæring før de får tilgang til kommunens systemer.
- Kommunen benytter sikker print på alle multifunksjonsskrivere (ID-kort eller kode for å skrive ut).
- Bærbare PCer og mobile enheter skal aldri bli liggende uten tilsyn.
- Beskyttelsesverdig informasjon skal ikke lagres på mobile enheter.
- All programvare på ansattes maskiner skal godkjennes.
- Lagring av jobbrelaterte opplysninger på private enheter er ikke tillatt.

Arbeidsforhold: Nytt, avslutning og permisjon

- Ansvarlig leder fyller ut en personalmelding ved inn- og utmelding. Administrator gir nødvendige tilganger.
- IT-kort, nøkler, PCer og mobile enheter leveres til IKT-avdelingen ved avslutning av arbeidsforhold.
- Ved utmelding skal IKT-avdelingen fjerne tilganger og melde til systemansvarlig angående sletting av tilganger i fagsystemer.
- IKT-avdelingen deaktiverer brukerkontoen fra fratredelsestidspunktet og sletter den tre måneder senere.

Avhending av utstyr

- Alt brukt IT-utstyr skal leveres NMT-IKT.
- Harddisker og andre lagringsmedier skal tas ut av brukt utstyr som kasseres eller gjenvinnes.
- Lagringsmedier som inneholder sensitiv informasjon, skal oppbevares på områder som er under kommunens kontroll.
- Ved kassering av harddisker:
    - Dokumenter på harddisken skal slettes med godkjent programvare.
    - Harddisken skal merkes tidspunkt for når den er tatt ut av produksjon, sted og utførende person.
    - Det skal holdes en oversikt over lagrede harddisker som er kassert.
- Innhold på minnepinner skal rutinemessig slettes. Disse skal ikke brukes til permanent lagring eller sikkerhetskopiering.

ID-kort

- ID-kort produseres av Nome og Midt-Telemark IKT. Kortet brukes som nøkkelkort og til sikker utskrift.
- Mistet ID-kort skal umiddelbart meldes inn.
- Ansatte som slutter eller går ut i permisjon skal levere ID-kort til nærmeste leder.
- Besøkende skal ikke oppholde seg i kommunens lokaler uten å være i følge av en ansatt.

2.5.2. Observasjoner fra enhetene og systemene

Flere av punktene nevnt ovenfor var tema under intervjuene med skolen og hjemmetjenesten i kommunen. I begge enhetene var det faste rutiner for de ansattes tilganger, både knyttet til etablering av brukerkontoer ved oppstart av arbeidsforhold, samt mer detaljert tilgangsstyring underveis i arbeidsforholdet. Enhetene har rutiner og løsninger som sørger for at de ansatte har de tilgangene som er nødvendig i utførelsen av sine oppgaver.

I begge enhetene blir det oppbevart og behandlet personopplysninger på papir. I hjemmetjenesten handler dette om medisinlister, samt annen informasjon knyttet til brukerne (arbeidslister og hovedkort). Noe av dette er en papirbasert sikkerhetskopi i tilfelle de digitale systemene er nede, men medisinlistene er i bruk i den vanlige driften. I intervjuet fremkom det at hjemmetjenesten har rutiner for fysisk sikring av de papirbaserte opplysningene. Dokumentene oppbevares på tjenestens vaktrom. Dette rommet er låst og kun tilgjengelig for de ansatte. Hjemmetjenesten

benytter kun papirer for opplysninger som er nødvendig for de nåværende brukerne. Dokumentene oppdateres jevnlig og gamle dokumenter blir makulert når det ikke lenger er behov for dem.

I skolen oppbevares det opplysninger på papir i form av et «skyggearkiv», som er en papirbasert kopi av arkivsystemet i kommunen, Websak. Denne løsningen har vært nødvendig da lærerne på skolen ikke har tilgang til Websak. I papirarkivet oppbevares det kun opplysninger om nåværende elever. Det er altså ment som et verktøy for lærerne, og ikke som et permanent arkiv (da brukes Websak, og dokumenter kan hentes ut av administrasjonen ved behov). Skolen har etablert rutiner for hvordan papirarkivet skal brukes. Dokumentene oppbevares i et låst arkivskap på et kontor i den delen av bygget hvor administrasjonen hører til. Når lærere har behov for opplysninger fra dette arkivet, skal dokumentene leses i det samme rommet som de oppbevares i. Lærerne tar ikke med dokumentene til sine egne arbeidsområder. Dokumentene forlater heller ikke skolens område.

I skolen behandles det også opplysninger på digitale lagringsmedier (utenfor kommunens digitale systemer). Dette gjelder rådgivere innenfor spesialpedagogikk, som har en minnepinne for hver elev de har ansvar for. Skolen har valgt denne løsningen ettersom rådgiverne må kunne jobbe med redigerbare dokumenter, men ønsker å unngå at dokumentene ligger lagret på et fellesområde hvor flere personer kan ha tilgang. Det jobbes kun via minnepinnene på et lukket rom hvor de også oppbevares. I etterkant arkiveres dokumentene i Websak som skolens administrasjon har tilgang til.

Hjemmetjenesten kommuniserer og utveksler dokumenter med andre aktører via sitt fagsystem, Profil, som har den nødvendige funksjonaliteten og kan brukes mot alle aktører de samhandler med. Det eneste unntaket er medisinlister som ikke ligger inne i Profil fra hjemmetjenestens side. Hvis det er behov for utveksling av medisinlister, blir listene overlevert på papir via tjenestens ansatte (utveksles typisk med andre enheter i kommunen). Dersom brukere eller pårørende ønsker tilgang til informasjon, har enheten en rutine for å skrive dette ut på papir og kalle inn til et møte, slik at de kan gå gjennom dokumentene sammen. Hjemmetjenesten opplyser imidlertid at de ikke får slike henvendelser, slik at dette ikke har vært en aktuell problemstilling.

Skolen kommuniserer med andre aktører via arkivsystemet Websak. I noen tilfeller kan det forekomme at skolen mottar informasjon på papir. Dette blir da arkivert i Websak for videre behandling. Skolen opplyser at de får krav om innsyn i elevmapper, enten fra foresatte eller fra (myndige) tidligere elever. Slike forespørsler behandles via Websak. Skolen har en rutine på å gå gjennom elevmappen for å fjerne interne notater før mappen utleveres. Interne notater er i denne sammenhengen informasjon som skolen har ment at bør dokumenteres. De som ber om innsyn, får ikke informasjon om at de interne notatene eksisterer og at de er blitt fjernet før mappen ble utlevert.

Begge enhetene opplyser at det jevnt over er oppmerksomhet på problemstillinger knyttet til informasjonssikkerhet og personvern. Hjemmetjenesten gir alle nye ansatte kurs i taushetsplikt, mobilbruk og rutiner angående brukernes personvern. Eksisterende ansatte tilbys regelmessig kurs som omhandler personvern og etikk. Skolens ansatte mottar jevnlig eposter fra kommunens

IT-tjeneste med informasjon om IT-sikkerhet og phising. Disse epostene inneholder også spørsmål som de ansatte kan svare på, og leder får en oversikt over hvilke ansatte som har fulgt opp dette.

Det har i senere tid vært medieoppslag om mulige personvernkonsekvenser av rutiner for tildeling av passord i grunnskolen basert på hendelser i andre kommuner[8]. Gjennom intervjuet med skolen var derfor generering og tildeling av passord et tema. Skolen har rutiner og tekniske løsninger som sørger for at elevene har ulike passord, og at tildelte passord endres ved første innlogging i systemet. For de yngste elevene anvender imidlertid skolen et felles passord for pålogging til Teams. Skolen og elevene bruker Teams til kommunikasjon, oppgaver, innleveringer og annet faglig arbeid. Dersom foreldre skal oppgi sensitive opplysninger i kommunikasjon med skolen skal de bruke sin egen tilgang i Visma, slik at denne typen opplysninger ikke skal forekomme i Teams.

2.5.3. Revisors vurdering av tekniske og organisatoriske tiltak

Nome kommune har tekniske og organisatoriske tiltak for å sikre personopplysningene, både overordnet på kommunenivå og i de utvalgte enhetene vi har observert.

Generelt sett ga de utvalgte enhetene inntrykk av å ha høy oppmerksomhet på personvern. Det ble redegjort for flere ulike tiltak og rutiner for å ivareta informasjonssikkerheten. I begge enhetene var det en stor grad av bevissthet rundt å bruke sikre kanaler for formidling av personopplysninger.

Vi mener at kommunen bør se på de overordnede rutinebeskrivelsene og vurdere hvorvidt noen av disse bør oppdateres. For eksempel virker det som om manuell kryptering av personopplysninger i eposter er en lite brukt løsning i kommunen. Ved slike behov bruker enhetene andre løsninger/kanaler for deling av informasjon og dokumenter.

Våre undersøkelser viser også at det kan være gevinster å hente på en videre digitalisering som fjerner eller reduserer behovet for å behandle personopplysninger på papir. Slik behandling utgjør en viss risiko for at personopplysninger kan komme på avveie. Et tydelig eksempel på dette er skolen, hvor personopplysninger må behandles og lagres i et papirarkiv og på minnepinner fordi lærerne ikke har tilgang til den digitale arkivløsningen Websak.

[8] Se for eksempel NRK sin artikkel om problemstillingen her: https://www.nrk.no/vestfoldogtelemark/alle-elevene-bruker-samme-passord-_-barn-logget-seg-inn-pa-hverandres-teams-kontoer-1.15612577

2.6. Håndtering av brudd på personopplysningssikkerheten

Nome kommune skal ha rutiner for å håndtere brudd på personopplysningssikkerheten.

Håndtering av brudd på personopplysningssikkerheten handler om å både ha rutiner og et egnet system for registrering og oppfølging av avvik. Med tanke på registrering er det vesentlig at kommunens ansatte er bevisste og har kompetanse på avviksregistrering. Videre må det være kompetanse og rutiner knyttet til oppfølging av de registrerte avvikene.

2.6.1. Rutiner for avvikshåndtering

Rutiner for håndtering av avvik er omtalt i informasjonssikkerhetshåndboken. I tillegg har kommunen et eget dokument, «Rutine for sikkerhetsbrudd på personvern», som redegjør for kommunens rutiner på dette området. Her fremgår det at et brudd innebærer utilsiktet eller ulovlig sletting, tap eller endringer av data, eller ulovlig spredning av eller tilgang til personopplysninger.

De mest sentrale delene av rutinen innebærer at et avvik på personvernområdet umiddelbart skal registreres i Compilo[9]. Deretter skal det foretas en risikovurdering og man skal vurdere om personvernombudet bør kontaktes direkte (personvernombudet får uansett en melding i Compilo). Videre skal det vurderes om bruddet er av en slik art at de berørte skal varslet. Ved brudd på personvernsikkerheten skal Datatilsynet varsles innen 72 timer. Hendelsen skal dokumenteres og det skal vurderes konsekvenser og tiltak.

Leder har ansvar for at alle ansatte er kjent med hvordan avvik skal registreres i Compilo. Personvernombudet skal være med på å vurdere alvorlighetsgraden og om andre ressurser skal involveres.

I intervjuet med personvernombudet kom det frem at det har vært ett tilfelle av brudd på personvernet som ble varslet til Datatilsynet, og hvor kommunedirektøren ble involvert i håndteringen. I samarbeid med leverandøren av det berørte systemet ble det satt i verk tiltak for å hindre at det kan skje på nytt.

Personvernombudet opplyser at det forekommer noe feilregistrering av avvik, men at dette da blir rettet i etterkant. Det er få avvik på informasjonssikkerhet og personvern. Det kan skyldes underrapportering, men det er vanskelig å fastslå det sikkert.

Verken skolen eller hjemmetjenesten (de to intervjuede enhetene) har registrert avvik som gjelder informasjonssikkerhet/personvern.

[9] Compilo er kommunens system for registrering og oppfølging av avvik.

2.6.2. Revisors vurdering av rutiner ved brudd på personopplysningssikkerheten

Kommunen har rutiner for å registrere, dokumentere og følge opp avvik som handler om brudd på personopplysningssikkerheten. Rutinene beskriver hele prosessen rundt håndtering av et brudd. Det er få avvik på dette området, men basert på personvernombudets erfaring med tidligere avvik er vårt inntrykk at kommunen har en rutine som er tilstrekkelig for å håndtere slike avvik.

2.7. Ivaretakelse av de registrertes innsynsrett

Nome kommune skal ha tiltak for å ivareta innsynsretten til de registrerte.

Kommunen skal gi klar og tydelig informasjon til den registrerte. Den registrerte skal også få informasjon om hvordan vedkommende kan utøve sine rettigheter. Datatilsynet anbefaler kommunen å ha en personvernerklæring på sine nettsider, med generell informasjon om kommunens personvernpolicy.

Den registrerte skal få informasjon fra kommunen ved innsamling av opplysningene (art. 13), og har rett til innsyn i de personopplysningene kommunen har om vedkommende (art. 15). Den registrerte skal ha rett til å få uriktige personopplysninger om seg selv rettet (art. 16), og kan også i spesielle tilfeller ha rett til å få slettet personopplysninger om seg selv (art. 17).

2.7.1. Tiltak for å ivareta de registrertes innsynsrett

På kommunens nettside er det informasjon om personvernregler og kommunens behandling av opplysninger om innbyggerne. Denne informasjonen finner man ved å navigere via følgende bane på nettsiden:

Personvern -> Personvernerklæring

Her opplyses det om kommunens behandling av opplysninger og hvilke rettigheter individer har, inkludert retten til innsyn, og det beskrives hvordan man kan gå frem dersom man ønsker å kontakte kommunen om dette, inkludert kontaktinformasjon. Det er også oppgitt kontaktinformasjon til kommunens personvernombud. I tillegg er det informasjon om hvordan man kan klage til Datatilsynet dersom man mener at kommunens behandling av opplysninger er i strid med personvernlovgivningen.

Informasjonssikkerhetshåndboken beskriver innsynsretten til personer som er registrert i kommunens systemer, og slår fast at disse alltid skal få innsyn i hvilke opplysninger som behandles, hva opplysningene brukes til, samt hvor lenge opplysningene vil bli lagret.

2.7.2. Observasjoner fra enhetene/intervjuene

Personvernombudet opplyser at hun har mottatt få spørsmål fra innbyggere angående personvern og innsynsrett, og ingen henvendelser om innsyn etter personvernloven. Intervjuer med to av

enhetene i kommunen viser samtidig at henvendelser om innsyn fra innbyggerne som regel kommer direkte til den relevante enheten og ikke via personvernombudet.

Skolen
Foresatte får en innføring i relevant fagsystemer og apper på foreldremøter og elevene får opplæring i dette i klasserommet. Utover dette har ikke skolen noen rutine for å informere om hvordan skolen behandler personopplysninger.

Skolen får innsynskrav, både relatert til nåværende og tidligere elever, og behandler slike henvendelser via Websak. Skolen har en rutine for å gå gjennom elevmappen og fjerne interne notater før innholdet i mappen blir utlevert. Det blir ikke opplyst til den som ber om innsyn at disse personopplysningene finnes, og dermed gis det heller ikke avslag med begrunnelse, henvisning til hjemmel, og informasjon om at avslaget kan påklages.

Hjemmetjenesten
Hjemmetjenesten informerer om hva slags opplysninger de har behov for og innhenter samtykke til dette, samt eventuelt samtykke/fullmakt for pårørende, ved førstegangsbesøk. De har ikke mottatt henvendelser om innsyn, men har en rutine for dette om det skulle være aktuelt.

2.7.3. Revisor vurdering av tiltak for ivaretakelse av de registrertes innsynsrett

Nome kommune har tiltak for å ivareta innsynsretten til de registrerte, både interne rutiner og informasjon til publikum om rettigheter og hvordan den registrerte kan utøve rettighetene i kommunen.

De undersøkte enhetene (skolen og hjemmesykepleien) mottar og håndterer innsynskrav, og de har rutiner som sikrer at personopplysninger ikke blir utlevert til uvedkommende. Vi registrerer at skolen i noen tilfeller tar ut interne dokumenter før det gis innsyn i saksmapper. Vi har ikke vurdert denne praksisen opp mot annet regelverk utover personopplysningsloven (forvaltningslov, offentlighetslov, mv.v), men en slik praksis kan være i strid med de grunnleggende rettighetene til den registrerte. Kommunen bør vurdere om rutinene og saksbehandlingen her ivaretar kravene i lovverket.

2.8. Databehandleravtaler

Nome kommune skal ha system for å sikre at kommunen har databehandleravtale med alle databehandlere, og at databehandleravtalene ivaretar kommunens behov.

2.8.1. Fakta om databehandleravtaler

Kommunens rutine, som finnes i informasjonssikkerhetshåndboken, sier at det skal inngås en databehandleravtale med leverandører eller andre partnere som behandler personopplysninger. Rutinebeskrivelsene knyttet til leverandører og partnere, samt anskaffelse av IT-systemer, er ellers ikke utdypende når det gjelder utformingen av databehandleravtaler, men det vises til kommunens mal for databehandleravtaler. Denne malen synes å inneholde de nødvendige punkter for å ivareta personvernforordningen art. 28 nr. 3.

Rutinen beskriver at alle databehandleravtaler skal arkiveres i kommunens sak-/arkivsystem og i tillegg kobles opp mot det aktuelle systemet i Digiorden. I forbindelse med stikkprøvekontrollen av behandlingsprotokollen for utvalgte systemer i Digiorden undersøkte vi også om det var koblet/lenket inn en databehandleravtale for systemet. Vår gjennomgang viste at det ikke var tilfellet. Dette betyr ikke at databehandleravtaler ikke finnes for disse systemene, det betyr kun at den ikke er lenket til systemet i kommunens oversikt i Digiorden.

Personvernombudet opplyser at hun har brukt en del ressurser på kommunens databehandleravtaler. Det gjelder både oppfølging og re-signering av eksisterende avtaler, samt rådgivning til ledere i kommunen i forbindelse med inngåelse av nye avtaler. Kommunen har hatt gående en prosess for å få eksisterende leverandører over på kommunens nye databehandleravtale og i noen tilfeller har det vært utfordrende. Ved alle nye anskaffelser er det kommunens databehandleravtale som skal brukes som standard.

Personvernombudet opplyser at det er utfordrende å kontrollere eksisterende avtaler ettersom det ikke foreligger en god nok oversikt over alle avtalene.

2.8.2. Revisors vurdering av databehandleravtaler

Kommunen har en oppdatert mal for databehandleravtaler som brukes ved nye anskaffelser. I tillegg har kommunen gående en prosess for å få eksisterende leverandører over på den nye avtalen. Kommunens standard databehandleravtale imøtekommer de kravene som stilles personopplysningsloven.

Kommunen ser ikke ut til å ha fulgt egen rutine om at databehandleravtalene skal kobles til fagsystemet i Digiorden. Dersom denne rutinen hadde vært fulgt ville det bidratt til å styrke personvernombudets mulighet til å følge opp og kontrollere avtalene. Dette er særlig relevant for eksisterende systemer med eldre databehandleravtaler som ikke følger den nåværende malen.

3. Konklusjoner og anbefalinger

3.1. Konklusjoner

I denne delen av rapporten vil vi oppsummere og konkludere rundt de to problemstillingene i forvaltningsrevisjonen.

Har Nome kommune etablert tiltak for å ivareta kravene i personopplysningsloven?
Vi finner at kommunen i stor grad har etablert gode tiltak for å ivareta kravene i personopplysningsloven, slik dette er beskrevet i styrende dokumenter på området og andre rutinebeskrivelser.

Samtidig mener vi at kommunen samlet sett har potensiale for forbedring. Noen rutiner som beskrives i styrende dokumenter på området følges ikke opp på alle punkter. For eksempel har det ikke vært gjennomført en årlig «ledelsens gjennomgang» med rapportering på informasjonssikkerhet og personvern, inkludert avvik, til kommunedirektøren. Det er samtidig slik at informasjonssikkerhet, personvern og avvik har vært oppe som tema på møter i kommunens ledergruppe.

Kommunen har ikke gjennomført risikovurderinger for alle sine systemer som behandler personopplysninger.

Styrende dokumenter på området informasjonssikkerhet inneholder noen punkter som fremstår som uavklarte, eller under arbeid. Det er behov for å oppdatere de styrende dokumentene.

Det er noen svakheter i kommunens oversikt over systemer og tilhørende dokumenter. Databehandleravtaler er ikke lenket til systemet i Digiorden, noe som gjør personvernombudets kontrollfunksjon mer utfordrende. For flere systemer i behandlingsprotokollen i Digiorden er det uklart hvilket behandlingsgrunnlag som ligger til for kommunens behandling av personopplysninger, da flere behandlingsgrunnlag er registrert samtidig. Det er en særlig utfordring at samtykke registreres som behandlingsgrunnlag sammen med rettslig forpliktelse eller andre behandlingsgrunnlag som ikke krever samtykke.

Hvordan blir personopplysningsloven og kommunens egne tiltak fulgt opp i praksis i kommunens enheter?

For å svare på denne problemstillingen har vi undersøkt to utvalgte enheter i kommunen, en skole og hjemmetjenesten, gjennom intervjuer med ledelsen ved enhetene.

På et overordnet nivå fikk vi et godt inntrykk av hvordan det tenkes rundt, og jobbes med, informasjonssikkerhet og personvern i disse enhetene. I denne oppsummeringen vil vi ta utgangspunkt i prinsippene om fortrolighet og tilgjengelighet, som er to viktige prinsipper innenfor området informasjonssikkerhet.

Når det gjelder fortrolighet er vårt inntrykk at begge enhetene er bevisste på å behandle personopplysninger om elever og pasienter/brukere i godkjente fagsystemer så langt det lar seg gjøre, og de er bevisste på å bruke andre sikre kanaler når det er behov for å utveksle personopplysninger utenom fagsystemene. Det er rutiner for kontroll av fullmakt ved innsynsforespørsler og gode rutiner for utsendelse av personopplysninger til rett mottaker.

Tilgjengeligheten på personopplysninger er godt ivaretatt i enhetene. Begge enhetene har gode systemer og gode rutiner som sørger for at ansatte har tilgang til de opplysningene som er nødvendige ut fra deres rolle og ansvarsområde. Enhetene har, i samarbeid med kommunen og IKT-drift, gode rutiner for tilgangsstyring. Hjemmetjenesten har en papirbasert sikkerhetskopi av viktige opplysninger for beredskapssituasjoner slik at nødvendig hjelp kan ytes til brukerne ved en hendelse som gjør det digitale systemet utilgjengelig. Medisinlister behandles på papir i den vanlige driften, men det er gode rutiner for sikkerhet/tilgang på disse dokumentene. Når det gjelder skolen, er bruken av papirkopier noe mer omfattende ved at elevmappene kopieres til et papirarkiv i tillegg til det digitale arkivet. Denne praksisen innebærer en viss risiko som kunne vært redusert dersom opplysningene var tilgjengelig digitalt. Skolen har imidlertid gode rutiner for tilgang til, og bruk av, minnepinnene og opplysningene i papirarkivet.

3.2. Anbefalinger

Vi anbefaler at Nome kommune

- oppdaterer informasjonssikkerhetshåndboken og andre styrende dokumenter på området informasjonssikkerhet og personvern, eventuelt utarbeider nye overordnede styringsdokumenter på området
- sikrer en formalisering av rapporteringen på området og sørger for at praksis samsvarer med rutiner som beskrives i styrende dokumenter,
- gjennomgår rutinene for registreringer i behandlingsprotokollen, og sørger for at behandlingsgrunnlaget for de ulike formålene blir presist og angitt
- gjennomfører risikovurderinger og DPIA i samsvar med lovkravene og egne rutiner
- vurderer om rutiner og saksbehandling knyttet til krav om innsyn i personopplysninger ivaretar de registrertes rettigheter
- vurderer om bruken av papirbaserte systemer helt eller delvis kan erstattes med digitale løsninger når kommunens enheter behandler personopplysninger

Litteratur og kildereferanser

Lover og forskrifter

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysingsloven)

Lov 22. juni 2018 nr. 83 om kommuner og fylkeskommuner (kommuneloven).

Forskrift 17. juni 2019 nr. 904 om kontrollutvalg og revisjon

Offentlige dokument

Prop.56 LS (2017–2018)	Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen)

Kommunens dokumenter

Dokument	Informasjonssikkerhetshåndbok.
Dokument	Roller og ansvar i internkontroll- og sikkerhetsarbeidet.
Dokument	Rutinebeskrivelsene fra NMT IKT vedlagt informasjonssikkerhetshåndbok.
Dokument	Personvern – innsyn rutine.
Dokument	Avviksrutine Nome.
Dokument	Kommunens oversendte risikovurderinger og DPIA.
Dokument	Kommunens mal for databehandleravtale.
System	Digiorden – Gjennomgang av kommunens registreringer.

Elektroniske kilder

Datatilsynet: https://www.datatilsynet.no/, nettsides beskrivelser og veiledere knyttet sentrale deler av etterlevelse av personvernloven:

- «Behandlingsansvarlig og databehandler», sist endret 17.07.19. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler
- «Behandlingsgrunnlag», sist endret 30.05.18. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/
- «Hvordan lage en databehandleravtale?», sist endret 20.12.19. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/hvordan-lage-en-databehandleravtale/
- «Veiledning om de grunnleggende personvernprinsippene», sist endret 16.07.19. https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/

NRK, *Alle elevene bruker samme passord: - Jeg ble rett og slett sjokkert,* nettside, 23.08.2021 https://www.nrk.no/vestfoldogtelemark/1.15612577

Bøker

Jarbekk, Eva og Simen Sommerfeldt, Personvern og GDPR i praksis. Oslo: Cappelen Damm Akademisk, 2019.

Vedlegg

Vedlegg 1: Kommunedirektørens uttalelse

NOME KOMMUNE

Vestfold og Telemark Revisjon Iks
Postboks 311
3701 SKIEN

Dato: 24.05.2022

Unntatt offentlighet OL§5

Vår ref:	**Att:**	**Saksbehandler:**
21/2794-6	v/L.F. Aa.Pedersen	Rune Engehult, 95980059 ruen0108@nome.kommune.no

Kommunedirektørens uttalelse

Jeg viser til utkast til forvaltningsrevisjonsrapport om informasjonssikkerhet og personvern.

I henhold til § 14 i forskrift om kontrollutvalg og revisjon legger jeg med dette fram min uttale til rapporten.

Jeg er ikke kjent med at rapporten inneholder mangler, feil eller misforståelser.

Etter min vurdering gir rapporten et godt bilde av den faktiske situasjonen; - det er i stor grad etablert gode tiltak for å ivareta kravene i personopplysningsloven, og det jobbes og tenkes godt med personvern og informasjonssikkerhet ute i virksomhetene. Samtidig er det nødvendig å sørge for at rutinene oppdateres og følges opp.

Rapporten gir gode anbefalinger for kommunens forbedringsarbeid innenfor informasjonssikkerhet og personvern.

Med hilsen

Rune Engehult
Kommunedirektør

Dokumentet er elektronisk godkjent og har derfor ingen signatur

Postadr: Ringsevja 30, 3830 Ulefoss | Besøksadr: Ringsevja 30, 3830 Ulefoss
E-post: postmottak@nome.kommune.no | www.nome.kommune.no | Tlf.: 35 94 62 00
Fakturaadr.: Ringsevja 30, 3830 Ulefoss | Org.nr. 964 963 371 | Bankkonto: 2650.07.01136

Vedlegg 2: Revisjonskriterier

Kommunens ansvar for forsvarlig håndtering av personopplysninger er regulert av personopplysningsloven. Personopplysningsloven gjennomfører EUs personvernforordning (GDPR) i norsk rett, jf. personopplysningsloven § 1. Formålet er å fastsette regler om vern av fysiske personer i forbindelse med behandling av personopplysninger, og regler om fri utveksling av personopplysninger.

Personopplysningsloven og forordningen gjelder for helt eller delvis automatisert behandling av personopplysninger og for ikke-automatisert behandling av personopplysninger dersom opplysningene inngår i eller skal inngå i et register, jf. personopplysningsloven § 2.

Kommunen behandler personopplysninger om innbyggere, ansatte og politikere. For å ivareta en forsvarlig behandling av personopplysningene, plikter kommunen å sette i verk egnede tiltak for å sikre og påvise at personopplysninger behandles i samsvar med regelverket, jf. personvernforordningen art. 24. Tiltakene skal være både tekniske og organisatoriske, og kommunen skal ha en systematisk tilnærming til dette (internkontroll). Internkontrollen skal ivareta den registrertes rettigheter og friheter, og ivareta virksomhetens mål med behandlingen av personopplysningene. Tiltakene skal dokumenteres og oppdateres ved behov.

Personopplysningene skal beskyttes mot uberettiget innsyn og endringer, men skal være tilgjengelige for de som trenger opplysningene, når de trenger dem.

Behandlingsansvarlig

Behandlingsansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. personvernforordningen art. 4. Det betyr at Nome kommune er behandlingsansvarlig for personopplysninger som kommunen samler inn og benytter.

Den som behandler personopplysninger på vegne av andre, er databehandler. Personvernforordningen setter strenge krav til databehandlere. Vi undersøker ikke situasjoner der Nome kommune eventuelt er databehandler på vegne av andre oppdragsgivere.

Det er Nome kommune som juridisk person som er behandlingsansvarlig. Ledelsen kan delegere oppgaver knyttet til behandling av personopplysninger, men selve behandlingsansvaret kan ikke delegeres.

Personvernombud

Offentlige myndigheter og organer som behandler personopplysninger, skal utpeke personvernombud. Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner, og særlig på grunnlag av dybdekunnskap om personopplysningsloven og praksis på området samt evne til å utføre oppgavene. Personvernombudet kan være en ansatt hos kommunen, eller kommunen kan kjøpe tjenesten. Personvernombudet skal ikke ha andre oppgaver som kommer i

konflikt med rollen, og kan ikke avsettes eller straffes for å utføre sine oppgaver som personvernombud. Personvernombudet skal gi råd til ledelsen i kommunen, kontrollere at kommunen følger personvernreglene og være kontaktpunkt for Datatilsynet (personvernforordningen art. 37, 38 og 39).

Personvernprinsippene

Når virksomheter behandler personopplysninger, skal behandlingen baseres personvernprinsippene i art. 5 i personvernforordningen. Prinsippene er:

- lovlighet, rettferdighet og åpenhet
- formålsbegrensning
- dataminimering
- riktighet
- lagringsbegrensning
- integritet og fortrolighet
- ansvarlighet

Personopplysningsloven bygger på disse prinsippene. Datatilsynet har utdypet prinsippene i en veileder. Nome kommune som behandlingsansvarlig har ansvar for å følge opp disse prinsippene.

Lovlig, rettferdig og gjennomsiktig

Personvernforordningen art. 6 regulerer i hvilke tilfeller det er lovlig å behandle personopplysninger. Det rettslige grunnlaget kan blant annet være samtykke fra den registrerte, at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse, eller for å utøve offentlig myndighet.

Dersom kommunen behandler sensitive personopplysninger, må i tillegg minst ett av vilkårene i personvernforordningen art. 9 være oppfylt. Disse kravene er blant annet at det foreligger uttrykkelig samtykke fra den registrerte, at behandlingen er nødvendige for at kommunen skal oppfylle sine forpliktelser innenfor arbeidsrett, trygderett og sosialrett, eller at behandlingen er nødvendig for å yte helse og sosialtjenester.

At behandlingen skal være rettferdig, innebærer at kommunen skal ha respekt for den registrertes interesser og rimelige forventinger.

At en behandling er åpen, innebærer at det er oversiktlig og forutsigbart for den registrerte. Personvernforordningen kapittel III omhandler den registrertes rettigheter. Art. 12 krever at kommunen skal gi klar og tydelig informasjon til den registrerte. Den registrerte skal også få informasjon om hvordan vedkommende kan utøve sine rettigheter. Datatilsynet anbefaler kommunen å ha en personvernerklæring på sine nettsider, med generell informasjon om kommunens personvernpolicy. Den registrerte skal få informasjon fra kommunen ved innsamling av opplysningene (art. 13), og har rett til innsyn i de personopplysningene kommunen har om vedkommende (art. 15). Den registrerte skal ha rett til å få uriktige personopplysninger om seg

selv rettet (artikkel 16), og kan også i spesielle tilfeller ha rett til å få slettet personopplysninger om seg selv (art. 17).

Formålsbegrensning
Personopplysninger skal bare brukes til det formålet de er innhentet for. Hvis personopplysninger skal gjenbrukes, må behandlingen enten være lovfestet eller det må innhentes nytt samtykke.

Dataminimering
Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere innsamlingsformålet.

Riktighet
Personopplysninger som behandles skal være korrekte. Opplysningene skal også oppdateres hvis det er nødvendig.

Lagringsbegrensning
Prinsippet om lagringsbegrensning innebærer at personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble innhentet for. Kommunen bør innføre tidsfrister for sletting eller periodisk gjennomgang for å sikre at personopplysninger ikke oppbevares lengre enn nødvendig.

Integritet og fortrolighet
Kommunen skal sørge for:

- beskyttelse mot uautorisert utlevering og tilgang til personopplysninger
- beskyttelse mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger
- at personopplysninger er tilgjengelige for autoriserte personer når det er nødvendig
- at personopplysninger ikke gjøres tilgjengelig for et ubegrenset antall mennesker uten den berørte personens medvirkning
- å spore endringer som gjøres i systemet og for å kunne håndtere sikkerhetsbrudd
- at systemene som behandler personopplysninger er robuste mot for eksempel sårbarheter, angrep og uhell

Ansvarlighet
Kommunen har ansvar for å opptre i samsvar med reglene for behandling av personopplysninger. Kommunen må også kunne vise at den faktisk opptrer i samsvar med reglene. Dette betyr at kommunen må ha internkontroll.

Internkontroll

Ifølge kommuneloven § 25-1 skal kommunen ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Kommunedirektøren er ansvarlig for internkontrollen.

Kravene til internkontroll for personvern står i kapittel IV i personvernforordningen.

Datatilsynets veileder for internkontroll og informasjonssikkerhet legger til grunn at internkontroll skal bestå av:

- styrende elementer, som i hovedsak retter seg mot ledelsen, herunder hvilke beslutninger og føringer de legger for internkontroll.
- gjennomførende elementer, som i hovedsak retter seg mot ansatte. her finner man beskrivelse av rutiner som er tilpasset den enkeltes arbeidssituasjon.
- kontrollerende elementer, som bidrar til å fange opp avvik fra systemet og til at det gjennomføres periodiske gjennomganger.

Typiske styrende og kontrollerende elementer i internkontrollen er blant annet at ansvar og myndighet må være tydelig plassert, og det må etableres rutiner for rapportering og kontroll.

Ved innføring av internkontroll må virksomheten først identifisere hvilke personopplysninger som behandles. Deretter må det utarbeides en risikovurdering. Så må kommunen lage rutiner og retningslinjer som reduserer risikoen til et akseptabelt nivå.

Art. 30 krever at kommune fører protokoller over behandlingsaktiviteter. En protokoll skal vise formålet med behandlingene, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Hvis det er aktuelt, skal også eventuelle databehandlere stå oppført i protokollen.

Art. 35 krever at ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter, skal kommunen gjennomføre en vurdering av personvernkonsekvenser, også kalt DPIA[10]. DPIA er nødvendig siden kommunen behandler sensitive opplysninger i stor skala. Vurderingen skal minst inneholde

a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen,
b) en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene,
c) en vurdering av risikoene for de registrertes rettigheter og friheter, og
d) de planlagte tiltakene for å håndtere risikoene og for å påvise at personvernreglene overholdes.

Personvernforordningen artikkel 5 nr. 1 bokstav e) krever at kommunen har rutiner som sikrer tilstrekkelig sikkerhet for integriteten og konfidensialiteten til personopplysningene. Kommunen skal sikre personopplysningene mot uautorisert eller ulovlig behandling, og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak. Ifølge artikkel 24 skal kommunen gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at

[10] DPIA står for Data Protection Impact Assessment

behandlingen utføres i samsvar med personvernforordningen. Ifølge artikkel 32 skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som passer til risikoen.

Kommunen skal ha et system for å fange opp brudd på personopplysningssikkerheten. Hvis det oppstår brudd på sikkerheten rundt personopplysninger, skal kommunen melde fra til Datatilsynet. Dersom det er sannsynlig at bruddet vil føre til risiko for personene det gjelder, skal kommunen underrette den registrerte. Alle brudd på personopplysningssikkerheten skal dokumenteres (art. 33 og 34).

Internkontroll og arbeidet med informasjonssikkerhet er et dynamisk arbeid som alltid vil være under utvikling. Datatilsynet anbefaler derfor å ha rutiner for å forbedre internkontrollen, herunder rutiner for rapportering fra sikkerhetshendelser, avvikshåndtering og egenkontroll. Rapporteringen skal beskrive hvilke erfaringer som er gjort og inneholde forslag til forbedringer.

Ledelsen i kommunen skal også ha en årlig gjennomgang av sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Målet for gjennomgangen er å sikre at internkontrollen oppfyller kommunens behov og gjøre nødvendige oppdateringer.

Registrertes rettigheter

Den registrerte er den personen personopplysningene omhandler. Den registrerte har rett til å få informasjon ved innsamling av opplysningene, blant annet om formålet og det rettslige grunnlaget for behandlingen, og eventuelle mottakere av personopplysningene (personvernforordningen art 13).

Den registrert har rett til innsyn i hvilke personopplysninger om vedkommende kommunen behandler (personvernforordningen art.15). Den registrerte har rett til å be om at uriktige personopplysninger om seg selv rettes (personvernforordningen art 16). Videre kan den registrerte be om å få personopplysninger om seg selv slettet (personvernforordningen art 17). Det er imidlertid flere begrensninger på retten til å få personopplysninger slettet. Blant annet kan ikke kommunen slette personopplysninger som skal bevares for arkivformål, eller som må bevares for å oppfylle en rettslig forpliktelse.

Databehandlere

En databehandler behandler personopplysninger på vegne av en behandlingsansvarlig (kommunen). Et eksempel på en databehandler er en leverandør av programvare som kommunen bruker til å behandle personopplysninger, hvis leverandøren har tilgang til programmet for å gjøre oppdateringer og support.

Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale. Avtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket, også av databehandleren, og skal sette en klar ramme for hvordan databehandleren

kan behandle personopplysningene. En databehandleravtale kan være en frittstående avtale mellom partene, eller en integrert del av annet avtaleverk.

Den behandlingsansvarlige kan bare benytte databehandlere og underleverandører som kan dokumentere tilstrekkelige garantier for

- at kravene i personopplysningloven blir ivaretatt
- at personopplysningene som behandles er tilstrekkelig sikret (personvernforordningen art. 28 nr. 1).

Kommunen skal vurdere om databehandleren gir tilfredsstillende garantier for de personopplysningene som skal behandles.

En databehandleravtale skal inneholde:

- behandlingens art, formål og varighet
- kategorier av registrerte og typer av personopplysninger
- pliktene og rettighetene til den behandlingsansvarlige
- forpliktelsene til databehandleren

Revisjonskriterier

På denne bakgrunn har vi utledet følgende revisjonskriterier:

Nome kommune skal ha

- **en organisasjon med klar plassering av ansvar og myndighet, samt rutiner for rapportering**
- **personvernombud, organisert i samsvar med personopplysningsloven**
- **protokoll over hvilke personopplysninger kommunen behandler**
- **risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA)**
- **tekniske og organisatoriske tiltak for å sikre personopplysningene**
- **rutiner for å håndtere brudd på personopplysningssikkerheten**
- **tiltak for å ivareta innsynsretten til de registrerte**
- **system for å sikre at kommunen har databehandleravtale med alle databehandlere**
- **system for å sikre at databehandleravtalene ivaretar kommunens behov**

Vedlegg 3: Metode og kvalitetssikring

Forvaltningsrevisjonen startet opp ved oppstartsbrev 29.09.21. Oppstartsmøte ble gjennomført 08.10.21 med kommunedirektør, personvernombudet og representant for kommunens IKT-tjeneste.

Forvaltningsrevisjoner skal gjennomføres på en måte som sikrer at informasjonen i rapporten er relevant og pålitelig. At dataene er relevante (gyldige/valide) innebærer at de beskriver de forholdene som problemstillingene omhandler. Pålitelighet (reliabilitet) handler om at innsamling av data skal skje så nøyaktig som mulig og at det ikke har skjedd systematiske feil underveis.

Innsamling av data, relevans og pålitelighet

Datainnsamlingen startet i oktober 2021, men revisjonen er i hovedsak gjennomført i perioden januar til april 2022. For å kartlegge kommunens tiltak for å ivareta kravene i personopplysningsloven har vi innhentet og gjennomgått dokumentasjon fra kommunen. Denne dokumentasjonen har vært styringsdokumenter, rutinebeskrivelser, samt registreringer i kommunens systemer. En slik kartlegging basert på innsendte dokumenter vil alene gi et begrenset innsyn når det gjelder i hvilken grad rutinene etterleves og hva som er praksis i kommunens daglige drift. Vi har derfor kombinert dokumentgjennomgangen med andre metoder, nærmeste bestemt intervjuer og en stikkprøvekontroll.

Intervjuer

Vi har gjennomført intervjuer med kommunens personvernombud, leder av hjemmetjenesten og rektor ved Holla skole. I intervjuet med skolen deltok også andre ansatte. Intervjuene var semi-strukturerte, hvilket betyr at det ble brukt en intervjuguide, men at intervjuene ellers var åpne med rom for oppfølgingsspørsmål, avklaringer og temaer utenfor intervjuguiden. Det ene intervjuet ble gjennomført digitalt via Teams, mens det andre intervjuet ble gjennomført ved fysisk møte i enhetens lokaler. Intervjudeltakerne mottok en agenda/tema for intervjuet i forkant, og i etterkant av intervjuene ble det sendt ut et referat til godkjenning. Her kunne deltakerne også korrigere eventuelle feil i referatet.

Stikkprøver

Vi gjennomførte en stikkprøvekontroll av kommunens behandlingsprotokoll (her bruker kommunen Digiorden). Det ble valgt ut fem systemer i stikkprøvekontrollen. To av systemene i stikkprøven ble valgt ut fra en vurdering av risiko (omfang og type opplysninger), mens tre av systemene ble valgt tilfeldig. Hensikten med stikkprøvekontrollen var å sjekke hvilke opplysninger som var registrert i protokollen, hvorvidt nødvendige opplysninger var registrert, og mer generelt undersøke hvordan kommunen bruker behandlingsprotkollen. Compilo og Visma Familia ble valgt ut manuelt til stikkprøvekontrollen, mens Komtek, CGM og Visma fakturering ble valgt ut tilfeldig.

Personopplysninger

I forbindelse med denne forvaltningsrevisjonen har vi behandlet personopplysninger som navn og epostadresse til ansatte i kommunen.

Vårt rettslige grunnlag for å behandle personopplysninger er kommuneloven § 24-2 fjerde ledd.

Vi behandler personopplysninger slik det er beskrevet i vår personvernerklæring. Personvernerklæringen er tilgjengelig på vår nettside vtrevisjon.no.

God kommunal revisjonsskikk - kvalitetssikring

Forvaltningsrevisjon skal gjennomføres, dokumenteres, kvalitetssikres og rapporteres i samsvar med kommuneloven og god kommunal revisjonsskikk.[11]

Kvalitetssikringen skal sikre at undersøkelsen og rapporten har nødvendig faglig og metodisk kvalitet. Videre skal det sikres at det er konsistens mellom bestilling, problemstillinger, revisjonskriterier, data, vurderinger og konklusjoner.

Vestfold og Telemark revisjon IKS har et system for kvalitetskontroll som er i samsvar med den internasjonale standarden for kvalitetskontroll.[12] Denne forvaltningsrevisjonen er kvalitetssikret i samsvar med vårt kvalitetskontrollsystem og i samsvar med kravene i RSK 001.

[11] God kommunal revisjonsskikk i forvaltningsrevisjon og eierskapskontroll kommer til uttrykk først og fremst i RSK 001 Standard for forvaltningsrevisjon og RSK 002 Standard for eierskapskontroll. Gjeldende standarder er fastsatt av Norges Kommunerevisorforbunds styre høsten 2020. Standardene bygger på norsk regelverk og internasjonale prinsipper og standarder, fastsett av International Organization of Supreme Audit Institutions (INTOSAI) og Institute of Internal Auditors (IIA).

[12] ISQC 1 Kvalitetskontroll for revisjonsfirmaer som utfører revisjon og begrenset revisjon av regnskaper samt andre attestasjonsoppdrag og beslektede tjenester

På vakt for fellesskapets verdier

Rapporten er utarbeidet av
Vestfold og Telemark revisjon IKS

Har du spørsmål til rapporten?
Ta kontakt med oss:
Telefon: 33 07 13 00
E-post: post@vtrevisjon.no

www.vtrevisjon.no

22: 3816 402