Vestfold og Telemark revisjon

Er innbyggernes opplysninger sikre?

Informasjonssikkerhet i Sandefjord kommune

Forvaltningsrevisjon | Sandefjord kommune

2021:3804 404

Innhold

1. Sammendrag

I denne forvaltningsrevisjonen har vi sett på hvordan Sandefjord kommune arbeider for å etterleve kravene i personopplysningsloven. Loven har som formål å sikre vern om personopplysninger og gir kommunen en rekke plikter som den må oppfylle i den forbindelse.

I hvilken grad har Sandefjord kommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Vi mener at Sandefjord kommunes arbeid med informasjonssikkerhet samlet sett, har potensiale for forbedring.

Sandefjord kommune har i utgangspunktet etablert gode tiltak og føringer for å ivareta kravene i personopplysningsloven, primært i styringsdokumentet *Informasjonssikkerhet og personvern overordnet styringsdokument*. Men dette dokumentet følges ikke opp på alle punkter, for eksempel

- blir det ikke rapport til rådmannen i samsvar med føringer i dokumentet
- kommunen gjennomfører ikke risikovurderinger for sine systemer i det omfang som følger av styringsdokumentet. I dokumentet fremgår det at risikovurderinger skal gjennomføres ved anskaffelse av et system, ved større endringer og ellers minst hvert andre år

Kommunen har en tydelig ansvars- og rollebeskrivelse i stillingsprofilen for personvernombudet, men vi mener at den kan styrkes ved at personvernombudets uavhengighet blir tydeligere beskrevet. Personvernombudet er en 50 prosent stilling tillagt en ansatt med 50 prosent stilling som beredskapskoordinator. Grunnet koronapandemien har personvernombudet blitt bedt om å nedprioritere tidsbruk til oppgaver som personvernombud og prioritere arbeidet med samfunnssikkerhet og beredskap i 2020/21. Personvernombudsrollen skal nå organiseres under kommuneadvokaten og det er to nytilsatte jurister som vil ivareta denne rollen.

Kommunen har opprettet en sikkerhetsgruppe i etterkant av at styringsdokumentet ble vedtatt. Denne gruppa har i økende grad fått en sentral plass i kommunens arbeid med informasjonssikkerhet, men gruppas rolle og oppgaver er enda ikke blitt formalisert i et mandat eller på annen måte.

Kommunen bruker programmet iConfirm til å føre protokoll over sin behandling av personopplysninger. Kommunen har ikke fylt ut protokollen for alle systemer slik som personopplysningsloven krever.

I visse tilfeller er kommunen pålagt å gjennomføre en utvidet risikovurdering, en vurdering av personvernkonsekvenser (DPIA). Kommunen har gjennomført én DPIA og vi mener at kommunen bør vurdere om deres rutiner sikrer at DPIAer blir gjennomført i tilstrekkelig grad.

Kommunen har rutiner for registrering av avvik og har tall som viser hvor mange avvik som er registrert. Vi mener at disse tallene er usikre, fordi funn viser at avvik feilaktig har blitt registrert som avvik på personvern og informasjonssikkerhet.

Kommunen har utarbeidet rutiner som skal sikre trygg bruk av IKT-systemene for sine ansatte, men kommunen bør sikre at alle rutinene er tilgjengelige for ansatte i intranett og kvalitetssystem, noe som ikke er tilfellet i dag. Et annet tiltak for å sikre trygg bruk av IKT-systemene er opplæring. Våre undersøkelser tyder på at kommunen gjennomfører opplæring om informasjonssikkerhet både til ansatte og ledere.

Kommunen har etablert en rutine for anskaffelse av nye systemer hvor blant annet gjennomføring av ROS-analyse, databehandleravtale og involvering av sikkerhetsgruppa i anskaffelsesprosessen blir ivaretatt. Dette mener vi er et godt tiltak for å ivareta kravene i personopplysningsloven.

Har de undersøkte områdene ivaretatt sentrale krav i personopplysningsloven?
For å besvare denne problemstillingen har vi undersøkt fire områder (casestudier). Vi valgte ut to enheter i kommunen en skole og en hjemmesykepleieenhet. Vi valgte også ut to fagsystemer, det skoleadministrative programmet Visma Flyt Skole og SmartVakt Felt. SmartVaktFelt brukes blant annet til å varsle ansatte om utløste trygghetsalarmer (SafeMate), og det er denne funksjonen vi har fokusert på.

Overordnet sett var vårt inntrykk at det er godt fokus på personvern og informasjonssikkerhet, både på de to enhetene og blant de ansvarlige for de to fagsystemene.

I dette sammendraget har vi fokusert på de tre sentrale prinsippene for informasjonssikkerhet: fortrolighet (at opplysningene ikke blir tilgjengelige for uvedkomne), riktighet (at opplysningene i kommunens systemer er korrekte) og tilgjengelighet (at opplysningene er tilgjengelige for de som skal ha tilgang, når de skal ha tilgang). Vi viser til eksempler på hvordan disse prinsippene er ivaretatt i utvalgte enheter/fagsystem.

Når det gjelder fortrolighet, var vårt inntrykk at begge enhetene var beviste på å behandle personopplysninger om elever og pasienter i fagsystemene og bruke sikre kanaler når det var behov for å gjengi personopplysninger i kommunikasjon med andre. Det var også bevissthet rundt fortrolighet når enhetene fikk henvendelser per telefon.

Viktigheten av at opplysninger var riktige fikk vi illustrert i både i Visma Flyt Skole og i den utvalgte skolen. Foresatte har tilgang til opplysninger om elevene i en nettportal. Alle foresatte skal ikke ha tilgang til informasjon om sine barn, derfor er det viktig at det er riktig tilknytning mellom foresatt og elev. Her kunne både de ansvarlige for systemet og skole vise til kontrollrutiner for å sikre at foresatte ikke får tilgang til opplysninger de ikke skal ha.

Det var utarbeidet beredskapsplaner for når SmartVakt Felt og de tilhørende trygghetsalarmene var ute av drift eller var utilgjengelige. I tillegg har hjemmesykepleieavdelingene oversikter på papir

over brukere av trygghetsalarmer i tilfelle systemet er utilgjengelig. Det var ikke tilsvarende beredskapsplaner for Visma Flyt Skole. Begrunnelsen for dette var at systemet har en veldig god oppetid og at hvis systemet hadde nedetid kunne arbeidsprosesser gjøres manuelt og senere ajourføres i systemet.

Tilgangsstyring for ansatte er viktig, både for å sikre fortrolighet og tilgjengelighet til personopplysningene. I SmartVakt Felt er tilgangsstyringen knyttet til journalsystemet CosDoc og det er en sentral enhet i kommunen som registrerer nye ansatte. I Visma Flyt Skole er tilganger i systemet styrt ut fra rolle, denne tilgangsstyringen er satt opp sentralt og den enkelte skole kan ikke endre på dette.

Logging er også et tiltak for å sikre utilsiktet bruk av systemet, og dermed opplysningenes fortrolighet. I begge systemene blir bruken av systemet logget.

I begge enhetene så vi eksempler på at personopplysninger ble behandlet fysisk på papir, selv om det fantes digitale alternativ. Etter vår vurdering vil en digital løsning gi bedre informasjonssikkerhet, fordi den gir bedre mulighet til å styre hvem som får tilgang på informasjonen.

1.1. Anbefalinger

Vi anbefaler kommunen å:

- sikre at rutiner og føringer for informasjonssikkerhet og personvern er oppdaterte og i samsvar med gjeldende krav og anbefalinger
- sikre at det blir skrevet protokoll i samsvar med personopplysningsloven for alle systemer som behandler personopplysninger
- gjennomføre ROS-analyser av alle IKT-systemer som behandler personopplysninger
- sikre at det blir gjennomført vurderinger av personvernkonsekvenser (DPIA) i samsvar med personopplysningsloven
- sikre at avvik om informasjonssikkerhet og personvern blir korrekt registret

2. Innledning

2.1. Kontrollutvalgets bestilling

Forvaltningsrevisjonen er bestilt av kontrollutvalget i Sandefjord kommune i sak 12/21.

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.

2.2. Problemstilling og revisjonskriterier

Rapporten handler om følgende problemstillinger:

1. I hvilken grad har Sandefjord kommune etablert tiltak for å ivareta kravene i personopplysningsloven?
2. Har de undersøkte områdene ivaretatt sentrale krav i personopplysningsloven?

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

2.3. Avgrensning og definisjoner

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

Vi er gjort oppmerksom på at det er tilsatt to nye jurister hos kommuneadvokaten som skal ta over rollen som personvernombud. Disse tiltrer stillingene i november og desember 2021. Henvisninger til personvernombudet i denne rapporten er til den som har rollen frem til november/desember 2021, med mindre noe annet er indikert.

Kommunestyret vedtok å endre tittelen rådmann til kommunedirektør 30. september 2021 (jf. sak 108/21). Da prosjektet vårt ble påbegynt før denne endringen fant sted, har vi valgt å bruke tittelen rådmann i rapporten.

2.4. Metode og kvalitetssikring

Denne forvaltningsrevisjonen er gjennomført av forvaltningsrevisorene Trygve Børsting, Lars Pedersen og Anne Hagen Stridsklev, med Kirsti Torbjørnson som oppdragsansvarlig.

Som en del av datainnhentingen har vi sett nærmere på to enheter (én skole og én hjemmesykepleieavdeling) og to digitale fagsystemer (Visma Flyt Skole og SmartVakt Felt,

[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.

sistnevnte med fokus på trygghetsalarmen SafeMate). På hver av de to enhetene gjennomførte vi et intervju med enhetsleder (og andre som enhetsleder ønsket skulle delta), i forbindelse med intervjuet fikk vi også en kort befaring på enheten. For de to fagsystemene gjennomførte vi et intervju med systemansvarlig og systemeier (dvs. de som har ansvaret for fagsystemet), i et av intervjuene deltok også en ansatt fra IKT. I teksten under vil de bli omtalt som de utvalgte enhetene og systemene. For mer detaljer om utvalget se vedlegg 3.

Vi har tatt stikkprøver av systemer registrert i kommunens protokoll over behandlinger av personopplysninger. Vi har tatt 10 stikkprøver tilfeldig valgt blant systemene registrert i kommunens protokoll. Tre av programmene ble valgt blant de som er klassifisert med risiko kritisk, mens øvrige syv er valgt blant alle programmene. Stikkprøvene er brukt til å vurdere om registeringen av informasjon om systemene i protokollen og til å vurdere gjennomføring av risiko og sårbarhetsanalyser. Se detaljer i vedlegg 3.

I tillegg har vi hatt intervju med personvernombudet. Vi har også hatt en løpende kontakt med IKT-leder, personvernombud og sikkerhetsansvarlig.

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

2.5. Om personopplysningsloven og sentrale begreper

Den gjeldende personopplysningsloven trådte i kraft juli 2018. Loven implementerer EUs personvernforordning (kjent som GDPR). Forordningsteksten er inndelt i artikler, mens de norske særreglene er inndelt i paragrafer, i rapporten følger vi denne inndelingen.
Personopplysningsloven inneholder en del begreper som vi vil kort gjøre rede for her:

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 6-1.

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 28-3.

Personopplysning – definert i personopplysningsloven artikkel 4-1 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 personopplysningsloven artikkel 9-1. Det er ikke tillatt å behandle disse opplysningene med mindre man har hjemmel i artikkel 9-2.

Uttrykket «Kategorier av» brukes i regelverket og kan løst oversettes til «forskjellige typer av».

2.6. Kommunedirektørens uttalelse

Rapporten er presentert i et møte med administrasjonen i kommunen og sendt til uttalelse 10.11.21, jf. forskrift om kontrollutvalg og revisjon § 14. Kommunedirektørens uttalelse ligger i vedlegg 1.

3. Informasjonssikkerhet og personvern

I hvilken grad har Sandefjord kommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Har de undersøkte områdene ivaretatt sentrale krav i personopplysningsloven?

3.1. Organisering – ansvar, myndighet og rapportering

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

3.1.1. Ansvars- og myndighetsfordeling

Sandefjord kommune har utarbeidet dokumentet *Informasjonssikkerhet og personvern overordnet styringsdokument*[2] (heretter styringsdokument for informasjonssikkerhet) hvor organisering, ansvar, myndighet og rutiner for rapportering er beskrevet.

I styringsdokumentet fremgår det at rådmannen har det overordnede ansvaret for informasjonssikkerheten i kommunen. Samtidig er ansvaret for å følge opp lover, regler og interne rutiner vedrørende informasjonssikkerhet i det daglige arbeidet delegert til kommunalsjefene.

Kapittelet strategi i styringsdokumentet, inneholder flere punkter som rådmannen har ansvar for. Blant annet skal han uttrykke en forventing om at ledere skal være pådrivere i arbeidet med informasjonssikkerhet. Rådmannen har opplyst om at dette fulgt opp i flere forum, blant annet i rådmannens ledermøter, i oppfølgingsmøter med seksjonsledere etter formannskapsmøtene, i medarbeidersamtaler med ledere og i arbeidet med rammesak og handlings- og økonomiplan. Temaet ble også diskutert i forbindelse med ny organisering av virksomheten. Rådmannen har i tillegg sendt ut informasjon om og begrunnet viktigheten av informasjonssikkerhet overfor ledere og ansatte i kommunen.

Kommunalsjefene, eventuelt andre som har fått delegert myndighet fra rådmannen, er systemeiere og har dermed myndighet til å velge systemer og inngå avtaler med leverandører, herunder også databehandlere. Det fremgår av styringsdokumentet at IKT-leder og arkivleder alltid skal bes om råd ved anskaffelser av nye systemer. Sikkerhetsleder i kommunen skal involveres i valg av databehandlere og utforming av databehandleravtaler. Systemeier skal utpeke en systemansvarlig for hvert system. De systemansvarlige har det praktiske og daglige ansvaret for å forvalte hvert enkelt system. Dette daglige ansvaret omfatter blant annet tilgangsstyring, retting og sletting av data, autorisering av brukere og oppfølging av internkontroll. Den systemansvarlige kan utpeke én

[2] Styringsdokumentet ble vedtatt av kommunestyret den 18.09.18. Det er ikke blitt revidert siden vedtak, men IKT-leder har opplyst om at det er planlagt en revidering i 2021 eller tidlig 2022.

eller flere systemadministratorer som får tilgang til å opprette brukere eller gjøre andre bestemte endringer i systemet.

Kommunen har en egen sikkerhetsgruppe. Denne ble opprettet i etterkant av at styringsdokument for informasjonssikkerhet ble vedtatt. Det er ikke utarbeidet et eget mandat for gruppa. Etter personvernombudets oppfatning ble gruppa opprettet for å sikre: at protokoll kom på plass, læring, prosess for å ta i bruk nye system og at databehandleravtaler kom på plass. Gruppa har også en rolle og myndighet i forbindelse med anskaffelse av IKT-systemer og andre systemer som behandler personopplysninger (se flyt i vedlegg 4). Gruppa består i dag av sikkerhetsansvarlig, IKT-leder, arkivleder, representant fra kommuneadvokaten og personvernombudet.

I styringsdokument for informasjonssikkerhet fremgår det at det skal utarbeides en årlig handlingsplan for å oppnå sikkerhetsmål. Rådmannen opplyser om at dette er sikkerhetsgruppas ansvar. Det er ikke utarbeidet en skriftlig overordnet handlingsplan, men rådmannen opplyser at følgende tiltak er planlagte:

- utarbeidelse av protokoll i iConfirm
- opplæring og utfylling av protokoll for systemansvarlige
- prosessflyt anskaffelser
- valg av mal databehandleravtale
- tilleggsanskaffelser av nye systemer for ytterligere sikring av kommunens servere

Videre opplyser rådmannen at det er utarbeidet handlingsplan for økt sikkerhetskultur som gjennomføres i 2021-2022.

Intervjuobjektene for de utvalgte enhetene og fagsystemene ble spurt om de hadde kjennskap til sikkerhetsgruppa. En enhet sa at de hadde kjennskap til den på overordnet nivå, mens den andre kjente ikke til gruppa. Systemeier og systemansvarlig for de to utvalgte systemene hadde god kjennskap til sikkerhetsgruppa.

Sikkerhetsgruppa har også en undergruppe (sikkerhetskulturgruppa) som arbeider med å øke ansattes kompetanse slik at de kan identifisere digitale trusler og handle riktig. De skal arbeide for at informasjonssikkerhet skal bli en integrert del av organisasjonskulturen. I tillegg skal gruppa opparbeide og utvikle kommunens kompetanse på området.

IKT sikkerhetsgruppa er en egen gruppe i kommunens IKT-avdeling, som blant annet følger opp rapporterte hendelser i IKT-systemene.

3.1.2. Rapportering

Ledere i kommunen skal rapportere en oversikt over internkontrollaktiviteter hver tredje måned. Kommunalsjefer og øvrige ledere i rådmannens ledergruppe skal rapportere årlig til sikkerhetsansvarlig, som igjen forbereder årsrapporten og ledelsens gjennomgang.

Ifølge styringsdokumentet for informasjonssikkerhet skal rådmannen ha en gjennomgang av informasjonssikkerheten med ledergruppen hvert år. Ifølge rådmannen, er ledelsens gjennomgang planlagt gjennomført i løpet av høsten 2021. I denne gjennomgangen vil rådmannens ledergruppe, sikkerhetsansvarlig og IKT-sjef delta. Personvernombud vil delta om det er behov. Rådmannen er ikke kjent med at det er gjennomført en slik gjennomgang tidligere.

I styringsdokumentet er det også fastsatt at rådmannen skal etterspørre flere typer rapportering. Han skal be om resultater fra avvikshåndtering, egenkontroll og evalueringer. Her opplyser rådmannen at han får løpende rapportering om større avvik. Han opplyser også at kommunen har etablert praksis for erfaringsdeling og evaluering etter større hendelser, og at slik evaluering vil også bli gjort hvis det er et større avvik på personvern eller informasjonssikkerhet.

Rådmannen skal videre etterspørre rapport om IKT-hendelser to ganger i året. Rådmannen opplyser at han får løpende varsel om IKT-hendelser av en viss størrelse. Videre er status for IKT-området inkludert i grunnlaget for rammesak og handlings- og økonomiplan.

Rådmannen skal også etterspørre rapport fra personvernombudet to ganger per år. Rådmannen opplyser om at dette gjøres i hovedsak muntlig, men at personvernombudet også henvender seg skriftlig i enkeltsaker. Se også personvernombudets tilbakemelding angående rapportering i avsnitt 3.2.1.

3.1.3. Revisors vurdering av organisering

Styringsdokument for informasjonssikkerhet gir en god beskrivelse av roller, ansvar, myndighet og rapportering på overordnet nivå. I praksis er ikke informasjonssikkerhetsarbeidet organisert helt i samsvar med styringsdokumentet. Sikkerhetsgruppa inngår ikke styringsdokumentet, og vi kan ikke se at det er vedtatt mandat annet sted. Vi mener at sikkerhetsgruppas ansvar og rolle bør formaliseres.

Styringsdokumentet gir også klare forventninger for rapportering til rådmannen. Ifølge rådmannen, mottar han rapporter om informasjonssikkerhet, men rapporteringen følger ikke det mønster og systematikk som det legges opp til i styringsdokumentet for informasjonssikkerhet. Rapporteringen av informasjonssikkerhetsavvik og IKT-hendelser synes i stor grad å bli gjort løpende, og ikke systematisk. Iht. styringsdokumentet skal det fastsettes en årlig handlingsplan med tiltakene for å oppnå sikkerhetsmålene. Selv om rådmannen kan redegjøre for tiltakene, er planen ikke skriftliggjort i et dokument, vi mener at kommunen bør vurdere å skriftliggjøre handlingsplanen.

Når det gjelder ledelsens årlige gjennomgang av informasjonssikkerheten skal dette gjennomføres høsten 2021, men tilbakemeldingene fra kommunen tyder på at dette ikke har vært gjennomført i tidligere år.

3.2. Personvernombud

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

3.2.1. Stillingsbeskrivelse og rapportering

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.

Kommunen har utarbeidet en stillingsprofil (stillingsbeskrivelse) for personvernombudet. Kommunen har tatt utgangspunkt i Datatilsynets veileder for personvernombud, når de utarbeidet stillingsprofilen. Stillingsprofilen lister opp relevante ansvarsområder for personvernombudet. Følgende oppgaver er listet opp i kommunens stillingsprofil:

- *Informere og gi råd til rådmann og de ansatte som behandler informasjon i henhold til personopplysningsloven.*
- *Veilede personer som er registrert i kommunens informasjonssystemer med personopplysninger om deres rettigheter etter nye personvernregler.*
- *På anmodning gi råd om vurdering av personvernkonsekvenser.*
- *Kontrollere at kommunen overholder personvernreglene, kommunens egne retningslinjer, rutiner, internkontrollrutiner, holdningsskapende tiltak og opplæring av personell.*
- *Kontrollere gjennomføring av personvernkonsekvenser.*
- *Rapportere direkte til rådmann.*
- *Samarbeide med Datatilsynet.*
- *Personvernombudet skal kunne utføre andre oppgaver relatert til internkontroll og informasjonssikkerhet, såfremt vedkommende har eller får kompetanse som kreves.*

Det fremgår av personopplysningsloven 38-3 at personvernombudet skal være uavhengig, det vil si at hen ikke kan instrueres i utførelsen av oppgavene og at ikke kan avsettes eller straffes for utførelsen av oppgavene sine. Dette fremgår ikke av stillingsprofilen til Sandefjord. Det fremgår heller ikke av styringsdokumentet for informasjonssikkerhet, men det fremgår der at personvernombudet ikke skal ha ansvar for informasjonssikkerhet.

I styringsdokumentet for informasjonssikkerhet fremgår det at personvernombudet skal rapportere til rådmannen to ganger hvert år. Personvernombudet har opplyst om at han har rapportert til rådmannen én gang årlig tidligere, men det ble ikke rapportert i 2020 og 2021. Den tidligere rapporteringen inneholdt antall innsynsforespørsler, status for protokoll og sikkerhetsbrudd.

I de utvalgte enhetene og systemene fortalte de fleste om god kjennskap til personvernombudet og at de hadde vært i kontakt med ham. De to enhetene fremhevet begge at det ville være naturlig å ta kontakt, hvis de hadde spørsmål om personvern, og en enhet mente at det også var aktuelt å ta kontakt ved mistanke om data på avveie. De ansvarlige for de to systemene fortalte om en tettere kontakt med personvernombudet, enn hva de to enhetene hadde. Aktuelle samarbeidstemaer for dem var opplæring, protokoll og innføring av nye systemer.

3.2.2. Kompetanse og ressurser

Det fremgår av personopplysningsloven art. 37-5 at personvernombudet skal være faglig kvalifisert og ha dybdekunnskap på området som er tilstrekkelige for at hen kan utføre arbeidet. I stillingsprofilen for personvernombudet er det spesifisert hvilke kvalifikasjoner personvernombudet skal ha, dette inkluderer blant annet:

- innsikt og erfaring med kommunal drift
- gode kommunikasjonsevner
- dybdekunnskap om personvernregler, inkl. regler i særlov og om barns rettigheter
- IKT-kunnskap
- kunnskap om internkontroll og risiko og sårbarhetsvurderinger
- 3-årlig universitetsutdannelse
- utdanningsretning: samfunnsfag, juss, offentlig forvaltning og ledelse

Personvernombudet er utdannet sykepleier og har arbeidet som leder innenfor helse og omsorg i mange år, og dessuten har han arbeidet med internkontroll på fulltid i to år. Han har også videreutdanning i ledelse, organisasjonskultur og sikkerhetskultur fra høyskole. Personvernombudet ledet også arbeidet med overordnet styringsdokument for informasjonssikkerhet før han be oppnevnt til personvernombud. Han har vært ansatt som personvernombud siden 2018.

Personvernombudet hadde før Koronapandemien en delt stilling. 50 prosent av stillingen var avsatt til å være personvernombud og 50 prosent var avsatt til å være rådgiver og koordinator for samfunnssikkerhet og beredskap. Personvernombudet har fortalt at det har gått mye tid til å utarbeide protokoll over behandlingsaktivitetene. Dette har ført frem til utviklingen av iConfirm som i dag fungerer som kommunens protokoll. Programmet er utviklet i et samarbeid mellom IKT-tjenesten og selskapet iConfirm. Videre er det brukt mye tid på kompetanseheving blant ansatte og ledere. Personvernombudet har også arbeidet med sikkerhetsansvarlig og vurdert sikkerhetsbrudd og avvik. Personvernombudet mottar også henvendelser direkte fra innbyggere og ansatte, bla. om innsyn i registrerte personopplysninger. Personvernombudet opplyser at han er i tillegg til å

være rådgiver på personvernområdet, også ivaretar han den kontrollerende funksjonen som personvernombudet skal ha.

Når koronapandemien brøt ut, forteller personvernombudet at han måtte prioritere ned arbeidet som personvernombud og isteden bruke en større del av stillingen på samfunnssikkerhet og beredskap. Dette ble avklart med rådmannen. Personvernombudet har opplyst at han har allikevel prioritert viktige oppgaver ved behov som avvik/brudd på personvernregler og deltakelse i møter. På spørsmål om prosjekter har blitt nedprioritert som følge av omdisponeringen av stillingen, bekrefter han dette, men understreker at sikkerhetsgruppa også har tatt en større rolle under pandemien enn tidligere.

Høsten 2021 skal Sandefjord kommune endre organiseringen av personvernarbeidet. Nåværende personvernombud skal nå jobbe kun med samfunnssikkerhet og beredskap. Rollen som personvernombud blir flyttet til kommuneadvokaten, hvor det er tilsatt en advokat og en advokatfullmektig som skal dele på rollen som personvernombud. Disse to tiltrer henholdsvis desember og november 2021. Kommuneadvokaten har opplyst om at rollen som personvernombud skal deles mellom de to, med totalt 30 prosent stilling. Stillingsstørrelsen er fastsatt etter anslag av behov gjort av nåværende personvernombud, og det vil bli vurdert om rollen krever en større del av stillingene deres. Når stillingene hos kommuneadvokaten ble utlyst var GDPR/personvern omtalt som en del arbeidsoppgavene.

3.2.3. Revisors vurdering av personvernombud

Ansvarsområdene og rollen for personvernombudet er tydelig beskrevet i stillingsprofilen for personvernombudet og i tråd med veiledningen fra Datatilsynet. Personvernombudets uavhengighet er ikke omtalt i stillingsprofilen.[3] Dette fremgår heller ikke av det styringsdokumentet for informasjonssikkerhet, men her fremgår det at personvernombudet ikke skal ha ansvar for informasjonssikkerhet på noe nivå i organisasjonen. Dette mener vi er et tiltak som bidrar til å sikre personvernombudets uavhengighet, men vi mener likevel personvernombudet burde ha fremgå av stillingsprofilen. Videre bør stillingsprofilen oppdateres slik at den stemmer over ens med ny plassering i organisasjonen.

Personvernombudet har både videreutdanning og betydelig erfaring fra kommunaldrift, internkontroll og personvernarbeid. Etter vår mening oppfyller han derfor kompetansekravet i personopplysningsloven art. 37-5. Vi mener også at han oppfyller kravene til kompetanse i kommunens liste over kvalifikasjoner i stillingsprofilen.[4] Vi har ikke vært i kontakt med de nytilsatte som skal overta personvernrollen og har derfor heller ikke vurdert deres kompetanse.

Etter vår vurdering er ikke personvernombudets rapportering til rådmannen i samsvar med overordnet styringsdokument. Ifølge styringsdokumentet skal personvernombudet rapportere to

[3] Jf. personopplysningsloven art. 38-3.
[4] Vi har ikke vurdert personvernombudets personlige egenskaper og egnethet.

ganger i året. Personvernombudet har ikke rapportert til rådmannen i 2020 eller i 2021. Tidligere ble det rapportert én gang i året.

Personvernombudet har til nå vært en 50% stilling tillagt en ansatt med 50% stilling som beredskapskoordinator. Som et resultat av koronapandemien har personvernombudet blitt bedt om å nedprioritere tidsbruk til oppgaver som personvernombud og prioritere oppgavene innenfor sikkerhet og beredskap. Vi har forståelse for denne prioriteringen i den unntakssituasjonen som har vært, men dette har påvirket hvor mye tid personvernombudet har hatt til å arbeide med personvern. Etter ny organisering vil også stillingen til personvernombudet bli endret fra i utgangspunktet 50 prosent til 30 prosent fordelt på to personer, fordelt jevnt vil dette da utgjøre 15 prosent av hver av deres stilling og derfor utgjøre en mindre del av deres totale ansvarsområde. Vi mener at kommunen må sikre at personvernombudet har tilstrekkelig tid og ressurser til å utføre sine oppgaver.

Vi vil i tillegg kommentere at personopplysningsloven art. 37-1 presiserer at det skal være «et personvernombud». Jarbekk og Sommerfelt understreker at dette skal forstås bokstavelig; virksomheten kan ikke ha mer enn ett personvernombud.[5] Kommunen bør derfor sikre at én av de to nye som skal arbeide med personvern har den formelle rollen som personvernombud.

3.3. Protokoll over behandlingsaktiviteter

Sandefjord kommune skal ha protokoll over hvilke personopplysninger kommunen behandler.

3.3.1. Rutiner og opplæring

Rutinen Prosess for anskaffelse av nye systemer fastsetter at protokollen skal utfylles for et nytt system etter det er utarbeidet ROS-analyse, men før databehandleravtale og kontrakt inngås med leverandør. Det er systemansvarlig som har ansvaret for å legge inn informasjon i protokollen og oppdatere denne ved behov.

Kommunen benytter programmet iConfirm for fylle ut og håndtere protokollen. Administrasjonen har gjennomført opplæring i iConfirm. Det er opprettet en egen Teamsgruppe for systemansvarlige, hvor spørsmål blir besvart av sikkerhetsgruppen. Det er også planlagt et webinar med alle systemansvarlige i januar 2022 hvor man skal gjennomgå alle protokoller. IKT-leder fremhever også at utfylling av protokollen sjekkes nøye av sikkerhetsgruppa ved godkjenning av nye systemer.

[5] Jarbekk og Sommerfeldt, *Personvern og GDPR i praksis*, s. 171.

Styringsdokument for informasjonssikkerhet omtaler ikke iConfirm da dokumentet ble utformet før iConfirm ble tatt i bruk i 2019.[6]

3.3.2. Program for protokoll – iConfirm

iConfirm har én side per program med forskjellige felter som systemansvarlig fyller ut. Alle feltene har veiledningstekst som skal hjelpe systemansvarlig i utfyllingen, og det vises også til relevante hjemler i personopplysningsloven.

Administrasjonen opplyser at de er i ferd med å innføre en ny funksjon i iConfirm hvor risikoen knyttet til systemet bestemmer hvor mye informasjon som skal fylles ut i protokollen. Hvert system blir da risikoklassifisert etter hvilke opplysninger som systemet behandler. Denne klassifiseringen avgjør deretter hvilke felt som skal fylles ut for hvert system i iConfirm, og skal bidra til å gjøre arbeidet med utfyllingen av protokollen enklere. Systemene blir klassifisert i følgende kategorier: kritisk, høy, middels og lav. I iConfirm er det en veiledningstekst med kriterier for å klassifisere de forskjellige kategoriene, men det blir også vektlagt at dette er en subjektiv vurdering som hver enkelt virksomhet selv må gjøre og sette manuelt. IKT-leder har bekreftet at veiledningsteksten i iConfirm følges ved klassifiseringen av systemene.

I listen over systemer fremgår det også i hvilken grad feltene for hvert system er utfylt.

Opplysninger i iConfirm

I personopplysningslovens artikkel 30 fremgår det hvilken informasjon protokollen skal inneholde. Datatilsynet har også utarbeidet en mal til hvordan protokollen kan utformes, denne viser både hvilken informasjon som er obligatorisk å ha i protokollen og hvilken informasjon Datatilsynet anbefaler å ha i protokollen.[7] Protokollen skal blant annet vise formålet med behandlingene, hvilke kategorier personopplysninger som kommunen behandler, og, hvis det er mulig, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak.

Vi har gjort en gjennomgang av iConfirm og sammenlignet med Datatilsynets mal. Vår gjennomgang viser at iConfirm har felter for å fylle inn all den informasjonen som Datatilsynets mal foreslår, både obligatoriske og valgfrie.

Vi har også undersøkt feltene som skal fylles ut i iConfirm når man aktiverer funksjonen som justerer hvilken informasjon som skal fylles ut etter definert risiko (se beskrivelse over). Vi har sett på risikoklassene kritisk og lav. For begge disse risikoklassene skjules en god del felter når funksjonen aktiveres. Selv om de ikke er identiske, er forskjellen liten, på hvilke felt som skjules,

[6] iConfirm har vært under utvikling sammen med leverandør siden 2017. Kommunen begynte å legge inn data i 2019/2020, men IKT-leder opplyser at ble satt på ordentlig satt på dagsorden i 2021 hvor det er gjennomført opplæring og webinar.

[7] Malen er tilgjengelig her: https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/forordningen/artikkel-30_protokoll-behandlingsansvarlig.xlsx

mellom kritisk og lav. Det er noen felter som blir skjult for begge risikoklassene som enten er anbefalt eller obligatoriske i Datatilsynets mal. Dette gjelder følgende felter:

- Obligatorisk:
  - Kategorier av mottakere (jf. personopplysingsloven art. 30-1 d)
  - Navn på tredjeland eller internasjonale organisasjoner som personopplysningene overføres til (jf. personopplysningsloven art. 30-1 e)
- Anbefalt:
  - Funksjonsområde (hvilken del av kommuneorganisasjonen bruker systemet).
  - Kilde for personopplysningene.

I iConfirm kan man også ta ut protokollen som en rapport, denne tilsvarer i all hovedsak Datatilsynets mal. Alle obligatoriske felt blir fylt ut automatisk med data fra iConfirm. Det er også noen felter som skal fylles ut manuelt i rapporten fra iConfirm, men disse er ikke obligatoriske i Datatilsynets mal. Man kan velge om man vil ta ut protokollen basert på systemer eller prosesser. I Sandefjords tilfelle synes det at bruken av prosesser er fortsatt under utvikling da alle prosesser er markert med utkast.

3.3.3. Registeringer i protokollen

Vi har sjekket informasjon registrert i protokollen for et utvalg på 10 programmer (for informasjon om utvalget se vedlegg 3). Vi har sett på følgende programmer:

- Dips Communicator
- Visma samhandling arkiv
- ACOS Mottak
- Fri5 - Sandefjord kommune Booking program
- Kommunikasjon - Kommunekari
- Arrangementer - kursportal
- IKOS Elektronisk tavle
- Campus Increment
- Gemini Arena
- BliksundWeb & Prehospital Elektronisk Pasientjournal

Vi har sjekket om følgende informasjon er oppgitt i protokollen:

- formål med behandlingen av personopplysninger (jf. personopplysningsloven art. 30-1-b),
- kategorier av registrerte (dvs. hvem er det personopplysninger om, jf. personopplysningsloven art. 30-1-c) og
- kategoriene av personopplysninger (dvs. hvilke personopplysninger er registrert, jf. personopplysningsloven art 30-1-c).

Vi har også undersøkt om behandlingsgrunnlag er oppgitt. Det er ikke et krav å ha dette i protokollen, men det er anbefalt i Datatilsynets mal for protokoll. Det er også et krav at kommunen

må ha et gyldig behandlingsgrunnlag for å kunne behandle personopplysninger (jf. personopplysningsloven art. 6-1).[8] Merk at bruk av hjemmelsgrunnlagene i artikkel 6-1-c eller 6-1-e krever også hjemmel i en annen lov for å brukes.

Syv av systemene hadde oppgitt hva som var formålet med behandlingen av personopplysninger i systemet. For de tre andre systemene var det gitt en kort tjenestebeskrivelse. Disse tjenestebeskrivelsene sa noe om formålet med systemet, men bar ellers preg av å være generelle beskrivelser fra leverandøren.

Protokollen inneholdt informasjon om kategorier av registrerte og om kategoriene av personopplysninger for seks av systemene. Protokollen manglet denne informasjon om de fire andre systemene.

Protokollen inneholdt informasjon om behandlingsgrunnlag for å behandle personopplysninger for syv av systemene. Følgende hjemler er oppgitt i protokollen:

Tabell 1 Oppgitt behandlingshjemmel for systemer i stikkprøve

System	Hjemmel	Beskrivelse hjemmel og tilleggshjemmel
Dips Communicator	6-1-c	Rettslig forpliktelse, jf. sivilbeskyttelsesloven §§ 14 og 15
Visma samhandling arkiv	6-1-c	Rettslig forpliktelse, jf. riksarkivarens forskrift §§ 7-28 (9), 7-29 (2), § 7-30 (2), Barnevernsloven § 1-4, Lov om arkiv § 6,
ACOS Mottak	Mangler hjemmel	
Fri5 - Sandefjord kommune Booking program	6-1-e	Allmenhetens interesse, jf. vedtak kommunestyret
Kommunikasjon - Kommunekari	6-1-a/ 6-1-e	Samtykke, allmenhetens interesse (hjemmel ikke oppgitt).
Arrangementer - kursportal	Mangler hjemmel	
IKOS Elektronisk tavle	6-1-b	Avtale
Campus Increment	Mangler hjemmel	

[8] Undersøkelsen ble gjort den 15.10.21 og 16.10.21.

System	Hjemmel	Beskrivelse hjemmel og tilleggshjemmel
Gemini Arena	6-1-e	Allmenhetens interesse, jf. plan og bygningsloven § 1-4
BliksundWeb & Prehospital Elektronisk Pasientjournal	6-1-b/ 6-1-c	Avtale, rettslig forpliktelse, jf. rett til helsehjelp og dokumentere ytelse av helsehjelp og oppfølgning

De to utvalgte systemene (casestudie) er registrert i iConfirm, men det er et pågående arbeid med å ferdigstille informasjonen i protokollen. Når det gjelder SmartVakt Felt er det ikke avklart hvilket behandlingsgrunnlag som skal benyttes for trygghetsalarmene. I intervjuet viste de ansvarlige for systemet til at dette var et komplekst spørsmål, og at man arbeidet med for å finne rett grunnlag. Videre opplyste de om at det ble innhentet samtykke fra bruker når kommunen tok i bruk trygghetsalarmene. Etter avklaring med personvernombudet gikk man bort fra dette, med begrunnelsen at når bruker har samtykket til å ta i bruk trygghetsalarm (ved at hen søker på tjenesten) er det ikke behov for et ekstra samtykke.

3.3.4. Revisors vurdering – protokoll

Kommunen har med iConfirm et program som gir god oversikt over protokollen, og gjør det mulig å registrere opplysninger i protokollen i samsvar med personopplysningslovens art. 30-1.

Stikkprøvene våre viste at et for et flertall av systemene vi sjekket, var opplysningene vi kontrollerte registrert i protokollen. Men undersøkelsen viste også at det gjenstår en del arbeid med å registrere informasjonen og med å sikre at denne er av tilstrekkelig kvalitet.

Kommunen må ha et behandlingsgrunnlag (hjemmel) etter personopplysningsloven artikkel 6-1 for å kunne behandle personopplysninger. Derfor er det viktig at det er tydelig hvilken hjemmel kommunen bruker og at denne er korrekt. For tre av systemene i stikkprøven vurderer vi det som usikkert om hjemmelen som er brukt, er korrekt eller om den er tilstrekkelig hjemlet i annet lovverk. Dette gjelder følgende systemer:

- For Fri5 er art. 6-1-e (allmennhetens interesse) valgt som hjemmel. Ved bruk av dette grunnlaget skal det vises til lovhjemmel, men det er kun oppgitt «vedtak kst [kommunestyre]». Vi mener at dette ikke er tilstrekkelig grunnlag.
- For Kommune-Kari er art. 6-1-a (samtykke) valgt som hjemmel. Dette er en tjeneste tilgjengelig på kommunens hjemmeside og vi kan ikke se at det blir bedt om samtykke. I tillegg er art. 6-1-e (allmennhetens interesse) valgt som hjemmel, uten at lovhjemmel er valgt.
- For BliksundWeb & Prehospital Elektronisk Pasientjournal er art. 6-1-c (rettslig forpliktelse) valgt som hjemmel. Forpliktelsen er beskrevet, men den er ikke hjemlet konkret i lov eller

forskrift, noe som er påkrevd. Det også valgt hjemmel art. 6-1-b (avtale) uten at det er klart hvilken avtale dette er eller hvordan den inngås den registrerte.

Når det gjelder Smart Vakt Felt og hjemmel for trygghetsalarmene mener vi at det burde vært avklart hvilen hjemmel som var korrekt, før man gikk bort fra å innhente samtykke.

Protokollen er et viktig verktøy for å oppfylle kravene i personopplysningsloven, og det er derfor viktig at protokollen inneholder den informasjonen om kommunens systemer som er påkrevd i lovverket og forutsatt i iConfirm.

Vi mener at overordnet styringsdokument bør oppdateres slik at det fremgår at kommunen bruker iConfirm som protokoll.

3.4. Risikovurderinger og vurderinger av personvernkonsekvenser

Sandefjord kommune skal ha risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA).

3.4.1. Overordnede risikovurderinger

Kommunen har gjennomført en overordnet ROS-analyse for IKT-systemet sitt. Denne ble utarbeidet i 2020 og er oppdatert i mai 2021. Det er beskrevet uønskede hendelser som det er vurdert risiko for, tiltak for å redusere risikoen og forventet risiko etter tiltak er utført. Det er også angitt status for gjennomføringsgraden til hvert tiltak.

Vi har også mottatt ROS-analyse for krypteringsvirus[9] etter samme mal fra 2021. Det er imidlertid ikke beskrevet like tydelig og detaljert hva status er for gjennomføringen av tiltakene som i den overordnede ROS-analysen.

Det er også gjennomført en ROS-analyse for Office 365. Her er det gjennomført en overordnet analyse for hele systemet, for hver av enkeltkomponentene i Office 365 og for behandlingen av personopplysninger. Den overordnede analysen fokuserer på risikoer for konfidensialitet, integritet og tilgjengelighet, og status for tiltakene er angitt. De øvrige ROS-analysene fokuserer blant annet på risikoer for konfidensialitet, integritet og tilgjengelighet, og i de fleste av disse ROS-analysene er status på tiltakene beskrevet.

3.4.2. Risikovurderinger for systemer

Rutine for risikovurderinger

I henhold til rutinen for anskaffelse av nytt system (se vedlegg 4) skal det gjennomføres en ROS-analyse for anskaffelsen av systemet. Dette inkluderer vurdering av personvern. ROS-analysen skal gjennomføres av systemeier, så snart sikkerhetsgruppen har godkjent behovsvurderingen. I

[9] Krypteringsvirus eller kryptovirus gjør filene på det infiserte systemet utilgjengelige ved å kryptere dem, det blir ofte framsatt et løsepengekrav.

tillegg fremgår det av styringsdokument for informasjonssikkerhet at risikovurdering også skal gjennomføres ved vesentlige endringer og minimum hvert andre år.

ROS-analysen utføres med et eget verktøy som heter Compilo KSX. Verktøyet deler ROS-analysen opp i flere steg som brukeren blir ledet igjennom. Disse er:

- Deltakere – her inviteres de som skal delta i prosessen.
- Risiko-objekt – her legges inn de risikoobjekter eller typer risikoer som skal vurderes.
- Risikoidentifisering – her legges inn mulige uønskede hendelser eller risikofaktorer. Her kan også eksisterende tiltak legges inn.
- Risikoanalyse – her vil hver deltaker i prosessen vurdere sannsynlighet og konsekvens. I dette steget blir risiko som er over den definerte tiltaksgrensen identifisert.
- Risikoevaluering – her vurderes nye tiltak for å redusere sannsynlighet og/eller konsekvens.
- Risikohåndtering – her bestemmes forutsetningene og regimet for å sikre akseptabel risiko.
- Rapporter – her kan nødvendig dokumentasjon av ROS-analysene hentes ut.

Kommunen har et støttedokument som tar for seg noen risikoområder, med mulige risikoer og årsaker. Et av områdene er Personvern/GDPR. Listen over mulige risikoområder er kortere for dette temaet enn for andre tema og det er ikke lagt inn mulige årsaker.

Styringsdokumentet for informasjonssikkerhet har en normerende beskrivelse av konsekvens og sannsynlighet. Denne hjelper den som utfører ROS-analysen å velge riktig nivå for konsekvens og sannsynlighet for en uønsket hendelse. Det er også utformet en risikomatrise som viser risikonivå basert på sannsynlighet og konsekvens en uønsket hendelse.

Det er også bestemt hvem som har myndighet for å akseptere et visst risikonivå og hvilke forutsetninger som må være til stede for at risikonivået kan aksepteres.

Gjennomføring av risikovurderinger

Vi har tatt stikkprøver av risikovurderinger. Vi brukte de samme systemene som ved kontrollen av protokollen (se avsnitt 3.3.3 og vedlegg 3). Vi ba kommunen oversende de to siste gjennomførte risikovurderingene.

Totalt sett fikk vi tilsendt risikovurderinger for halvparten av systemene.[10] Der vi mottok risikovurderinger var samtlige datert etter vi hadde sendt forespørselen til kommunen. Ingen kunne fremlegge den foregående risikovurderingen. Vi mottok risikovurderinger for to av tre utvalgte systemer som var kategorisert som kritiske i iConfirm.

[10] For et av systemene mottok vi en ROS for avdelingens samlede IKT systemer fra 2018, men ikke det forespurte systemet.

Vi stilte spørsmål til de utvalgte enhetene og systemene om de hadde gjennomført eller deltatt i risikovurderinger. De ansvarlige for Visma Flyt Skole opplyste at det skal gjennomføres ROS-analyse for systemet. En teknisk ROS, som fokuserer på det tekniske aspektene av systemet, må gjennomføres i samarbeid med leverandøren. Det er også planer om å gjennomføre en «human» ROS-analyse (fokusert på bruken av systemet).

På skolen opplyste én av deltakerne at de hadde deltatt i et større ROS-prosjekt som var felles for kommunen og som omfattet skolen. Men det var ikke gjennomført risikovurderinger utover dette.

De ansvarlige for SmartVakt Felt viste til at det er en pågående prosess i kommunen med gjennomføring av ROS-analyser for flere systemer, heriblant SmartVakt Felt. Videre opplyste de at hjemmetjenesten og ansatte som bruker SmartVakt Felt, ikke er involvert i risikovurderingen, men at de kunne spørres eller involveres ved behov.

Deltakerne på intervjuet med hjemmesykepleieenheten fortalte at det ikke var gjennomført noen risikovurdering i enheten, men at det var det var bevissthet rundt temaet i enheten.

3.4.3. Vurdering av personvernkonsekvenser (DPIA)

Rutine for DPIA

Kommunen har en rutine for vurdering av personvernkonsekvenser (DPIA) i styringsdokumentet for informasjonssikkerhet. Rutinen beskriver hvilke tilfeller DPIA skal gjennomføres. I rutinen står det at DPIA skal gjennomføres i tilfeller med høy eller svært høy risiko, det er ikke presisert hvilken risiko dette gjelder. I personopplysningsloven artikkel 35-1 står det at DPIA skal gjennomføres når det er «høy risiko for fysiske personers rettigheter og friheter».

Videre vises det i rutinen til personopplysningslovens artikkel 35-3 hvor loven gir noen tilfeller hvor det skal er særlig nødvendig å gjennomføre DPIA. Det vises imidlertid ikke til listen som Datatilsynet har utarbeidet med tilfeller hvor det er påkrevd å gjennomføre en DPIA, denne listen er utarbeidet med hjemmel i artikkel 35-4.

I kommunens rutine vises det også til unntaket for å gjennomføre DPIA i artikkel 35-10. Her bør man merke seg at justisdepartementet i stortingsproposisjonen til personopplysningsloven, skriver at dette er en snever unntaksregel. Dette blir ikke fremhevet i kommunens rutine. Jarbekk og Sommerfeldt skriver om denne unntakshjemmelen at:

> *Det er interessant å merke seg at forordningen kun sier at det er unntak fra plikten til å gjøre DPIA dersom forarbeidene til loven eller i opprettelsen av myndigheten selv er gjort vurderinger som tilsvarende en DPIA. I realiteten er det nok sjelden tilfelle i Norge.*[11]

[11] Eva Jarbekk og Simen Sommerfeldt, *Personvern og GDPR i praksis*, s. 142

Kommunens rutine gir ikke noen beskrivelse av hvordan DPIA skal gjennomføres. Det vises ikke til skjemaet som kommunen har benyttet til den DPIAen de har gjennomført så langt, eller til hvordan kommunens ledelse skal involveres i prosessen.

Gjennomført DPIA
Vi har fått opplyst at administrasjonen har gjennomført én DPIA. Denne ble gjennomført for prosjektet Trygg Hjemme som er et forebyggingsprosjekt som brann og redning har gjennomført i samarbeid med helse, sosial og omsorg. Administrasjonen har opplyst at det i arbeidet med denne, ble benyttet et hjelpeskjema fra et prosjektsamarbeid med andre kommuner, samt veiledningen fra Datatilsynet.

For Trygg Hjemme prosjektet er DIPA-skjemaet utfylt, men de registrerte er ikke blitt involvert i prosessen (jf. personopplysningsloven art. 35-9) og det fremgår ikke om kommuneledelsen har gjennomgått DPIA før behandlingen startet. Vi har fått opplyst fra de som gjennomførte DPIAen at de registrerte, heller ikke har blitt involvert på et senere tidspunkt. Kommunens ledelse har ikke vært involvert, men leder for forebyggende var involvert i sluttfasen sammen med personvernombudet.

Vi har fått opplyst at DPIAen ble fulgt opp av Trygg Hjemme-gruppa, hvor man blant annet gjorde noen endringer i rutiner og tok i bruk fagsystemet CosDoc ID.

Vi har også spurt personvernombudet om kommunens praksis med DPIAer. Personvernombudet mener at kommunen kan bli bedre på å gjennomføre DPIAer, særlig sett i lys av at kommunen behandler store menger personopplysninger. Personvernombudet mener at antallet gjennomførte DPIAer må ses i sammenheng med at mange av kommunens store systemer har vært i bruk før den nåværende personopplysningsloven trådte i kraft, og DPIA er et verktøy som skal brukes i forkant av at systemet tas i bruk. Personvernombudet mener at risikovurdering må gjøres før man tar i bruk nye systemer og DPIA skal gjennomføres hvis risikovurderingen viser at det behov for dette eller dersom Datatilsynets veileder sier at det skal gjøres. Personvernombudet har sendt ut informasjon om dette, men han er ikke sikker på om dette blir fulgt opp. Et konkret eksempel er kameraovervåkning på offentlig sted. Her har personvernombudet varslet at det er behov for å vurdere DPIA, men han er usikker på om dette er gjort.

Vi fikk opplyst at det var usikkert om DPIA var gjennomført for SmartVakt Felt og det var ikke gjennomført DPIA for Visma Flyt Skole.

3.4.4. Revisors vurdering av risikovurderinger og DPIA

Risikovurderinger
Sandefjord kommune har rutiner for gjennomføring av ROS-analyser, veiledning for vurdering av risikoer knyttet til informasjonssikkerhet og verktøy for gjennomføringen av ROS-analyser.

Vi mener at kommunen ikke etterlever rutinene for gjennomføring av ROS-analyser i tilstrekkelig grad. Våre undersøkelser viser at kommunen ikke kunne fremlegge risikovurderinger for

halvparten av de utvalgte systemene. For den andre halvparten fremla kommunen risikovurderinger som var datert etter at vi ba kommunen om å fremlegge disse. Kommunen kunne heller ikke fremlegge den nest siste risikovurderingen for noen av de utvalgte systemene. Dette er ikke i samsvar med personopplysningslovens art. 24 og heller i samsvar med kommunes egne retningslinjer.

DPIA
Kommunen har en rutine for når det skal gjennomføres DPIA. Vi mener at kommunen bør oppdatere rutinen slik at det vises til Datatilsynets oversikt over behandlinger som krever at det gjennomføres DPIA, jf. personopplysningslovens art. 35-4. Rutinen mangler også en beskrivelse av hvordan DPIA skal gjennomføres, videre mangler det henvisning til skjemaet kommunen bruker og det fremgår heller ikke hvordan kommuneledelsen skal involveres i prosessen.

Etter det vi har fått opplyst, har kommunen kun gjennomført én DPIA. Kommunen behandler mye sensitive personopplysninger og bør vurdere behovet for å gjennomføre flere DPIAer. Et eksempel på dette er igangsetting av overvåkning på offentlig sted. Det er korrekt, som personvernombudet påpeker, at det ikke er nødvendig med DPIA for systemer som var tatt i bruk før gjeldende lovverk trådte i kraft, forutsatt at behandlingen enten var kontrollert av Datatilsynet eller personvernombudet før lovendringen. Vi mener imidlertid at det er grunn til å påpeke at dette gjelder kun til behandlingen blir endret og det er sannsynlig at denne endringen medfører at behandlingen utgjør en høy risiko for de behandledes rettigheter og friheter. Dette kan følge av at man tar i bruk ny teknologi i behandlingen, at man bruker dataene fra behandlingen på en ny måte, eller at andre sosiale sammenhenger har ført til økt risiko (eks. at en gruppe med behandlede blir sårbare for forskjellsbehandling).

Når det gjelder den ene DPIAen som er gjennomført, mener vi at de behandlede eller deres representanter skulle ha vært involvert i prosessen. I vurderingen av de registrertes rettigheter, er det ikke vurdert om det er forhold (f.eks nedsatte kognitive evner) som kan påvirke de registrertes evne til å gi et samtykke som oppfyller kravene til samtykke i personopplysningslovens art. 7. Det er heller ikke dokumentert om personvernombudet er blitt involvert i prosessen og eller om kommuneledelsen har vurdert DPIAen.

3.5. Tekniske og organisatoriske tiltak

Sandefjord kommune skal ha tekniske og organisatoriske tiltak for å sikre personopplysningene.

Dette avsnittet vil ta for seg noen tekniske og organisatoriske tiltak som Sandefjord kommune har for å sikre personopplysningene de behandler. Avsnittet vil først omhandle felles tiltak i hele kommunen, deretter vil vi gå nærmere inn på de to enhetene og to systemene som vi har valgt ut i prosjektet.

3.5.1. Felles tekniske og organisatoriske tiltak

Rutiner for bruk av kommunens IKT-systemer
Vi har mottatt en samling rutiner som gir generelle retningslinjer for ansatte om bruk av kommunes IKT-systemer, disse skal bidra til sikker bruk av systemene. Rutinene gjelder blant annet bruk av nettverk, e-post, sosiale medier, brukernavn og passord, administratorrettigheter m.m. Rutinene har en lik oppbygning og er kortfattede.

Ifølge rutinene har informasjonssikkerhetskoordinator IKT ansvar for rutinen og rutinen skal revideres hvert år. IKT-leder har opplyst om at det ikke er noe system for å ivareta revidering av rutinene. Han opplyser også at noen av rutinene er publisert på kommunens intranett Innsiden. Sikkerhetsansvarlig opplyser at rutinene ikke er publisert i kvalitetssystemet Compilo.

Databrukeravtale
Vi har mottatt datadisipinerklæring (databrukeravtale) med tilhørende rutine. Denne er til revidering hos sikkerhetskulturgruppa. Av den tilhørende rutinen fremgår det at erklæringen skal gjøres kjent for og signeres av alle ansatte i kommunen. IKT-leder opplyser at det arbeides med å få integrert erklæringen i arbeidsavtalen til nyansatte, samt at man vurderer hvordan man kan rulle avtalen ut til eksisterende ansatte. Erklæringen vil bli fremlagt for godkjenning i rådmannens ledergruppe før utrulling.

Passord
Kommunen har to retningslinjer for passordbruk, en for ansatte og en for elever. I retningslinjen for ansatte er det informasjon om brukernavn, minstekrav til passord og hvordan passord skal håndteres. Sikkerhetsansvarlig har bekreftet at rutinen er publisert på intranettet, men ikke i Compilo. I rutinen for passord for elever er det beskrevet minstekrav til passord og hvordan passord kan endres (lærer kan endre passord i elevportalen). Det er også presisert at hvis lærer setter passordet, skal hver elev ha et individuelt passord.

Intervjuobjektene for Visma Flyt Skole fortalte at i etterkant av mediesaken om like passord blant elever,[12] var det gjort tiltak. De har informert om at dette er en uønsket praksis og de har vært i kontakt med leverandøren for elevportalen, hvor lærerne kan sette passord. Det er gjort en endring som fjerner valget der man kan sette likt passord for hele klassen. Hvis læreren skal få til å gjøre det nå, må hen sette passordet manuelt for hver enkelt elev.

Ved den utvalgte skolen var de opptatte av at alle elever skulle ha individuelle passord og at dette ble fulgt opp. Det er imidlertid tilfeller hvor alle elever blir tildelt et passord fra skolen eller lærer, eks. når det deles ut nye datamaskiner til elever i 5. trinn. Det er da obligatorisk for elevene å bytte passordet i etterkant (dette kan settes som et krav i systemet).

[12] NRK, *Alle elevene bruker samme passord: - Jeg ble rett og slett sjokkert,* nettside, 23.08.21, https://www.nrk.no/vestfoldogtelemark/1.15612577

I hjemmesykepleieavdelingen er det et krav at passord skal endres jevnlig, både for pålogging på datamaskiner og systemer.

Opplæring
Det fremgår av styringsdokument for informasjonssikkerhet at kommunen «skal sikre tilstrekkelig kompetanse til alle som behandler informasjon generelt og personopplysninger spesielt. Kompetanse om prinsipper for behandling av personopplysninger prioriteres.»

Rådmannen har opplyst om at det er gjennomført kampanjer om viktigheten av informasjonssikkerhet, rettet både mot ledere og ansatte. Dette har vært sendt ut av rådmannen selv. I intervju med personvernombudet opplyste han også om at han har arbeidet med å øke kunnskap om personvernreglene både blant ledere og ansatte. Personvernombudet har også besøkt forskjellige prosjekter og avdelinger i dette arbeidet. Han viser også til at nanolæring (korte nettkurs) har vært brukt i kommunen for å spre kunnskap om informasjonssikkerhet blant ansatte.

I intervju de to utvalgte enhetene bekreftet begge, at de har fått tilbud om opplæring. I hjemmesykepleieenheten har både leder og ansatte fått tilbud om kurs om informasjonssikkerhet fra IKT-avdelingen, bla. om phishing.[13] Det ble også fremhevet at IKT-avdelingen har delt informasjon på Teams.

På skolen hadde også både ledere og ansatte fått opplæring i sikkerhet og personvern med nanolæring. Ledelsen hadde fått ekstra kurs og hatt møter med personvernombudet. Temaet har også blitt løftet og diskutert internt på skolen. Intervjudeltakerne på skolen fremhevet også at IKT-avdelingen er til stor hjelp for å sikre kompetanse på området og at dette oppleves som veldig trygt. Skolen har en egen kontaktperson på IKT og kontakten oppleves som veldig god.

Intervjudeltakerne for SmartVakt felt bekreftet at kommunen har tilbud om e-kurs til ansatte og ledere.[14]

Et annet bevistgjøringstiltak som IKT-avdelingen har gjennomført, er en phishing kampanje. Her ble det sendt ut en falsk melding fra rådmannen med vedlegg om julebord. Denne kampanjen ble nevnt i flere av de utvalgte enhetene og systemene.

Andre tiltak
Som organisatoriske tiltak kan også regnes organisering og rapportering (se avsnitt 3.1) og håndtering av avvik (se avsnitt 3.6).

[13] Phishing er at noen prøver å få penger, tilgang til persondata eller annen informasjon, eks. ved å sende e-post og utgi seg for å være noen annen.
[14] Grunnet tidsbegrensning fikk vi ikke spurt intervjudeltakerne for Visma Flyt Skole om opplæring.

3.5.2. Utvalgte enheter og systemer

Vi vil her beskrive våre observasjoner fra de utvalgte enhetene og systemene som vi har sett nærmere på.

Visma Flyt Skole

Om systemet

Visma Flyt Skole benyttes for administrasjon av elever og er hovedverktøyet for lærerne til dette formålet. Systemet behandler personopplysninger om elever. Arkivfunksjonen er i det digitale arkivet WebSak som er integrert med Visma Flyt. Visma Flyt blir også brukt i kommunikasjon mellom skole og foresatte via nettportalen Visma Foresatt.

Organisering

I Sandefjord kommune er det IKT-avdelingen som håndterer skolens IKT-systemer og det er ikke egne IKT-folk på den enkelte skole. Systemansvarlig for Visma Flyt Skole er skolefaglig rådgiver. Det gjennomføres ukentlige møter mellom systemeier, systemansvarlig og IKT-avdelingen i kommunen.

Behandling av personopplysninger i systemet

Intervjudeltakerne mente at Visma Flyt Skole og WebSak ivaretok alle behov i det daglige arbeidet. Slik sett er det ikke behov for å oppbevare personopplysninger på papir. Av hensyn til personvernet blir ansatte oppfordret til å ikke ha papirkopier.

Lærere har ikke tilgang til arkivet WebSak, hvor det lagres dokumenter om elever som ikke er tilgjengelig i Visma Flyt Skole. Intervjudeltakerne mener allikevel at dette ikke gjør det nødvendig med papirarkiv. Enkeltvedtak kan for eksempel skrives i Visma Flyt før de arkiveres i WebSak, da vil lærerne også kunne se disse Visma Flyt.

På punktet om papirarkiv vil vi også vise til våre observasjoner fra den utvalgte skolen, se beskrivelse under.

Systemet er i utgangspunktet ikke designet sensitive personopplysninger. Det kan imidlertid forekomme at sensitive personopplysninger blir lagret i systemet, dette kan være om helseforhold (som allergi) eller religion (eks. i kommunikasjon med hjemmet om permisjon). Slike opplysninger kan bare legges inne i fritekstfelt, og det er kun skoleadministratorer som kan skrive i disse fritekstfeltene. I tillegg blir både lærere og andre brukere sterkt oppfordret til å ikke bruke i Visma Flyt til sensitive personopplysninger. Foresatte får også beskjed i nettportalen om å ikke sende sensitive opplysninger i Visma Flyt. Foresatte oppfordres til å ta kontakt på telefon eller møte på skolen hvis de trenger å diskutere sensitive personopplysninger.

Tilgangsstyring

Tilganger i systemet styres ut fra rolle: rektor, lærer, sekretær osv. Det er administratorer både på kommunenivå og skolenivå. Den enkelte skole kan ikke bestemme tilgangsnivå, dette blir bestemt felles for alle i kommunen.

Foresatte har tilgang til nettportalen Visma Foresatt hvor de kan se informasjon om sine barn. Kommunen og skolene har rutiner i tilfeller hvor foresatte ikke skal ha tilgang og forholder seg til juridiske beslutninger om dette. Skolene skal sjekke etter hver oppdatering fra folkeregisteret (gjøres hver tredje måned) at elever som ikke skal ha sine opplysninger (bla. tilknytning til foreldre) oppdatert mot folkeregistret, ikke blir det. Barn på skjermet adresse (kategori 6) legges inn med fiktivt navn og uten personnummer. I nettportalen bekrefter også foresatte at opplysningene om dem er riktig ved jevne mellomrom. Dette gjelder også hvem av foreldrene som skal se opplysninger om barnet.

Logging av bruk
Bruken av Visma Flyt logges, og det finnes både en logg på kommunenivå og en på skolenivå (som er mindre detaljert). Loggen gjennomgås i hovedsak når det er et behov eller ved en hendelse.

Beredskapsplaner
Det er ikke utarbeidet noe beredskapsplan ved nedetid. Oppetiden til systemet er godt over 99 prosent og vurderingen er at ved nedetid vil man bruke manuelle prosesser og at disse kan ajourføres i Visma Flyt i ettertid.

En skole

Systemer som behandler personopplysninger
Det viktigste systemet som skolen behandler personopplysninger om elever er Visma Flyt Skole. Dette er arbeidsverktøyet til lærerne, her skrives blant annet halvårsvurderinger, vedtak og aktivitetsplaner. WebSak er skolens digitale arkiv, men her har kun skolens administrasjon tilgang. Skolen har også noen andre systemer som behandler opplysninger om elever til mer spesifikke formål. Skolen behandler kun opplysninger om elever i godkjente systemer.

Generelt er alle programmer som skolen benytter basert på kommunale avtaler, dette gjelder også program som benyttes i undervisningen. Skolens ansatte har ikke anledning til å legge til eller fjerne programmer fra de kommunale PCene eller nettbrett. Bruken av Teams under koronapandemien ble diskutert på skolen, særlig bruk av kamera og lyd. Eksempelvis problemstillinger rundt hva som avsløres om elevens hjemmesituasjon.

Behandling av personopplysninger
Når ansatte jobber med dokumenter lokalt på sin PC, skal disse være anonymisert. Dette er aktuelt ved utarbeidelse av individuelle opplæringsplaner. Etter at de er utarbeidet blir de sendt til sentralt arkiv for skanning. Det er imidlertid planer for at også disse kan skrives i Visma Flyt.

Skolen har et papirarkiv som alle lærere har tilgang til. Arkivet inneholder dokumenter fra WebSak som ikke er tilgjengelige i Visma Flyt. Arkivet inneholder dokumenter fra: PP-tjenesten, BUPA og barnevern. Følgelig inneholder dokumentene ofte sensitive opplysninger. Arkivskapet er låst med en nøkkel som henger lett tilgjengelig i et nøkkelskap ved siden av arkivet. Arkivskapet står inne på et kontor, som er låst utenfor kontortid, men åpent innenfor kontortid også når vedkommende

som sitter på kontoret, er fraværende. Dokumentene skal ikke forlate skolen og de skal leveres inn ved arbeidsdagens slutt. Det registreres imidlertid ikke hvem som henter ut hva. Intervjudeltakerne vurderer det som nødvendig med et papirarkiv da lærerne har behov for dokumenter som kun er lageret i WebSak, hvor de ikke har tilgang.

Ved innmelding av elever som skal starte i 1. klasse, leverer foreldrene innmeldingsskjema og kontrollerer at elevkortet er riktig. I denne forbindelse blir det fanget opp om det skal gjøres endringer av foresatte tilknyttet eleven. Det kreves dokumentasjon hvis det skal gjøres endringer. Det gjøres manuelle kontroller av om endringer av tilknytning er korrekte, gjerne i forbindelse med den kvartalsvise oppdateringen fra folkeregisteret. Det gis også informasjon til foresatte om hvordan de kan sjekke opplysninger og endre disse i nettportalen Visma Foresatt.

Utskrift og skanning
Skolen har printere for utskrift som gjøres med nøkkelkort eller med kode (7 siffer). Skolen har ikke skanning til sikker sone, skanning av sensitive dokumenter må derfor gjøres av arkivet sentralt i kommunen. Disse blir sendt i lukket konvolutt med internt postbud.

Kommunikasjon av personopplysninger
Ved kommunikasjon med andre etater i kommunen, brukes WebSak hvis det er snakk om personopplysninger. Ved overgang fra barneskole til (kommunal) ungdomsskole brukes Visma Flyt. Til generell kommunikasjon (uten personopplysninger) brukes også e-post og Teams.

Kommunikasjon med eksterne skjer via WebSak og SvarUt. Skolen er opptatt av å unngå at SMS og e-post benyttes til kommunikasjon med foresatte når kommunikasjonen inneholder personopplysninger. Foresatte blir derfor oppfordret til å bruke Visma Foresatt. Hvis foresatte henvender seg på SMS/e-post forsetter skolen dialogen i Visma Flyt og Visma Foresatt.

Skolen mottar henvendelser med spørsmål om elever per telefon. I slike tilfeller er det viktig å være bevist på at man kjenner den man prater med. Dersom man ikke kjenner hen, så ringer man opp igjen etter å ha sjekket nummeret.

SmartVakt Felt og SafeMate

Om systemet
Her fokuserer vi på SafeMate trygghetsalarmer og deres tilknytning til programmet SmartVakt Felt. Løsningen ble tatt i bruk i mai 2018.

SmartVakt er integrert mot CosDoc slik at nødvendige data om pasienter og ansatte hentes automatisk. SmartVakt registrerer automatisk utløste alarmer inn i pasientjournalen i CosDoc.

Tilgangsstyring
For at ansatte skal få tilgang til SmartVakt, må de registreres med arbeidssted og rolle i CosDoc, dette overføres til SmartVakt, men kan også endres i SmartVakt ved behov. Det er en sentral enhet i administrasjonen som registrerer nye ansatte på forespørsel fra enhetsleder.

Ansatte logger seg på alarmenheten med brukernavn og passord.

Logging av bruk
All bruk av SmartVakt blir loggført. Det er ikke noe rutine å sjekke loggen, men det kan gjøres ved behov.

Beredskap
Det er etablert rutiner ved nedetid på systemet. Hvis det er snakk om planlagt nedetid (eks. vedlikehold), så vil leverandøren følge med på alarmene og gi beskjed hvis en alarm er utløst. Hvis det er uplanlagt nedetid, vil leverandør varsle kommunen umiddelbart. Kommunen kan da sende ut melding på enhetene til ansatte (hvis de fortsatt er oppe) slik at ansatte kan foreta ekstra besøk til utsatte pasienter. Alle hjemmesykepleieenhetene har også oversikt på papir over pasienter med trygghetsalarm i tilfelle nedetid.

Hjemmesykepleieavdeling

Systemer som behandler personopplysninger
Hovedsystemet for kommunikasjon og behandling av personopplysninger om pasienter er CosDoc. Dette systemet brukes både til behandling av helseopplysninger om pasienter og for kommunikasjon mellom ansatte, tjenestene og eksterne aktører. Hjemmesykepleien har også flere andre systemer som brukes til mer spesifikke oppgaver hvor det behandles personopplysninger om pasienter. I tillegg til dette benyttes også e-post og Teams til mer generell kommunikasjon, men ikke personopplysninger eller sensitiv informasjon om pasienter.

Enheten holder til i en egen fløy i et større bygg, denne fløya er avlåst og man trenger kodekort for å komme inn (fra utsiden trenger man også kode).

Utskrift, skanning og makulering
Printeren som enheten bruker, står i et fellesareal i bygget hvor enheten holder til. Utskrift kan kun gjøres med en personlig kode på ca. 9 tegn eller med kort. Skanning gjøres også den samme printeren. Skanning til sikker sone kan gjøres til reseptprogrammet som enheten bruker. Det er ikke mulig å skanne dokumenter til CosDoc, disse må i så fall sendes med internpost for skanning i kommunens hovedpostmottak. Ved printeren er også en låst dunk hvor enheten kaster dokumenter som skal makuleres. Inne på enhetens (avlåste) område er det en eske hvor dokumenter som skal makuleres legges og som flere ganger i uka tømmes i den låste dunken i fellesarealet.

Enhetsleder har opplyst at enheten skal flytte til nye lokaler og som en del av flyttingen vil de se på hvordan de bedre kan løse utskrifter og mulighet for makulering inne på eget område.

Behandling av personopplysninger
I det daglige arbeidet i enheten er det noe bruk av papir. Arbeidslistene som inneholder personopplysninger om pasienter, er på papir. Disse blir skrevet ut to ganger daglig (til dag og kveldsskift) og ligger på kontoret til sykepleier 1. Enhetsleder fortalte at det har vært forsøk tidligere på digitale arbeidslister på nettbrett, men at man gikk tilbake til papirlister da det var for

store problemer med tilgjengelighet, bla. knyttet til manglende nettilgang. Det er nå et nytt system med digitale arbeidslister under utprøving i andre hjemmesykepleieenheter og det er forventet at det skal rulles ut til alle enheter.

Det benyttes også «meldingsbok», «dagbok» og «kveldsbok» til å formidle beskjeder mellom ansatte, eks. ved vaktskifte. Bøkene ligger på sykepleier 1 sitt kontor. Enhetsleder opplyser at det finnes en meldingsfunksjon i CosDoc, som er tatt i bruk av noen i enheten, men ikke alle. Denne funksjonen kan erstatte bøkene, men dette forutsetter tid til grundig opplæring, da man ikke kan risikere at viktige beskjeder ikke når frem.

I medisinrommet er det også en medisinliste med personopplysninger som henger opp på veggen. Rommet er låst når det ikke er en sykepleier til stede. Selv om listen er digital skrives den fortsatt ut. Det er planer om å etablere en rutine i løpet av høsten for full digitalisering, dvs. at sykepleierne både henter opplysninger og kvitterer ut digitalt.

Kommunikasjon av personopplysninger
I kommunikasjonen med andre enheter i kommunen bruker de i hovedsak CosDoc. CosDoc brukes også mye i kommunikasjonen med andre offentlige etater, som sykehus, fastlege og andre institusjoner. Telefon brukes også mye. Kontakten med pasienter gjøres enten med telefon eller når man er hjemme hos hen. De får regelmessig telefoner med spørsmål om pasienter, hvor det er viktig å være oppmerksom på at informasjon kun skal gis til nærmeste pårørende, da kan det være nødvendig å spørre om navn og ved behov sjekke opp mot journalen.

3.5.3. Revisors vurdering av tekniske og organisatoriske tiltak
Kommunen har tekniske og organisatoriske tiltak, både på kommunenivå og vi har observert dette i de utvalgte enhetene og systemene. Organisering og rapportering kan regnes som organisatoriske tiltak og vi viser til vår vurdering av dette i avsnitt 3.1.3. Det samme gjelder håndtering av avvik, se vurdering under i avsnitt 3.6.4.

For de overordnede tiltakene mener vi at det fortsatt på jobbes med å sikre en fullstendig implementering. Kommunen har rutiner som har til hensikt å bidra til en trygg bruk av kommunens IKT-tjenester. Det er imidlertid viktig at alle rutinene er tilgjengelig for kommunes ansatte, også i kvalitetssystemet Compilo, hvis de skal ha full effekt. Kommunen bør også sikre at rutinene vedlikeholdes. Kommunen har også til revidering en databrukeravtale, kommunen bør arbeide for at denne blir ferdigstilt.

Overordnet hadde de utvalgte enhetene og systemene har et godt fokus på personvern. Vi så flere typer tiltak for å ivareta informasjonssikkerheten. I begge enhetene var vårt inntrykk at det var stor bevissthet rundt at personopplysninger om elever og pasienter skulle behandles i fagsystemene. Det var også bevissthet rundt å bruke sikre kanaler når en skulle formidle personopplysninger både internt og eksternt. Dog var det i begge enhetene eksempler på informasjonsutveksling internt i kommunen eller mellom ansatte i enheten ble gjort på papir hvor det fantes digitale

løsninger som kunne implementeres. Begge avdelingene var beviste på at personopplysninger ikke måtte deles med uvedkommende også når de fikk henvendelser på telefon.

Tilgangsstyring for ansatte er også et viktig teknisk tiltak både for å ivareta informasjonssikkerheten og for at ansatte har tilgang til den informasjonen de trenger. For begge de utvalgte systemene er det lagt føringer for tilgangsstyringen sentralt. I SmartVakt Felt blir nye ansatte registert i systemet av en sentral enhet. I Visma Flyt Skole er tilganger i systemet styrt ut fra rolle, denne tilgangsstyringen er satt opp sentralt og den enkelte skole kan ikke endre på dette. Et viktig element for tilgangsstyringen er gode passord. Kommunen har rutiner på dette området både for ansatte og elever. Som følge av en mediasak er rutinen for elever nylig oppdatert og det er sendt ut informasjon internt. Kommunen bør, som for de øvrige rutinene sikre, sikre at rutinene for passord er tilgjengelige for ansatte og blir vedlikeholdt.

Logging er et teknisk tiltak for å forhindre utilsiktet bruk av systemet. Begge de to utvalgte systemene logget bruken av systemet.

Undersøkelsene våre tyder på at administrasjonen har gitt tilbud om opplæring på personvern og informasjonssikkerhet til ansatte. Vi vil fremheve det som positivt at flere av de utvalgte enhetene og systemene våre nevnte phishing-kampanjen kommunen har gjennomført, dette tyder på at den var effektiv i å skape bevissthet på området.

Undersøkelsen vår viser at det er gevinster å hente på videre digitalisering som kan fjerne behovet for dokumentasjon med personopplysninger på papir, hvor dette utgjør en risiko for at personopplysninger kan komme på avveie. Det tydeligste eksempelet på dette var skolen hvor sensitive personopplysninger som finnes digitalt, oppbevares på papir. Vi mener det er uheldig at noen av de mest senestive opplysningene om elever oppbevares på papir (dokumenter fra PP-tjenesten, BUPA og barnevern).

3.6. Håndtering av brudd på informasjonssikkerheten

Sandefjord kommune skal ha rutiner for å håndtere brudd på personopplysnings-sikkerheten

3.6.1. Rutine for avvikshåndtering

Styringsdokumentet for informasjonssikkerhet og personvern beskriver kommunens rutiner for rapportering i forbindelse med avvik. Alle avvik skal meldes av den som oppdager avviket. Dersom avviket innebærer brudd på personvernreglene, skal personvernombudet varsles samtidig. Nærmeste leder har ansvar for å håndtere avviket, eventuelt melde det til leder på nivået over ved behov. Hvis et avvik forblir ubehandlet i 14 dager blir det videresendt i systemet til leder over.

Avvik rapporteres i kommunens kvalitetssystem Compilo. Personopplysnings-/informasjons-sikkerhet er en av de fire hovedkategoriene av avvik som kan rapporteres. Disse hovedkategoriene er delt opp i fire underkategorier:

- brudd på den registrerte sine rettigheter
- sikkerhetsbrudd
- feil behandling av personopplysninger
- mangler ved det systematiske personvernarbeidet (internkontroll)

Hver av disse underkategoriene er igjen delt opp i underpunkter som spesifiserer nærmere hva slags avvik det er. Hvis et avvik blir klassifisert som Personopplysnings-/informasjonssikkerhet så får personvernombud og sikkerhetsansvarlig kopi med varsling på e-post og i Compilo.

Ved brudd på personopplysningssikkerheten skal Datatilsynet varsles innen 72 timer. Sikkerhetsansvarlig har ansvar for at dette blir gjort, jf. styringsdokument for informasjonssikkerhet. Styringsdokumentet presiserer også at det ikke er nødvendig å varsle Datatilsynet hvis bruddet ikke vil medføre risiko for den registrertes friheter eller rettigheter. Det er sikkerhetsansvarlig som vurderer om det skal varsles. Hvis det blir besluttet å ikke varsle Datatilsynet, skal administrasjonen begrunne hvorfor. Som et vedlegg til styringsdokumentet er det en egen rutine om varsling til Datatilsynet. Her utdypes styringsdokumentet noe, blant annet står det at kommunen må sikre at den har dokumentasjon som støtter opp informasjonen som blir gitt i varselet til Datatilsynet.

Ifølge personvernombudet, har han arbeidet med å formidle at alvorlige avvik på personvernet, skal registreres i Compilo. I tillegg skal man gi beskjed direkte til leder. Begge deler gjelder også dersom man er usikker på alvorlighetsgraden. Grunnen er, at det kan være nødvendig å gjøre strakstiltak for å begrense omfanget en datalekkasje og for å overholde tidskrav for ev. rapportering til Datatilsynet.

Rådmannens ledergruppe vedtok 13.09.21 en ny rutine og prosesskart for rapportering av avvik generelt. I denne er det gjort flere endringer som kan forebygge feilrapportering. Man har endret navnet på hovedkategorien for personvern/informasjonssikkerhet til personopplysnings-/informasjonssikkerhet. Det fremgår av rutinen at leder som mottar avviket, skal vurdere om det er rett kategori. Hvis leder mener at avviket kan medføre risiko for de registrertes rettigheter, skal hen straks kontakte personvernombudet eller sikkerhetsansvarlig slik at rapportering til Datatilsynet kan vurderes.

Videre har sikkerhetsansvarlig opplyst at han arbeider med en ny rutine og prosesskart for brudd på personopplysningssikkerhet og informasjonssikkerhet. Denne forventes ferdigstilt i løpet av november/desember 2021.

3.6.2. Statistikk på avvik og meldinger til Datatilsynet

Kommunen har byttet til en ny versjon av Compilo i 2021. Både personvernombudet og sikkerhetsansvarlig har gjort oss oppmerksom på at dette har medført en del utfordringer med at avvik som egentlig ikke handler om personvern, blir klassifisert som dette. Begge har opplyst om at det arbeides med å finne ut hvordan man kan unngå feilrapportering, se informasjon om ny rutine

for rapportering av avvik over. Grunnet denne feilklassifiseringen, er det vanskelig å hente ut god statistikk fra Compilo på personvernavvik for 2021.

Da vi mottok statistikken for 2018-2020, merket vi oss trender i dataene som kunne tyde på feilrapporteringen i 2021 også kunne gjelde for årene 2018-2020. Sikkerhetsansvarlig hadde sjekket noen avvik i 2020 og funnet flere som var feilregistrert, og han mente derfor at det var sannsynlig at feilregistrering også har forekommet i tidligere år.

Grunnet usikkerheten knyttet til om avvikene er riktig kategorisert og er tallene i statistikken usikre. Vi velger derfor å ikke presentere statistikk på dette området.

Ifølge administrasjonen er følgende avvik rapportert til Datatilsynet:

Tabell 2 Avvik rapportert til Datatilsynet

År	2019	2020	2021**
Antall avvik rapportert til Datatilsynet	3	1	6

Oppgitt etter år i saksnummer i arkivet.
** Per 14.09.21

3.6.3. Observasjoner fra de utvalgte enhetene og systemene

I intervju med de to enhetene spurte vi om hva de mente ville utgjøre et avvik på personvernet. Skolen sa at dette kunne være data på avveie, eksempelvis ved at noen har fått tilgang til noe de ikke skal ha tilgang til eller hacking. Hjemmesykepleieavdelingen ga følgende eksempler: skrive notat på feil pasient, brudd på taushetsplikt, gi ut informasjon til uvedkommende og lesning av journaler utover tjenstlig behov. Ledelsen ved skolen fortalte at de ikke hadde mottatt avvik på informasjonssikkerhet. Enhetsleder ved hjemmesykepleieavdelingen fortalte at det var lang tid siden vedkommende hadde mottatt noen avvik på dette området.

De ansvarlige for Visma Flyt Skole fortalte om at det har vært tilfeller hvor feil hadde oppstått i forbindelse med hvilken informasjon som foresatte hadde fått tilgang til. I et tilfelle var det en manuell inntasting som gjorde at en foresatt fikk flere barn enn hen skulle ha. Her gjorde Visma endringer i systemet for å forhindre at dette skulle skje igjen. I et annet tilfelle var det en feil hos BankID som gjorde at noen kom inn på feil profil.

De ansvarlige for SmartVakt Felt fortalte at ved avvik knyttet til personvern eller informasjonssikkerhet vil sikkerhetsgruppen bli koblet på automatisk. Videre oppfølgning av avviket og videre involvering av sikkerhetsgruppa vurderes konkret i hvert tilfelle.

3.6.4. Revisors vurdering av rutiner for håndtering av brudd på informasjonssikkerheten

Kommunen har rutiner både for å varsle om avvik på informasjonssikkerheten internt og for hvordan kommunen skal varsle Datatilsynet når det er påkrevd. Rutinen viser hvem som er ansvarlig både for å melde avvik, behandle avvik, og for å eventuelt varsle Datatilsynet. Rutinen for

varsling til Datatilsynet samsvarer med kravene i personopplysningslovens art. 33 og instruksjonen fra Datatilsynet.[15]

Avviksstatistikken vi har fått fremlagt for personvern/informasjonssikkerhet knytter det seg betydelige usikkerheter til. Vi ser at kommunen har gjort noen tiltak for å redusere feilrapporteringen, men vi mener at kommunen må følge opp dette arbeidet videre. God statistikk på området er et viktig grunnlag for læring og forbedring.

Ledelsen ved de to utvalgte enhetene hadde tanker rundt hva som kan utgjøre avvik på personvern/informasjonssikkerhet, men det var sjeldent (om aldri) at det ble meldt avvik på temaet i de to enhetene. De ansvarlige for de to systemene hadde mer erfaring med å motta avvik og løse disse. Siden hvert av fagsystemene dekker et større antall brukere/ansatte enn hva hver av de to enhetene gjør, er det sannsynlig at de ansvarlige for systemene håndterer flere avvik.

3.7. Tiltak for å ivareta innsynsretten

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

3.7.1. Rutine for innsyn

Rutine om innsynsretten følger som et vedlegg til styringsdokumentet for informasjonssikkerhet. Rutinen gjengir personopplysningslovens krav til hvilken informasjon som skal gis og i hvilke tilfeller det kan gis avslag på innsyn. Den fastsetter videre at det er systemansvarlig som vurderer innsynsbegjæringer, at avslag på innsyn skal gis skriftlig, at øvrig dialog også bør være skriftlig og at det, hvis mulig, skal gis en antydning hvor lang tid det vil ta å svare henvendelsen.

I personvernerklæringen på kommunens hjemmesider blir det informert om retten til innsyn og hvilke opplysninger den behandlede har rett til. Informasjonen er generell og gir ikke noe nærmere informasjon om hvordan man kan be om innsyn.

3.7.2. Observasjoner fra de utvalgte enhetene og systemene

Skolen fortalte om at de har mottatt forespørsler fra foresatte om innsyn i opplysninger i Visma Flyt Skole. De fortalte også at hvis de skulle få en forespørsel om innsyn i all informasjon om en elev, ville de ha hentet dette ut fra WebSak. Skolen var bevisst på at opplysninger om elever ikke skal utgis uten foresattes samtykke, dette gjaldt særlig ved telefonhenvendelser hvor det bes om opplysninger om elever.

I intervjuet om Visma Flyt Skole ble det opplyst om at de fleste innsynsforespørsler gikk til den enkelte skole. Sentralt har man mottatt innsynsforespørsler fra tidligere elever hvor hen ber om innsyn i alle dokumenter. Dette er forespørsler man har erfaring med og rutiner for å håndtere.

[15] Vi vil imidlertid bemerke at den som skal fylle ut skjemaet må ha rolle som utfyller/innsender i Altinn, dette er ikke nevnt i kommunens rutine.

Hjemmesykepleieenheten opplyste om at den siste forespørselen de har mottatt om innsyn, var om innsyn i hva som ble notert i journalen i etterkant av et hjemmebesøk. Også denne enheten får henvendelser per telefon om pasienter, og her er det også bevissthet rundt at informasjon kun skal gis ut til nærmeste pårørende (noe som er registret i journalen).

3.7.3. Revisors vurdering av tiltak for å ivareta innsynsretten

Kommunen har en rutine for behandling av innsynskrav som samsvarer med kravene i personopplysningsloven § 16 og art. 15. Den angir hvem som er ansvarlig for å behandle krav, men gir begrenset veiledning utover dette. Rutinen mangler opplysninger om tidsfristene for å svare på forespørsler som er fastsatt i personopplysningslovens art. 12-3.

Det gis informasjon om innsynsretten i personvernerklæringen til kommunen, men denne kunne vært tydeligere, blant annet på om hvordan man ber om innsyn.

I de utvalgte enhetene og systemene ser vi at det er bevissthet rundt retten til innsyn i egne opplysninger og at taushetsplikten begrenser muligheten til å utlevere opplysninger.

3.8. Databehandleravtaler

Sandefjord kommune skal ha system for å sikre at kommunen har databehandleravtale med alle databehandlere

3.8.1. Inngåelse av databehandleravtaler

I henhold til rutinen for anskaffelse av nye system skal det vurderes om det er behov for databehandleravtale og hvis så skal denne utarbeides før kontraktinngåelse med leverandøren. Databehandleravtalen skal godkjennes av kommuneadvokaten.

Det er systemeiere og rådmannen som har myndighet til å inngå databehandleravtaler. Systemeiere må imidlertid alltid konferere med IKT-leder, arkivleder og sikkerhetsansvarlig før databehandleravtaler inngås.[16]

Sikkerhetsgruppen besluttet den 28.09.21 å gå over til å bruke Digitaliseringsdirektoratets standardmal for databehandleravtale. Det kreves imidlertid også noen endringer i iConfirm før standardmalen fra Digitaliseringsdirektoratet kan tas i bruk. Inntil dette er på plass bruker kommunen sin egen mal for databehandleravtale.

Kommunen har en rutine med retningslinjer for anskaffelse av skytjenester og kravspesifikasjon for anskaffelse av skytjenester. I retningslinjen er det sjekklister for anskaffelsesprosessen og det er en egen liste for personvern og det er fastsatt at disse punktene skal ivaretas i databehandleravtalen. Kommunen skal sikre:

[16] Rutine inngåelse av databehandleravtale.

- oversikt over hvilke land som leverandøren behandler personopplysninger i – gjelder både lagring og hvor personer som skal håndtere dataene befinner seg
- kommunens rett å gjøre revisjoner hos leverandøren
- overføring av personopplysninger til utlandet må skje i samsvar med bestemmelsene i personopplysningsloven
- at leverandøren skal ha plikt til å varsle om brudd på sikkerheten som medfører risiko for at personopplysninger er kommet på avveie

I kravspesifikasjonen er det et punkt hvor leverandøren blir bedt om å svare på om de kan signere på kommunes databehandleravtale eller eventuelt EUs standardkontrakt.

I kommunens protokoll (iConfirm) er databehandler oppgitt som avtalepart (med mindre noe annet er oppgitt) og administrasjonen ønsker at databehandleravtalen skal lagres i iConfirm (og WebSak) for alle de systemene som skal ha dette. I vår stikkprøve av registeringer i protokollen hadde 8 av 10 programmer oppgitt avtalepart og for fire av programmene var databehandleravtalen lagt inn.

Ifølge sikkerhetsansvarlig har systemeier ansvaret for å sikre databehandleravtaler til eksisterende systemer. Sikkerhetsansvarlig opplyser om at sikkerhetsgruppen det siste året har startet et arbeid for å sikre kvaliteten på databehandleravtalene. I forlengelse av dette arbeidet, vil det bli tatt initiativ til kontrollarbeid rettet mot systemeiere og å utarbeide en rutine som sikrer at eksisterende systemer har databehandleravtaler som ivaretar kommunens behov. Sikkerhetsansvarlig viser også til at det registreres informasjon om databehandleravtalen i iConfirm. I tillegg er det gitt informasjon om databehandleravtale i webinar om iConfirm.

Vi spurte om status på databehandleravtale for de to utvalgte systemene. De ansvarlige for Visma Flyt Skole fortalte at kommunens databehandleravtale hadde blitt benyttet. De var oppmerksomme på at utviklingen av nye funksjoner i Visma Flyt Skole, medførte at det var et behov for å sikre at avtalen samsvarte med innholdet i produktet. De opplyste at en slik gjennomgang var planlagt. Deltakerne i intervjuet om SmartVakt Felt fortalte at kommunen var i dialog med leverandøren for å revidere databehandleravtalen.

3.8.2. Revisors vurdering av databehandleravtaler

Kommunens har egen mal for databehandleravtale, som synes å inneholde det som er minstekrav etter personopplysningsloven art. 28, tredje ledd. Kommunen har nylig besluttet å gå over til å bruke Digitaliseringsdirektoratets standardmal og er i prosess for å innføre denne som standardmal.

Kommune har et system for innføring nye systemer hvor behovet for databehandleravtale blir vurdert. Ansvaret for å følge opp databehandleravtalen for eksisterende systemer ligger til systemansvarlige. Sikkerhetsgruppen har i tillegg igangsatt med at arbeid for å sikre både at databehandleravtaler er på plass og kvaliteten på disse. Vi mener at det er et fornuftig tiltak fordi gode databehandleravtaler er viktig for å sikre at kommunen kan følge opp sine plikter og at de behandledes kan håndheve sine rettigheter.

Det kan også legges inn informasjon om databehandler og databehandleravtalen i iConfirm og kommunen ønsker at en kopi av databehandleravtalen også legges inn. Hvis dette gjennomføres, vil dette bidra til å holde oversikt over databehandlere og databehandleravtaler.

4. Konklusjoner og anbefalinger

4.1. Konklusjoner

I hvilken grad har Sandefjord kommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Vi mener at Sandefjord kommunes arbeid med informasjonssikkerhet samlet sett har potensiale for forbedring.

Sandefjord kommune har i utgangspunktet etablert gode tiltak og føringer for å ivareta kravene i personopplysningsloven, primært i styringsdokumentet *Informasjonssikkerhet og personvern overordnet styringsdokument*. Men dette dokumentet følges ikke opp på alle punkter, for eksempel

- blir det ikke rapport til rådmannen i samsvar med føringer i dokumentet
- kommunen gjennomfører ikke risikovurderinger for sine systemer i det omfang som følger av styringsdokumentet

Kommunen har ikke fylt ut protokollen for alle systemer slik som personopplysningsloven krever.

Kommunen har gjennomført én vurdering av personvernkonsekvenser (DPIA) og vi mener at kommunen bør vurdere om deres rutiner sikrer at DPIAer blir gjennomført i tilstrekkelig grad.

Kommunen har rutiner for registrering av avvik og har tall som viser hvor mange avvik som er registrert. Vi mener at disse tallene er usikre fordi funn viser at avvik feilaktig har blitt registrert som avvik på personvern og informasjonssikkerhet.

Kommunen har utarbeidet rutiner som skal sikre trygg bruk av IKT-systemene for sine ansatte, men kommunen bør sikre at alle rutinene er tilgjengelige for ansatte i intranett og kvalitetssystem. Våre undersøkelser tyder på at kommunen gjennomfører opplæring om informasjonssikkerhet både til ansatte og ledere.

Kommunen har etablert en rutine for anskaffelse av nye systemer hvor blant annet gjennomføring av ROS-analyse, databehandleravtale og involvering av sikkerhetsgruppa i anskaffelsesprosessen blir ivaretatt. Dette mener vi er et godt tiltak for å ivareta kravene i personopplysningsloven.

Har de undersøkte områdene ivaretatt sentrale krav i personopplysningsloven?
For å besvare denne problemstillingen har vi undersøkt to utvalgte enheter og to utvalgte systemer. Vi valgte ut en skole og en hjemmesykepleieenhet. Vi valgte også ut to fagsystemer, det skoleadministrative programmet Visma Flyt Skole og Smart Vakt Felt, sistnevnte med fokus på trygghetsalarmene SafeMate.

Overordnet sett var vårt inntrykk at det er godt fokus på personvern og informasjonssikkerhet, både på de to enhetene og blant de ansvarlige for de to fagsystemene.

Vi fokuserer her på de tre sentrale prinsippene for informasjonssikkerhet: fortrolighet, riktighet og tilgjengelighet. Vi viser til eksempler på hvordan de to enhetene og to systemene har ivaretatt disse prinsippene.

Når det gjelder fortrolighet, var vårt inntrykk at begge enhetene var beviste på å behandle personopplysninger om elever og pasienter i fagsystemene og bruke sikre kanaler når det var behov for å gjengi personopplysninger i kommunikasjon med andre. Det var også bevissthet rundt fortrolighet når enhetene fikk henvendelser per telefon.

Viktigheten av at opplysninger var riktige fikk vi illustrert både i Visma Flyt Skole og i den utvalgte skolen. Foresatte har tilgang til opplysninger om elevene i en nettportal. Alle foresatte skal ikke ha tilgang informasjon til sine barn, derfor er det viktig at det er riktig tilknytning mellom foresatt og elev. Her kunne både de ansvarlige for systemet og skole vise til kontrollrutiner for å sikre at foresatte ikke får tilgang til opplysninger de ikke skal ha.

Det var utarbeidet beredskapsplaner for når SmartVakt Felt og de tilhørende trygghetsalarmene var ute av drift eller var utilgjengelige. I tillegg har hjemmesykepleieavdelingene oversikter på papir over brukere av trygghetsalarmer i tilfelle systemet er utilgjengelig. Det var ikke tilsvarende beredskapsplaner for Visma Flyt Skole. Begrunnelsen for dette var at systemet har en veldig god oppetid og at hvis systemet hadde nedetid kunne arbeidsprosesser gjøres manuelt og senere ajourføres i systemet.

Tilgangsstyring for ansatte er viktig både for å sikre fortrolighet og tilgjengelighet til personopplysningene. I SmartVakt Felt er tilgangsstyringen knyttet til journalsystemet CosDoc og det er en sentral enhet i kommunen som registrerer nye ansatte. I Visma Flyt Skole er tilganger i systemet styrt ut fra rolle, denne tilgangsstyringen er satt opp sentralt og den enkelte skole kan ikke endre på dette.

Logging er også et tiltak for å sikre utilsiktet bruk av systemet, og dermed opplysningenes fortrolighet. I begge systemene blir bruken av systemet logget.

I begge enhetene så vi eksempler på at personopplysninger ble behandlet fysisk på papir, selv om det fantes digitale alternativ. Etter vår vurdering ville en digital løsning sikre en bedre informasjonssikkerhet fordi den gir bedre mulighet til å styre hvem som får tilgang på informasjonen.

4.2. Anbefalinger

Vi anbefaler kommunen å:

- sikre at rutiner og føringer for informasjonssikkerhet og personvern er oppdaterte og i samsvar med gjeldende krav og anbefalinger
- sikre at det blir skrevet protokoll i samsvar med personopplysningsloven for alle systemer som behandler personopplysninger
- gjennomføre ROS-analyser av alle IKT-systemer som behandler personopplysninger
- sikre at det blir gjennomført vurderinger av personvernkonsekvenser (DPIA) i samsvar med personopplysningsloven
- sikre at avvik om informasjonssikkerhet og personvern blir korrekt registret

Litteratur og kildereferanser

Lover og forskrifter

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

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	Informasjonssikkerhet og personvern; overordnet styringsdokument (vedtatt kommunestyret den 18.09.18)
Dokument	Prosess for anskaffelse av nye systemer

Elektroniske kilder

Datatilsynet: https://www.datatilsynet.no/, nettside herunder følgende veiledere:

- «Behandlingsansvarlig og databehandler», sist endret 17.07.19, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler
- «Behandlingsgrunnlag», sist endret 30.05.18, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/
- «Hvordan lage en databehandleravtale?», sist endret 20.12.19, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/hvordan-lage-en-databehandleravtale/
- «Etablere internkontroll», sist endret 30.10.18, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/
- «Veiledning om de grunnleggende personvernprinsippene», sist endret 16.07.19, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/
- «Informasjon og åpenhet», sist endret 08.06.18, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/gi-informasjon/informasjon-og-apenhet/

- «Mal for behandlingsansvarliges protokoll», datert april 2018, https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/forordningen/artikkel-30_protokoll-behandlingsansvarlig.xlsx
- «Melde avvik til Datatilsynet», sist endret 07.08.18, hentet 24.08.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/
- «Når og hvordan melde avvik?», sist endret 07.08.18, hentet 25.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/nar-skal-jeg-melde-avvik/
- «Protokoll over behandlingsaktivteter», sist endret 19.06.18, hentet 02.07.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/
- «Risikovurdering», sist endret 16.07.19, hentet 25.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/risikovurdering/
- «Sjekkliste for vurdering av personvernkonsekvenser (DPIA)», https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf
- «Vurdering av personvernkonsekvenser (DPIA)», sist endret 17.07.19, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

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

Bøker

ISO/ICE 2701:2013 Informasjonsteknologi – sikringsteknikker – styringssystemer for informasjonssikkerhet

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

Vedlegg

Vedlegg 1: Kommunedirektørens uttalelse

Vi mottok følgende uttalelse fra kommunedirektøren den 22.11.21:

Kommunedirektørens uttalelse til forvaltningsrapporten

Kommunedirektøren mener at forvaltningsrevisjonsrapporten om informasjonssikkerhet i Sandefjord kommune gir et godt bilde av status og utfordringer på dette området. Ledelsen i kommunen har økt oppmerksomheten og innsatsen på dette feltet de siste par årene, men det er fortsatt behov for organisatoriske og andre grep som bringer oss dit vi ønsker å være. Først og fremst handler dette om å følge opp rutiner og tiltak som allerede er beskrevet på en bedre og mer systematisk måte. Rapporten og anbefalingene vil bli fulgt opp som et viktig bidrag for å bringe kommunen dit.

Kommunedirektøren legger opp til å revidere styringsdokumentet og rutinene slik at det beskriver den praksisen kommunen ønsker å følge. Tydeligere rutiner for systematisk rapportering til kommunedirektøren vil gi kommunen bedre kontroll. Rapporteringen bør strekke seg ut over det rent hendelsesstyrte. Kommunedirektøren har konsultert personvernombudet som støtter anbefalingene revisjonen kommer med.

Kommunedirektøren er enig i at det foreligger et forbedringspotensial innenfor arbeidet med ROS analyser og GDPR protokoll. Kommunen har nå fått utviklet ICONFIRM som gjør arbeidet mye mer effektivt. Kommunen er systemansvarlige for en rekke systemer, og har nå gjennom IKT etablert et prosjekt for å sikre at alle systemer vi er ansvarlige for har oppdatert protokoll og ROS analyser.

Kommunedirektøren vil prioritere arbeidet med å styrke internkontrollsystemet. Videre arbeid med ajourhold av styringsdokument, utvikling av rutiner, prosedyrer, prosessflytkart og rapportering i internkontrollverktøyet som er tilgjengelig for alle i organisasjonen vil etter kommunedirektørens vurdering bidra til å styrke internkontrollen innen informasjonssikkerhet.

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 med GDPR 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. GDPR 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, ifølge GDPR art. 4. Det betyr at Sandefjord kommune er behandlingsansvarlig for alle personopplysninger de behandler.

Det kan være noen få unntak, når kommunen gjør oppdrag på vegne av andre. Da vil Sandefjord kommune være databehandler på vegne av oppdragsgiver, oppdragsgiver vil være databehandler. GDPR setter strenge krav til databehandler. Vi undersøker ikke situasjoner der Sandefjord kommune er databehandler på vegne av andre oppdragsgivere.

Det er Sandefjord 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 oppgaver som kommer i konflikt

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

Personvernprinsippene

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

- lovlig, rettferdig og gjennomsiktig
- formålsbegrensning
- dataminimering
- riktighet
- lagringsbegrensning
- integritet og fortrolighet
- ansvarlighet

Personopplysningsloven er bygd opp rundt disse prinsippene. Datatilsynet har utdypet prinsippene i en veileder. Sandefjord kommune som behandlingsansvarlig har ansvar for å følge opp disse prinsippene.

Lovlig, rettferdig og gjennomsiktig

GDPR 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 GDPR art. 9 være oppfylt. Disse kravene er blant annet 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 gjennomsiktig, innebærer at det er oversiktlig og forutsigbart for den registrerte. GDPR kapittel III omhandler den registrertes rettigheter. Art. 12 krever at kommunen skal gi klar og tydelig informasjon til den registrerte. Den registrert 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). Den registrerte 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 personopplysninger om seg selv slettet (art. 17).

Formålsbegrensning
Personopplysninger skal bare brukes til det formålet det 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 GDPR.

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 blant annet vise formålet med behandlingene, hvilke kategorier personopplysninger kommunen behandler, og hvis det er mulig tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Hvis det er aktuelt, anbefaler Datatilsynet at 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[17]. 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 forordning overholdes.

Personvernforordningen artikkel 5.1 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

[17] DPIA står for Data Protection Impact Assessment

behandlingen utføres i samsvar med GDPR. 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 også omfatte hvilke erfaringer og 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 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 flere begrensninger på retten til å få personopplysninger slettet, blant annet kan ikke kommunen slette personopplysninger når de skal bevares for arkivformål eller for å oppfylle en rettslig forpliktelse.

Databehandlere

En databehandler behandler personopplysninger på vegne av en behandlingsansvarlig. Kommunen er behandlingsansvarlig for personopplysningene de behandler. 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, og setter en klar ramme for hvordan databehandleren kan behandle opplysninger. 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 artikkel 28 nr. 1).

Kommunen skal vurdere om databehandleren gir tilfredsstillende garantier sett i sammenheng med personopplysningene som skal behandles.

En databehandleravtale skal inneholde:

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

Revisjonskriterier

På denne bakgrunn har vi utledet følgende revisjonskriterier:

Sandefjord 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

Vedlegg 3: Metode og kvalitetssikring

Forvaltningsrevisjonen startet opp ved oppstartsbrev 11.05.21. Oppstartsmøte ble holdt 21.05.21 med rådmann, økonomisjef, IKT-leder, personvernombud, sikkerhetsansvarlig med flere til stede. Både oppstartsmøte og sluttmøte ble gjennomført på Teams.

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.

Vi vil nedenfor redegjøre for datagrunnlaget vårt og hvilke metoder vi har brukt for å svare på problemstillingene. Vi vil også beskrive hvilke tiltak som er brukt for å sikre dataenes relevans og pålitelighet.

Innsamling av data, relevans og pålitelighet

Datainnsamling og rapportskriving har foregått i perioden juni til oktober 2021.

For å kartlegge kommunens tiltak for å ivareta kravene i personopplysningsloven har vi gjennomgått dokumentasjon fra kommunen som styringsdokumenter og rutiner. Vi har hatt løpende skriftlig korrespondanse per e-post med IKT-leder, sikkerhetsansvarlig og personvernombud for å avklare forskjellige spørsmål.

Kartlegging av rutiner vil alene gi et begrenset innsyn i hvilken grad rutinene etterleves, derfor har vi kombinert dokumentgjennomgangen med andre metoder – nærmere bestemt intervjuer, ulike stikkprøvekontroller og gjennomgang av utvalgte enheter og systemer.

Intervjuer

Vi har intervjuet personvernombudet på Teams. I tillegg har vi gjennomført intervju med de to enhetene og de to systemene, se informasjon om dette under. For alle intervjuene mottok intervjudeltakerne en intervjuguide i forkant og i etterkant mottok de et referat til godkjenning.

Stikkprøver

For å undersøke etterlevelsen av rutinen for risikovurdering og om protokollen var utfylt med påkrevd informasjon, gjennomførte vi en stikkprøve. Det samme utvalget ble brukt i begge stikkprøvene. Utvalget ble gjort fra alle systemene registrert i kommunens protokoll (iConfirm). Utvalget ble gjort i to omganger. Først ble det tilfeldig valgt ut tre systemer blant de som var klassifisert med risiko «kritisk». Deretter ble syv systemer tilfeldig valgt ut blant alle de som var registrert i iConfirm. Tabellen på neste side viser hvilke systemer som ble valgt ut.

Tabell 3 Utvalgte systemer til stikkprøve

Utvalg	System	Risikoklassifisering i iConfirm
Kritisk	Dips Communicator	Kritisk
Kritisk	Visma samhandling arkiv	Kritisk
Kritisk	ACOS Mottak	Kritisk
Alle	Fri5 - Sandefjord kommune Booking program	Uklassifisert
Alle	Kommunikasjon - Kommunekari	Uklassifisert
Alle	Arrangementer - kursportal	Medium
Alle	IKOS Elektronisk tavle	Uklassifisert
Alle	Campus Increment	Medium
Alle	Gemini Arena	Høy
Alle	BliksundWeb & Prehospital Elektronisk Pasientjournal	Høy

Vi fikk fremlagt statistikk på avvik og rapportering av avvik til Datatilsynet. Vi fikk også tilgang til iConfirm som kommunen bruker til sin protokoll og kvalitetssystemet Compilo.

Casestudier (undersøke områder)
Vi gjennomførte fire casestudier, ellers omtalt som utvalgte enheter og systemer. Dette for å besvare om disse hadde ivaretatt sentrale krav i personopplysningsloven. I samsvar med bestillingen fra kontrollutvalget valgte vi ut enheter og systemer fra kommunalområdene kunnskap, barn og unge og helse, sosial og omsorg. Begrunnelsen for å velge disse to områdene, er at det er områder som behandler store mengder med personopplysninger om innbyggere, disse opplysningene omhandler ofte sensitive grupper (barn, unge, eldre og pleietrengende) og det kan også være sensitive personopplysninger.

Vi valgte derfor ut et fagsystem og en enhet fra hver av de to kommunalområdene. Enhetene ble valgt ut tilfeldig ut blant alle enhetene henholdsvis hjemmesykepleie og skoler i kommune. Systemene ble valgt ut etter en konkret av vurdering av opplysningene de behandlet og vi vektla at det var systemer som ble brukt i de to aktuelle enhetene. De utvalgte systemene er det skoleadministrative systemet Visma Flyt Skole og SmartVakt Felt. Når det gjelder SmartVaktFelt har vi fokusert på funksjonen som varsler ansatte om utløste trygghetsalarmer.

For de to enhetene gjennomførte vi et intervju med leder og de som leder ønsket å ha med seg i intervjuet. Vi fikk også en kort befaring på de to enhetene.

For de to fagsystemene fikk vi tilsendt dokumentasjon for systemet og vi gjennomførte intervju med systemeier og systemansvarlig. I et av intervjuene deltok også en fagperson fra IKT-avdelingen.

I tillegg til å godkjenne referatet fra intervjuet mottok de utvalgte enhetene og systemene avsnittene i rapportens faktadel hvor opplysninger om dem fremkom til en ekstra gjennomlesning.

Vi har sjekket ut med administrasjonen at fakta i rapporten er korrekt framstilt. Rapporten er sendt kommunedirektøren til uttalelse, jf. forskrift om kontrollutvalg og revisjon § 14. Uttalelsen ligger i vedlegg 1.

Personopplysninger

I forbindelse med denne forvaltningsrevisjonen har vi behandlet personopplysninger som navn, stilling 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.[18]

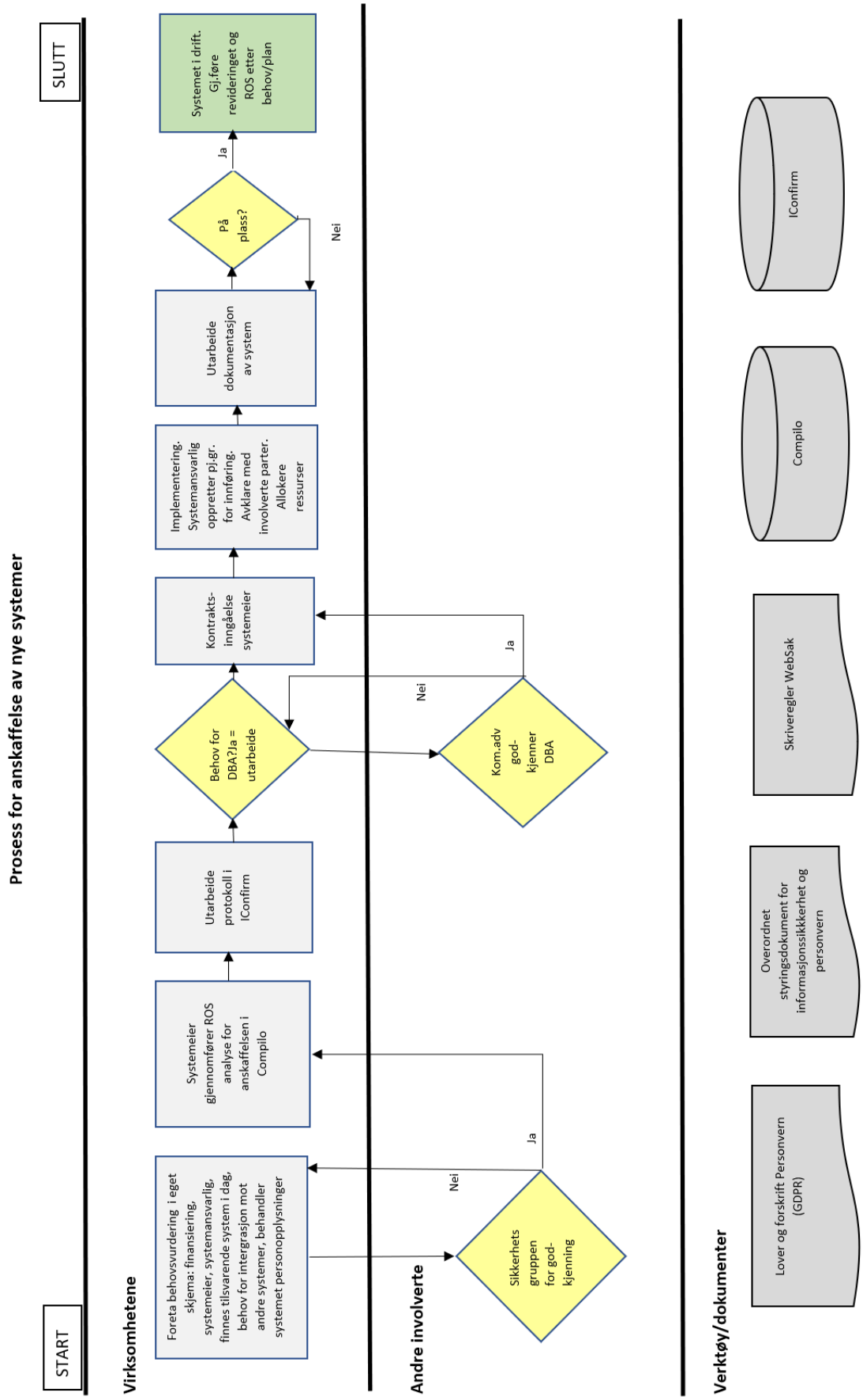
Kvalitetssikringen skal sikre at undersøkelsen og rapporten har nødvendig faglig og metodisk kvalitet. Videre skal det sikres at det er konsistens mellom bestilling, problemstillinger, revisjonskriterier, data, vurderinger og konklusjoner.

Vestfold og Telemark revisjon IKS har et system for kvalitetskontroll som er i samsvar med den internasjonale standarden for kvalitetskontroll.[19] Denne forvaltningsrevisjonen er kvalitetssikret i samsvar med vårt kvalitetskontrollsystem og i samsvar med kravene i RSK 001.

[18] 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. Standarden bygger på norsk regelverk og internasjonale prinsipper og standarder, fastsett av International Organization of Supreme Audit Institutions (INTOSAI) og Institute of Internal Auditors (IIA).

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

Vedlegg 4: Prosess for anskaffelse av nye systemer



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