Rogaland Revisjon

Forvaltningsrevisjon

Personvernreglene

Sandnes kommune, 2022

INNHOLD

OPPDRAGET

Bestilling

Kontrollutvalget i Sandnes kommune bestilte 18.09.20 en forvaltningsrevisjon om personvern.

Formål

Formålet med prosjektet er å vurdere hvordan Sandnes kommune sikrer at personvern ivaretas ved endring og utvikling av systemer og hvordan virksomheter følger opp personvernreglene i praksis.

Problemstillinger

- I hvilken grad sikrer kommunen at personvern ivaretas ved endring og utvikling av systemer?
- I hvilken grad sikrer kommunen at ansatte er kjent med hvordan personopplysninger skal håndteres?
- I hvilken grad oppbevarer, behandler og sletter virksomhetene personopplysninger i henhold til regelverket?
- Hvordan håndterer kommunen brudd på personvernreglene og hvordan følges dette opp?[1]

[1] Problemstillingen ble lagt til av kontrollutvalget i kontrollutvalgsmøte 11.12.20

SAMMENDRAG

På oppdrag fra kontrollutvalget har Rogaland Revisjon utført forvaltningsrevisjon av personvernreglene i Sandnes kommune. Formålet med prosjektet er å vurdere hvordan Sandnes kommune sikrer at personvern ivaretas ved endring og utvikling av systemer, og hvordan virksomheter følger opp personvernreglene i praksis. I prosjektet er det foretatt dokumentanalyse, gjennomført intervjuer, og kontroller i Draftit[2] og postliste.

Hovedbudskap

- Kommunen har på plass rutiner for å ivareta personvernkrav i de digitale løsninger kommunen har valgt, og disse blir i stor grad etterlevd i praksis.
- For å sikre at personvernkrav ivaretas i digitale løsninger, bør kommunen sørge for at alle systemer registreres i kommunens oversikt over alle behandlinger og tilknyttede systemer (Draftit).
- Kommunen bør sørge for at det gjennomføres risikovurderinger for digitale løsninger som tas i bruk.

I hvilken grad sikrer kommunen at personvern ivaretas ved endring og utvikling av systemer?

Ansvaret for å ivareta krav til personvern er delegert til systemeier i den enkelte enhet. Dette innebærer for eksempel krav til å registrere systemet i Draftit, sørge for databehandleravtale og å gjennomføre en risikovurdering. Rutiner som sikrer at personvernet ivaretas er oversiktlig beskrevet i informasjonssikkerhetshåndboken. Kommunen har maler for databehandleravtale og risikovurdering, som vi vurderer som tilstrekkelige i henhold til personvernkrav. Ny mal for databehandleravtale er også under utarbeidelse, og vil bygge på vedtatt standard fra EU/EØS, noe som vil høyne kvaliteten. Kostnadsmessig større digitale løsninger, anskaffes i tråd med lov om offentlige anskaffelser. Krav til personvern er også beskrevet i kommunens arkitekturprinsipper. I anskaffelsesprosesser er det etablert praksis å koble på faglige støttefunksjoner for å kunne stille de riktige personvernkravene til leverandør, samt å sørge for gjennomføring av risikovurderinger og utarbeidelse av en databehandleravtale.

Kommunen tar også i bruk digitale løsninger, som kostnadsmessig ikke utløser krav etter lov om anskaffelser. Slike systemer kan ha omfattende behandling av personopplysninger, som gratistjenester fra Google. I slike tilfeller involveres ikke de samme faglige støttefunksjoner og anskaffelsesavdeling, og den enkelte enhet er derfor mer alene om å ivareta personvernkrav. De intervjuede forteller om økt bevissthet rundt hvilke krav som stilles ved bruk av digitale løsninger. Men, det hender at gjennomføring av risikovurdering og registrering i Draftit ikke alltid blir gjort. Ett eksempel er skolene, som i 2020 tok i bruk programmet «G Suite for Education», uten å gjennomføre risikovurderinger og sikre andre krav til personvern.

[2] Elektronisk løsning som gir oversikt over system som behandler personopplysninger.

I hvilken grad sikrer kommunen at ansatte er kjent med hvordan personopplysninger skal håndteres?

Kommunens informasjonssikkerhetshåndbok gir tilfredsstillende informasjon om hvilke krav som stilles til ansatte og ledere når det gjelder personvern, og tar for seg tema som tilgang, bruk av e-post, avvik, lagring, anskaffelser, internkontroll og avhending. Ifølge kommunens egen spørreundersøkelse er informasjonssikkerhetshåndboken godt kjent blant de ansatte,

Kommunen har obligatoriske e-læringskurs som omhandler personvern og informasjonssikkerhet, som skal sikre at ansatte er kjent med hvordan personopplysninger skal håndteres. Status per oktober 2021 er at 34 prosent av de ansatte har gjennomført kurset. Gjennomføringsgraden bør økes for å sikre kompetanseheving for hele organisasjonen. Kommunen opplyser også i intervju at de jobber aktivt for å få flere til å gjennomføre kurset.

I hvilken grad oppbevarer, behandler og sletter virksomhetene personopplysninger i henhold til regelverket?

Kommunen behandler personopplysninger og sensitive opplysninger både digitalt i fagsystemer og i skriftlig form. Rutiner for behandling av personopplysninger er beskrevet i informasjonssikkerhetshåndboken, og de intervjuede forteller at rutinene i stor grad blir fulgt opp. For eksempel blir ikke sensitive opplysninger sendt per e-post. Inneholder en e-post sensitive opplysninger, blir disse slettet før et eventuelt svar blir sendt.

For å sikre personvernkrav skal systemer registreres i Draftit. Her blir blant annet behandlingsgrunnlag beskrevet, hvorvidt databehandleravtaler foreligger, og om risikovurderinger er gjennomført. Ifølge de intervjuede har det vært en økende bevissthet om personvern i kommunen de siste årene. Likevel er ikke alle systemer blitt registrert i Draftit, og her gjenstår noe registreringsarbeid ute i enhetene.

Hva som publiseres på de offentlige postlistene blir styrt fra sentralt hold i kommunen. Dette sikrer felles praksis, og i vår kontroll av kommunens postliste, har vi ikke funnet personopplysninger eller sensitive opplysninger, noe som er positivt.

Ved ansettelse eller ved avslutning av arbeidsforhold tildeles tilganger til de fagsystem som er knyttet til den stilling/rolle vedkommende ansatt skal ha. Utover dette sjekkes nødvendige tilganger i liten grad. Kommunens undersøkelse viser at 14 prosent av lederne ikke vet hvordan tilganger blir sjekket. Ansattes bruk av fagsystemer blir per i dag loggført. I noen systemer blir det foretatt stikkprøver av slike logger, men kommunen har ikke formalisert kontrollen av logger. Det er positivt at kommunen har systemer med loggføring og rutiner for tilgangsstyring. For å hindre brudd på personvernet, ville det vært hensiktsmessig med økt kontroll på logg og tilganger.

Hvordan håndterer kommunen brudd på personvernreglene og hvordan følges dette opp?

Kommunen benytter seg av Compilo som er et system for kvalitetsarbeid og avviksoppfølging, og rutiner for avvikshåndtering er beskrevet i informasjonssikkerhetshåndboken. Avvik i Compilo meldes inn av den enkelte ansatte, og sendes til linjeleder som iverksetter tiltak og lukker avviket. Informasjonssikkerhetssjef og personvernombud mottar også disse avvikene og

har en kontrollrolle, noe som innebærer en gjennomgang av avvikene for å identifisere forbedringspunkter. Kommunen har utarbeidet en rutine for hvordan avvik skal meldes til Datatilsynet.

Inntrykket vi sitter igjen med fra intervju med kommunens ansatte og resultatene fra kommunens egen spørreundersøkelse, er at ikke alle avvik knyttet til informasjonssikkerhet og personvern meldes i Compilo. Her viser de ansatte til en manglende kultur for å melde avvik, noe som kommunen bør jobbe videre med. I tillegg fremhever de intervjuede at enheter som benytter seg av Compilo for andre typer avvik, sannsynligvis er flinkere til å melde inn avvik knyttet til personvern og informasjonssikkerhet.

Våre anbefalinger

- Kommunen bør sørge for å få registrert alle systemer som behandler personopplysninger i Draftit.
- Kommunen bør sikre at det gjennomføres risikovurderinger ved bruk av digitale løsninger.
- Kommunen bør øke gjennomføringsgraden for e-læringskurset for personvern og informasjonssikkerhet
- Kommunen bør vurdere tiltak som kan skape en kultur for å melde inn avvik på informasjonssikkerhet og personvern.

KOMMUNEDIREKTØRENS KOMMENTAR

Personvernforordningen (Forordning 2016/679, på engelsk General Data Protection Regulation, forkortet GDPR) er en forordning som skal styrke og harmonisere personvernet ved behandling av personopplysninger i Den europeiske union (EU). I Norge trådte forordningen i kraft 20. juli 2018.

Siden forordningen har det pågått et systematisk arbeid med å implementere forordningen, etablere og forbedre rutiner i hele virksomheten. Anbefalingene i rapporten er i tråd med det arbeidet som er igangsatt og som må forbedres. Det må jobbes med holdningene hos alle ansatte slik at alle tilstreber mest mulig gode rutiner knyttet til arbeidet med å sikre kommunens personopplysninger.

Informasjonssikkerhetssjef og personvernombudet må bli involvert og informert i prosesser som omhandler personopplysninger. Kommunens ledelse og behandlingsansvarlig må ha personvern som tema jevnlig, og invitere informasjonssikkerhetssjef og personvernombudet inn i møtene.

Kommunen har utarbeidet en sikkerhetserklæring som en vil vurdere at alle ansatte skal signere på linje med en taushetserklæring.

Kommunedirektøren tar anbefalingene fra rapporten til Rogaland revisjon til etterretning og vil sørge for å forbedre rutiner og arbeid knyttet til de ulike anbefalingene.

1. Kommunen bør sørge for å få registrert alle systemer som behandler personopplysninger i Draftit.

Kommentar: Kommunen har system (Draftit) og beskrevet rutiner på dette.Kommunen vil øke fokus på dette arbeidet i organisasjonen spesielt innenfor skoleområdet for å registrere alle behandlingene i Draftit.

2. Kommunen bør sikre at det gjennomføres risikovurderinger ved bruk av digitale løsninger.

Kommentar: Kommunen har verktøy og det tilbys faglig støtte ved gjennomføring av ROS og DPIA. Det er viktig at dette gjøres godt kjent for ledere og systemansvarlige. Det er viktig at aktuelle faginstanser involveres i anskaffelsesprosessen.

3. Kommunen bør øke gjennomføringsgraden for e-læringskurset for personvern og informasjonssikkerhet

Kommentar: Kommunen vil sikre at alle ansatte gjennomfører dette kurset. Ledere på alle nivå har ansvar og vil få påminnelser. Det vil bli lagt inn som tema i ledersamtale/oppfølgning/internkontrakt. En vil samtidig vurdere om opplæringen kan

gjennomføres på en annen måte for å nå større arbeidsgrupper som f.eks. innen skole, barnehager, helse/ velferd, renhold.

4. Kommunen bør vurdere tiltak som kan skape en kultur for å melde inn avvik på informasjonssikkerhet og personvern.

Kommentar: Det arbeides med å etablere en god avvikskultur på alle områder i kommunen – også innen informasjonssikkerhet og personvern. I høst har det vært gjennomført HMS-kurs innen avvikshåndtering med god deltakelse fra verneombud og ledere – nye kurs er satt opp ut over våren 2022.

For å få ansatte til å melde avvik må de oppleve at avviket blir tatt på alvor og blir fulgt opp. Det er også viktig at ansatte blir gjort kjent med Compilo som avvikssystem. Det er grunn til å tro at når ansatte øker kjennskap til hvordan avvik meldes og håndteres generelt vil dette øke bevisstheten til å melde inn avvik knyttet til informasjonssikkerhet og personvern.

INNLEDNING

1.1 BAKGRUNN OG AVGRENSNING

I 2018/19 gjennomførte Rogaland revisjon en forvaltningsrevisjon om informasjonssikkerhet, drift og sårbarhet i Sandnes kommune, og kom da med følgende anbefalinger:

- Påse at retningslinjer og prosedyrer blir tilgjengelig for ansatte på intranett så fort som mulig.
- Sikre at de systemansvarlige får tilstrekkelig tid og mulighet til å utøve sitt ansvar som systemansvarlig.
- Prioritere å utarbeide en plan for oppfølging av risikoanalysen fra 2017/2018.
- Foreta en kontroll av registreringene i Draftit, både i forhold til hvilke systemer det er registrert behandlinger i forhold til og fullstendigheten i utfyllingen av skjemaene. Det må også kontrolleres at det foreligger nødvendige databehandleravtaler der det er påkrevd.
- Vurdere behovet for et sikkerhetsovervåkingssystem som et proaktivt vern mot stadig mer avanserte og komplekse trusler og angrep.

I oppfølgingen av revisjonen svarer kommunen at det er utarbeidet ny informasjonssikkerhetshåndbok. Det er gjort grep i IT-drift, som å sikre god oppetid og lage prosesser for IT-drift (ITIL). Sikkerhetsovervåkning er en utfordring som kommunen ser på sammen med andre kommuner i ulike regionale og nasjonale nettverk. Kommunen svarer at det er utfordrende å tilføre systemansvarlig ytterligere ressurser, men at støttesystemer og samordning med IT-drift skal bidra til at systemansvarligansvaret blir ivaretatt. Til slutt svarer kommunen at registrering av Draftit er nytt og vil være en kontinuerlig prosess[3].

I denne forvaltningsrevisjonen har vi ikke gått nærmere inn på områder innen IT drift, men i hovedsak fokusert på hvordan Sandnes kommune følger opp personvernreglene i praksis, både i det daglige arbeidet og ved utvikling av nye løsninger. I prosjektet har vi vurdert Sandnes kommunes systemer og struktur for informasjonssikkerhet, med særlig fokus på ansvarsfordeling og personvern.

[3] Saksdokumenter og møter - Møter - Kontrollutvalget i Sandnes (15.05.2020) (opengov.cloudapp.net)

1.2 DEFINISJONER AV SENTRALE BEGREPER

Personvernbegrepet refererer til vernet av privatlivets fred, og den enkeltes personlige integritet og rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv[4]. Det skilles mellom to typer opplysninger:

Personopplysning: Enhver opplysning om en privatperson som er identifisert eller som kan identifiseres, for eksempel navn, adresse, telefonnummer, e-post, fødselsnummer, atferdsmønstre og et bilde dersom personer kan gjenkjennes.[5]

Sensitive personopplysninger (særlige kategorier av personopplysninger): Dette er for eksempel: rase, opplysninger om politisk oppfatning, religion, helseopplysninger og seksuell legning[6]. Det skal mere til for å kunne behandle denne typen opplysninger.

Informasjonssikkerhet: Handler om å beskytte all type informasjon på en tilfredsstillende måte, slik at informasjon ikke blir gjort kjent for uvedkommende, ikke blir endret utilsiktet. Informasjonen skal være tilgjengelig når de som skal ha tilganger, har behov for det.

GDPR-forordningen: Som en del av personopplysningsloven, inngår EØS-avtalens vedlegg XI nr. 5e forordning / Europaparlaments- og rådsforordning (EU) 2016/679 av 27.04.16. Denne omhandler vern av fysiske personer i forbindelse med behandling av personopplysninger og utveksling av slike opplysninger[7]. Forordningen inneholder et omfattende personopplysningsregelverk, herunder de grunnleggende prinsippene og vilkårene for å behandle personopplysninger, rettigheter for enkeltpersoner og plikter for behandlingsansvarlige og databehandlere. Det skal utarbeides rutiner som er nødvendige for å oppfylle virksomhetens plikter og de registrertes rettigheter, og det stilles krav om internkontroll.

Velferdsteknologi: «*[…] teknologisk assistanse som bidrar til økt trygghet, sikkerhet, sosial deltakelse, mobilitet og fysisk og kulturell aktivitet, og styrker den enkeltes evne til å klare seg selv i hverdagen til tross for sykdom og sosial, psykisk eller fysisk nedsatt funksjonsevne. Velferdsteknologi kan også fungere som teknologisk støtte til pårørende og ellers bidra til å forbedre tilgjengelighet, ressursutnyttelse og kvalitet på tjenestetilbudet. Velferdsteknologiske løsninger kan i mange tilfeller forebygge behov for tjenester eller innleggelse i institusjon.*»[8]

[4] https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/
[5] https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/ og artikkel 4 i Europaparlaments- og rådsforordning (EU) 2016/679 av 27.04.16 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.
[6] https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/
[7] EØS-avtalen vedlegg XI nr. 5e forordning / Europaparlaments- og rådsforordning (EU) 2016/679 av 27.04.16
[8] "NOU 2011: 11 Innovasjon i omsorg." (2011).

1.3 REVISJONSKRITERIER

I dette prosjektet er følgende kilder lagt til grunn for utvikling av revisjonskriterier:

- Kommuneloven
- Personopplysningsloven og personvernforordningen (GDPR)
- eForvaltningsforskriften
- Datatilsynets veileder for internkontroll
- Veiledere fra Digitaliseringsdirektoratet
- Veiledere fra Nasjonal Sikkerhetsmyndighet (NSM)
- Sandnes kommune informasjonssikkerhetshåndbok
- Sandnes kommunes rutiner for personvern

Revisjonskriteriene vi har brukt for å belyse de ulike problemstillingene viser ikke nødvendigvis til alle krav innenfor GDPR-regelverket. Revisjonen har gjort en vurdering av hvilke GDPR-krav som er sentrale for kommunens oppgaver og som knytter seg til hovedprinsippene for GDPR (artikkel 5). En nærmere beskrivelse av bakgrunn og utledning av revisjonskriterier kommer frem i fakta- og vurderingsdelen.

1.4 METODE

I prosjektet er det foretatt dokumentanalyse og kontroll i Draftit og postliste. Det er gjennomført intervjuer med personvernombud, informasjonssikkerhetssjef, leder dokumentsenter, skolesjefdigitaliseringsleder, rådgiver i anskaffelsesavdelingen, kommuneadvokat, samt fire virksomhetsledere innen oppvekst barn og unge, og helse og velferd. Følgende spørreundersøkelser er også brukt som datagrunnlag for revisjonen:

Fra tidligere revisjon:
Spørreundersøkelse utført av Rogaland Revisjon IKS i forbindelse med forvaltningsrevisjon av informasjonssikkerhet, drift og sårbarhet. Undersøkelsen ble sendt til alle de systemansvarlige i. Sandnes kommune (43 respondenter) med en svarprosent på 65 prosent9.

Kommunens egen spørreundersøkelse:
Kommunen har egen digital spørreundersøkelse om informasjonssikkerhet som har blitt sendt ut til ansatte og ledere i tre tjenesteområder; Oppvekst barn og unge, Oppvekst skole og Organisasjon. Resultatet gir svar på etterlevelse av rutiner og praksis for tre av kommunens enheter, og kan nødvendigvis ikke brukes som svar på hvordan hele organisasjonen etterlever personvernkrav.

[9] Link til rapporten

Undersøkelsen ble sendt ut til ledere i november 2020, mens ansatte fikk den i januar 2021. Undersøkelsen ble videreformidlet via ledere, og det er ikke regnet ut svarprosent for undersøkelsen. Respondenter for undersøkelsen vises i tabell under:

Tabell 1. Antall respondenter på kommunenes informasjonssikkerhetsspørreundersøkelse.

Enhet	Ansatte	Ledere
Oppvekst barn og unge	109	25
Oppvekst skole	103	19
Organisasjon	63	6
Totalt	**275**	**50**

1.5 AVGRENSNING

Sandnes kommune ble i 2020 slått sammen med Forsand kommune. I innledende intervju med personvernombud og informasjonssikkerhetssjef ble det informert om at det er Sandnes kommune sine systemer som er blitt brukt etter kommunesammenslåingen. Revisjonen har derfor ikke tatt hensyn til systemer, rutiner og praksis i tidligere Forsand kommune.

1.6 ORGANSISERING AV TJENESTER I SANDNES

Kommunen har den siste tiden gjennomført omorganiseringer[10]. En av endringene er sammenslåing av Digitalisering og IT. Digitaliseringsavdelingen ble opprettet i 2016 med 3-4 ansatte som jobbet med utvikling av nye digitale løsninger. Avdelingen ble i august 2021 slått sammen med IT-avdelingen som er en driftsavdeling. Den nye avdelingen, «Digitalisering og IT», har ca. 20 ansatte.

Personvernombudet hadde tidligere også rollen som sikkerhetsansvarlig. En slik dobbeltrolle kan gi interessekonflikter og er ifølge Datatilsynet ikke en anbefalt løsning. Hovedregelen er at personvernombudet skal sikres uavhengighet og ikke samtidig bestemme formål og måten personopplysninger behandles. Fra 2019/20 har Sandnes kommune skilt ut rollen som sikkerhetsansvarlig til en ny stilling som informasjonssikkerhetssjef.

[10] Organisasjonskartet er per november 2021 ikke oppdatert og derfor ikke inkludert

2 ENDRING OG UTVIKLING AV NYE SYSTEMER

Problemstilling: «I hvilken grad sikrer kommunen at personvern ivaretas ved endring og utvikling av systemer?»

2.1 REVISJONSKRITERIER

Personvernforordningen artikkel 24, 25, 32 og 35 stiller krav om at behandlingsansvarlig og databehandler vurderer risiko ved behandling av personopplysninger. Etter artikkel 32 skal det gjennomføres risikovurderinger før nye løsninger tas i bruk, ved endringer og ellers bli regelmessig oppdatert[11]. Digitaliseringsdirektoratet[12] beskriver følgende trinn i risikovurderinger:

1) Risikoidentifisering: Her identifiseres mulige hendelser som kan føre til at personopplysninger ikke blir behandlet korrekt.

2) Risikoanalyse: Potensielle hendelser blir analysert etter sannsynligheten for at det skjer og for hvor stor konsekvens hendelsen vil ha for personvernet. Ut ifra sannsynlighet og personvernkonsekvens settes det et risikonivå for hendelsen.

3) Risikoevaluering: Evalueringen skal si noe om hvilke risikoer som skal håndteres og i hvilken rekkefølge.

Risikovurderingen identifiserer tiltak som må gjøres for å oppnå et egnet sikkerhetsnivå. Tiltakene kan være både av teknisk eller organisatorisk art. Etter artikkel 30 skal behandlingsansvarlig føre protokoll over behandlingsaktiviteter for personopplysninger.

Hvis behandling av personopplysninger medfører høy risiko for personers rettigheter og friheter, skal det etter personvernforordningen artikkel 35 gjennomføres vurderinger av personvernkonsekvenser (Data Protection Impact Assessment - DPIA). DPIA gjennomføres av behandlingsansvarlig i samarbeid med personvernombud. Det finnes en rekke ulike maler for DPIA, og det er vanlig at større virksomheter lager egne maler som er tilpasset bruken av personopplysninger.

Virksomheter benytter seg gjerne av skytjenester for lagring av data, ulike IT-løsninger og andre eksterne leverandører. Ved slik behandling av personopplysninger skal behandlingsansvarlig inngå egne databehandleravtaler med databehandleren, jamfør personvernforordningen artikkel

[11] Veiledning om DPIA | Datatilsynet

[12] Hva er risikovurdering? | Digitaliseringsdirektoratet - Difi

28-29. Avtalen inneholder instrukser for databehandleren for å kunne ivareta GDPR og andre relevante lovverk.

Ved utvikling av nye systemer skal behandlingsansvarlig sørge for at prinsippene for innebygd personvern blir brukt (artikkel 25). Dette betyr at prinsippene i GDPR (artikkel 5) skal være en integrert del av systemet.

Revisjonskriterier:

- Kommunen skal gjennomføre risikoanalyser ved utvikling eller endring av systemer.
- Kommunen skal ha databehandleravtaler som ivaretar krav til personvern.

2.2 KOMMUNENS PLANER OG STRATEGIER

Hvilke rutiner som er gjeldende for utvikling og anskaffelse av nye systemer, er avhengig av kostnadsnivået. Innkjøp av systemer over kr. 100 000 eks. mva. styres av lov om offentlig anskaffelser, som har egne rutiner. Mindre innkjøp eller bruk av gratis digitale løsninger gjøres av enhetene selv. Kommunenes planer og strategier har rutiner som er felles for alle måter å ta i bruk nye systemer på, men også rutiner som spesifikt gjelder ved kjøp over terskelverdien på 100 000 kr eks. mva.

I Sandnes kommune sin «Arkitekturprinsipper for digitalisering[13]» beskrives *«[…] felles prinsipper og retningslinjer for utvikling og utforming av digitale tjenester»*. Dokumentet inneholder elleve prinsipper, hvorav sikkerhet er ett av flere prinsipper:

[13] arkitekturprinsipper-for-digitalisering-i-sandnes-kommune.pdf

Figur 1. Utdrag fra kommunens «Arkitekturprinsipper for digitalisering»

2.8 Sikkerhet

Forklaring	Sikkerhetsprinsippet skal sikre at offentlige IT-løsninger blir etablert og driftet på en sikkerhetsmessig god måte, samtidig som informasjon og tjenester er elektronisk tilgjengelig for de som har behov for og/eller rettigheter til disse. Enhver elektronisk tjeneste som etableres skal defineres til et gitt sikkerhetsnivå (klassifisering) basert på en risikoanalyse. Tjenesten skal konstrueres slik at sikkerhetsnivået kan endres ved behov. Sikkerhetsnivået må dokumenteres, slik at det blir helt klart for den som tar løsningen i bruk hvilke krav som er oppfylt. Krav om konfidensialitet, integritet og tilgjengelighet skal oppfylles. Sikkerhetsprinsippet kan begrense andre prinsipper, dersom dette er avgjørende for tilliten til offentlig sektor.
Konsekvenser	Sandnes kommune må kartlegge relevante krav til informasjonssikkerhet som følger av regelverk, instrukser og avtaler med tredjepart, og dokumentere at IT-løsningen oppfyller disse. I tillegg må virksomheten: • Kartlegge hvilket informasjonsinnhold løsningen skal omfatte • Ha definert et nivå for hvilken risiko som aksepteres • Gjennomføre en risikoanalyse av løsningen, basert på virksomhetens behov og egenart • Tilordne løsningen et passende sikkerhetsnivå • Implementere sikkerhetstiltak for IT-løsningen, som tilfredsstiller det sikkerhetsnivået som er besluttet • Teste at sikkerhetstiltakene fungerer som forventet IT-løsningens sikkerhetsnivå må kunne endres ved behov. Virksomheten må vurdere om, og i så fall hvordan, prinsippet om sikkerhet begrenser noen av de øvrige arkitekturprinsippene. Uavhengig av dette prinsippet eksisterer det både generelt og sektorspesifikt regelverk som den enkelte offentlige virksomhet må etterleve. Konkrete krav til gjennomføring følger av både regelverk, standarder for informasjonssikkerhet og sertifiseringsordninger

Sandnes kommune har laget en egen «Metodikk for arbeid med digitalisering, smartby og innovasjon»[14]. Et av prinsippene er å «ivareta innbyggernes personvern og redusere risiko for misbruk av data». Kommunen lister også opp tolv punkter som det skal jobbes med for å realisere hovedmålet om å forbedre tjenestene. Her er et av punktene er «Prioritering av informasjonssikkerhet og personvern».

[14] sandneshelt-enkelt-metodikk-for-arbeid-med-digitalisering-smartby-og-innovasjon.pdf

I Informasjonssikkerhetshåndboken – «Livsløp for informasjonsinnholdet i IT-løsninger» finner vi et dokument som beskriver oppgaver ved anskaffelse, forvaltning og avhending av IT-systemer. Ved anskaffelser skisserer dokumentet følgende krav og oppgavebeskrivelse:

- I anskaffelser skal det stilles krav om innebygd personvern som standardinnstilling
- Det skal utnevnes systemeier som er behandlingsansvarlig og er ansvarlig for oppgaver rundt forvaltning og risikoanalyse. Systemeier kan rådføre seg med personvernombudet.
- Systemeier er sammen med informasjonssikkerhetssjef ansvarlig for å gjennomføre ROS analyse. Det skal alltid vurderes om en DPIA skal utarbeides.

Kommunens overordnede styringsdokument for anskaffelser er «Anskaffelsespolitikk for Sandnes kommune» fra 2018. I dette dokumentet defineres roller og oppgaver i anskaffelsesprosesser. Ansvar for å ivareta personvernregelverket er ikke spesifikt beskrevet. Faglige ressurser utpekes av bestiller og danner et brukerutvalg som jobber sammen under anskaffelsesprosessen.

Tabell 2. Roller og oppgaver hentet fra «Anskaffelsespolitikk for Sandnes kommune (2018)

ROLLER	OPPGAVER
Bestiller	• Eier behovet • Premissgiver for anskaffelsen • Iverksette oppstart av anskaffelsesprosess i samarbeid med anskaffelsesenhet • Ansvarlig for å bemanne prosess med tilstrekkelig faglig kompetanse • Signerer kontrakt • Ansvarlig for oppfølging av kontrakt – ansvarlig for å utpeke en kontraktsansvarlig
Anskaffelsesenhet	• Eier anskaffelsesprosessen • Ansvarlig for å iverksette oppstart av anskaffelsesprosess i samarbeid med bestiller. • Ansvarlig for at prosessen planlegges og gjennomføres på en formålseffektiv og kostnadseffektiv måte i hht. rammebetingelser • Ansvarlig for at prosessdeltakerne får tilstrekkelig informasjon og inkluderes på en god måte • Ansvarlig for involvering av aktuelle interessenter • Ansvarlig for å sikre at prosessen gjennomføres i henhold til lov og forskrift • Godkjenner anskaffelsesplan
Faglig ressurser	• Ansvarlig for å sikre at kravspesifikasjonen ivaretar anskaffelsens formål innen alle aktuelle kompetanseområder • Bistå etter behov med planlegging og gjennomføring av prosessen. • Kvalitetssikre dokument før kunngjøring

Som del av anskaffelsesarbeidet utarbeides det også strategier for fireårsperioder som skal gi felles grunnlag for alle ansatte som er involvert i anskaffelser. Anskaffelsesstrategien 2018-2022 er generell for alle typer anskaffelser, men inneholder ingen beskrivelse av anskaffelser for systemer som behandler personopplysninger.

2.3 DATABEHANDLERAVTALE

Kommunens mal for databehandleravtale er tilgjengelig for ansatte på intranettet. Her beskrives det hva en databehandleravtale er, samt oppfordring om at: *«Alle brukere av malen anbefales på det sterkeste å sette seg inn i hva den krever av behandlingsansvarlige (kommunen) og databehandleren (leverandøren)»*. For spørsmål knyttet til databehandleravtalen henvises det til en ansatt i avdeling for anskaffelser.

Databehandleravtalen som kommunen bruker, er basert på mal fra rettsdata. Tilpasninger i malen er gjort av en egen arbeidsgruppe, «DBA-gruppen», som består av kommuneadvokat, personvernombud, informasjonssikkerhetssjef og rådgiver i anskaffelsesenheten (sistnevnte er ikke fast medlem). Tilpasninger ble ifølge en av de vi intervjuet gjort for å sikre kostnadsfri bistand fra leverandører for å oppfylle forpliktelser i henhold til personvernforordningen, hvor kommunen ikke selv kan oppfylle slike forpliktelser alene. Etter innføring av GDPR har anskaffelsesavdelingen, ifølge ansatt, hatt flere gjennomganger for å se på mulighet for databehandleravtale for allerede eksisterende avtaler. En har derimot ikke mulighet til å tvinge leverandører til å inngå kommunens databehandleravtale for eksisterende avtaler. De intervjuede viser til at det ikke alltid er mulig å få de større leverandørene til å bruke kommunens egen databehandleravtale.

Per september 2021 jobber DBA-gruppen med å lage en ny mal for databehandleravtale som bygger på Datatilsynet i Danmark sin standard (vedtatt av Datatilsynsmyndighetene i EØS). Det er ikke satt frist for når ny databehandleravtale skal være klar. Arbeidet har ikke blitt fullført grunnet permisjon, fravær og pandemi, og er satt på vent.

Innholdet i nåværende mal per 22.10.21 er av revisjonen sjekket opp mot DFØ sin sjekkliste og Datatilsynets anbefaling av innhold i databehandleravtale. Malen inneholder på overordnet nivå de krav som DFØ og Datatilsynet har satt for å ivareta krav i personvernforordningen.

2.4 ANSKAFFELSESPROSESSEN

Anskaffelsesenheten i kommunen ligger under økonomiavdelingen og er ansvarlig for alle innkjøp over kr. 100 000 eks. mva. Enheten anskaffer for eksempel fagsystemer, leiekontrakter, varer og tjenester knyttet til bygg og anlegg. Ifølge de intervjuede har den nye personvernforordningen ført til nytt fokus på personvern i anskaffelsesenheten og medført endringer i hvordan det jobbes.

I forkant av anskaffelser kan det gjennomføres markedsundersøkelser. Slike undersøkelser inneholder, ifølge de intervjuede, ofte spørsmål om hvordan leverandør ivaretar krav i personvernforordningen, fordi enheten erfaringsmessig opplever at markedet ikke alltid kan etterleve alle sikkerhetskrav kommunen ønsker å stille. Dersom kommunen stiller for spesifikke minimumskrav, kan man ende opp med at ingen leverandører kan levere, og at kommunen må avlyse konkurransen. I tilfeller hvor kommunen mistenker at markedet ikke kan levere på

spesifikke krav, blir kravene av og til formulert mindre spesifikt slik at alle sikkerhetskrav kan oppfylles på andre måter, for å unngå avvisning.

En av de intervjuede forteller at kommunen - som en del av anskaffelsesprosessen - finner anskaffelser fra andre kommuner på Doffin.no for å se hvordan de har gjennomført lignende konkurranser. Det hender at kommunen har møter med andre kommuner for erfaringsdeling. På et nylig erfaringsdelingsmøte med en annen kommune ble spørsmål om sikkerhet og etterlevelse av GDPR tatt opp.

I anskaffelsen stilles det sikkerhetskrav til leverandører. Kommunen bruker lister med krav hentet fra for eksempel DFØ, nasjonal sikkerhetshetsmyndighet (NSM) og Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Ansatt i anskaffelsesenheten oppgir at enheten jobber med å lage en egen liste basert på slike kilder. Et av kravene som stilles er at leverandør signere kommunens egen databehandleravtale. Her møter kommunen gjerne motstand i større anskaffelser. I likhet med kommunen, ønsker ikke store leverandører å måtte forholde seg til mange forskjellige avtaler med forskjellig innhold.

Det er varierende i hvilken grad anskaffelser behandler personopplysninger. Mange anskaffelser inneholder for eksempel kun kontaktinformasjon for ansatte i kommunen. I intervju med ansatt i anskaffelsesenheten fortelles det om praksis for å inngå databehandleravtale, selv om behandlingen av personopplysninger er begrenset til kun kontaktinformasjon til ansatt (som for eksempel mobilnummer som både er jobb- og privattelefon). Men at enheten hadde en avklaring rundt praksisen med Datatilsynet i 2021 hvor det kom fram at avtaler må omhandle behandling av personinformasjon utover jobbinformasjon/kontaktinformasjon for at det skal foreligge krav til databehandleravtale. Enheten har nå endret praksis i tråd med Datatilsynets vurdering.

Det er bestillende enhet som er ansvarlig for å inngå databehandleravtale med leverandør. Utfylling av databehandleravtale skjer i samarbeid mellom brukerutvalg og representant fra anskaffelser. I anskaffelsesprosessen er det ikke skriftlig rutine for at krav rundt databehandleravtale blir ivaretatt. Men flere av de intervjuede forteller at databehandleravtaler kommer opp som tema i anskaffelsesprosessen, enten som forslag fra anskaffelsesavdelingen eller at brukerutvalget etterspør databehandleravtale som del av forarbeidet. Når krav om databehandleravtale er med i anskaffelsen sikrer anskaffelsesavdelingen at avtalen signeres sammen med kontrakten.

Anskaffelsesenheten har ikke rutine på å sjekke at bestiller har vurdert eller gjennomført risikovurdering eller inngått databehandleravtale. Det er bestillende enhet som er ansvarlig for disse punktene, noe som kommunes rutiner også viser. Men det er ifølge ansatt i enheten vanlig praksis at anskaffelsesenheten foreslår at databehandler inngås der det er nødvendig. Brukerutvalget har, ifølge enhet for anskaffelser, fått mer kunnskap om plikter rundt GDPR, og etterspør gjerne databehandleravtale selv. Flere av de intervjuede sier at vurdering av databehandleravtale er godt innarbeidet i praksis for anskaffelser.

Registrering av systemer i Draftit er også en del av systemeiers/bestillende enhets ansvar. Ifølge de intervjuede, blir dette også ivaretatt av andre involverte, som gjerne etterspør Draftit-registrering.

Risikovurderinger i anskaffelsesprosesser gjøres av systemeier i samarbeid med brukerutvalget. Risikovurdering blir ifølge de intervjuede ofte diskutert som del av forarbeidet i en anskaffelse. DPIA gjennomføres via Draftit og gjøres med bistand fra informasjonssikkerhetssjef. En av de vi intervjuet forteller at kommunen kanskje kunne fått flere rutiner for personvern som helhet, blant annet for å klargjøre rammer for risikovurdering og når i prosessen DPIA skal gjennomføres.

En leder sier i intervju at utvikling av nye systemer som behandler personopplysninger kan gå litt seint. Det blir fort stort fokus på risiko ved nye systemer, samtidig som eldre systemer gjerne har større risikoer som ikke er vurdert. Lederen viser blant annet til diskusjon rundt SvarUt. I denne tjenesten kan mottaker delegere innkomne brev til andre. For eksempel kan sensitive opplysninger sendt til en lege være delegert videre til merkantilt ansatt, regnskapsfører eller lignende, noe som kan utgjøre en personvernrisiko. Alternativet for å unngå risiko blir gjerne at brev sendes fysisk, noe som reiser andre risikoer, og som ikke nødvendigvis er et bedre alternativ.

2.5 FAGLIGE RESSURSER I ANSKAFFELSER

Dokumentsenteret deltar som faglig støtte i anskaffelsesprosesser. Det er ikke skriftlig rutine for når dokumentsenteret skal involveres, men det er praksis for at de blir invitert inn i prosessen av den aktuelle bestillende enhet, av IT-avdelingen eller anskaffelsesavdelingen. Dokumentsenteret har blant annet vært involvert i anskaffelser av fagsystem i PPT, oppvekstadministrativt system og avvikssystemet Compilo.

Ifølge en ansatt blir personvernombudet involvert tidlig i anskaffelsen når det gjelder ny type behandling. Men, hvis anskaffelsen gjelder kopi av tidligere leveranse er det ikke alltid personvernombudet blir involvert. Personvernombudet informeres om planlagte innkjøp og kan stille kritiske spørsmål rundt ivaretakelse av personvern i systemene.

Informasjonssikkerhetssjef forteller i intervju at hun ikke alltid blir spurt om å delta i anskaffelsesprosesser, men at hun nå i større grad enn før blir invitert med. I det siste har hun vært med i anskaffelse av det nye saks- og arkivsystemet. Når informasjonssikkerhetssjef er med i anskaffelsesprosesser tar hun opp tema omkring informasjonssikkerhet i krav til leverandør.

Digitaliseringsenheten

Digitalisenheten skal ifølge kommunens måloppnåelse for tjenesteområdene (årsrapport 2020) være «[…] *en pådriver for endring og forbedring som skal koble kompetanse og ressurser slik at Sandnes kommune leverer bedre og mer effektive løsninger i nært samarbeid med innbyggere og andre partnere, og i tråd med målene i strategien Helt enkelt*» Enhetene er organisert sammen med IT som ifølge samme måloppnåelse skal støtte digitaliseringsprosjekter og digitale løsninger.

En ansatt i digitaliseringsenheten opplever at enheten stort sett har vært involvert i utvikling av nye systemer, men at de er en støttefunksjon og derfor avhengig av at den enkelte avdeling involverer dem. Digitaliseringsavdelingen involveres i prosjekter av ulike størrelser, fra store anskaffelser til bruk av mindre skytjenester. Enheten har ifølge ansatt vært involvert i ca. 5-10 fagsystem som behandler personopplysninger etter 2018. Enheten er i tillegg involvert i mange andre forvaltningssystemer og støtteapplikasjoner.

Digitaliseringsenheten jobber ut ifra arkitekturprinsippene til kommunen, som for eksempel innebygd personvern, minimert databehandling. Fra intervju får vi vite at vanlig framgangsmåte er å starte med lovgrunnlaget for behandlingen av personopplysninger for det konkrete systemet. Lovverket vil da styre hvilke kriterier som må ligge til grunn for å sikre krav til personvern. Utviklingsmessig handler dette, ifølge en ansatt, også om å redusere bruk av uavhengige kontaktregistre med ulik grad av oppdateringer. Ved å utvikle systemer koblet til sentrale registre vil man sikre at korrekt og oppdatert kontaktinformasjon brukes.

Ansatt i digitaliseringsenheten sier at enheten har et tett og godt samarbeid med anskaffelsesavdelingen, og peker blant annet på juridisk støtte som blir gitt av anskaffelsesavdelingen.

Faglige nettverk

Kommunen er med Digi Rogaland som er et samarbeid om felles digitale løsninger for innbyggere i Rogaland[15]. Alle kommunene i fylket deltar i dette samarbeidet sammen med statsforvalteren, fylkeskommunen og KS Rogaland. I samarbeidet er det opprettet flere faggrupper, deriblant faggruppe for Informasjonssikkerhet og personvern som ledes av informasjonssikkerhetssjef i Sandnes kommune. Kommunen er også med i KS sitt strategiske nettverk for informasjonssikkerhet og personvern (SNIP).

2.6 NYE SYSTEMER SOM IKKE ER EN ANSKAFFELSE

Kommunen tar også i bruk digitale løsninger som behandler personopplysninger utenom anskaffelsesrutiner. Dette er systemer som av kostnad ikke utløser krav rundt anskaffelser eller som er gratis. Personvernkrav er uansett de samme som for anskaffelser, og behandling av personopplysninger kan være omfattende (som Google sine gratisløsninger). Det er bestillende enhet som står for innkjøpet og som da har systemeieransvaret. Systemeier skal gjøre registrering i Draftit, inngå databehandleravtale og gjennomføre risikovurderinger. Kommunen har en lukket PC-løsning, noe som betyr at alle nye programmer som skal lastes ned må gjøres av IT-avdelingen.

[15] Digi Rogaland

Ifølge en av virksomhetslederne er det etter 2018 terpet på rutiner for å ta i bruk nye systemer på skolene. Digitale løsninger skal ikke tas i bruk før det er gjennomført ROS-analyse og inngått databehandleravtale.

En av de vi intervjuet, melder at det trolig ikke alltid er inngått databehandleravtale for systemer, men at det har vært økt fokus på dette kravet etter innføring av den nye personvernforordningen.

PPT benytter seg av flere digitale kartleggingsverktøy som ikke er del av anskaffelser, f.eks. evnekartleggingsverktøyene WISC, CAS og Celf. I intervju sier PPT-leder at kartleggingsverktøyene er registrert i Draftit og at de benytter de nyeste versjonene som også har oppdaterte personverninnstillinger. Personvernet ivaretas også av interne rutiner, som at kartlegginger som skrives ut på papir skal skannes inn i digitalt journalsystem og makuleres.

2.7 RISIKOVURDERINGER FOR NYE SYSTEMER

Kommunen har nylig innført en egen mal for risikovurdering. Det ble gjennomført risikovurderinger også før denne nye malen, med da ikke etter standardisert mal. DPIA gjennomføres via Draftit. Det finnes også mal for risikovurdering i avvikssystemet Compilo. Denne malen er mer dynamisk, ved at en kan delegere ansvar til ansatte, noe som gjør det lettere å følge opp risikovurderingen aktivt. Det er opp til hvert prosjekt å velge hvilken mal for risikovurdering som blir brukt. Men det er et ønske fra digitaliseringsenheten at malen i Compilo brukes ettersom oppfølging er vanskelig å gjøre med et «statisk» dokument.

I risikovurderinger legges det fram ulike scenarioer som vurderes etter konsekvens og sannsynlighet. Ifølge en av de intervjuede vil det ofte i risikovurderinger være tenkte hendelser med liten sannsynlighet, men med stor konsekvens. Slike hendelser blir fort satt til høye, «røde» risikoer, selv om sannsynligheten kan være lav.

En av de intervjuede påpeker at det ligger et forbedringspotensial i hvordan kommunen følger opp risikovurdering. En vanlig risiko er tilgang til systemet og utfordringer ved at brukere har tilgang til mer enn tjenstlig behov tilsier.

2.8 ENDRING AV SYSTEMER

Anskaffelsesenheten er, i etterkant av anskaffelsen, involvert i for eksempel kontraktsmessige endringer, prisjusteringer, endring av kontaktperson og konflikter rundt mislighold. Enheten har ifølge an av de vi intervjuet, ikke vært involvert i endringer av systemer som har konsekvenser for personvernet.

Tekniske endringer av systemer blir behandlet av avdeling for digitalisering og IT. Avdelingen benytter seg av Information Technology Infrastructure Library (ITIL) som er et rammeverk for å kvalitetssikre IT. En del av denne prosessen er Change Advisory Board (CAB) hvor tekniske endringer blir vurdert i felleskap på jevnlige møter. I CAB vurderes konsekvenser for både små

og større tekniske endringer. Ifølge ansatt blir personvern ivaretatt i slike vurderinger ved å blant annet følge anbefalingene i Normen[16] og at en gjennomfører ROS-analyser.

2.9 STØRRE ANSKAFFELSER SISTE ÅRENE

De siste årene har kommunen anskaffet et nytt oppvekstadministrativt system (IST) som dekker skole og barnehage. En av de intervjuede forteller at det i denne anskaffelsen ble inngått databehandleravtale og at mange sikkerhetskrav i anskaffelsen omhandler behandling av opplysninger, som for eksempel håndtering av kontaktopplysninger for personer på skjult adresse.

I 2019 startet kommunen anbudsprosess for nytt skybasert arkivsystem, som dokumentsenteret er prosjekteier og systemeier for. Status per oktober 2021 er at anbudet nylig har gått ut. I forkant av anbudet er det satt et absolutt krav til at leverandør må bruke kommunens databehandleravtale. Informasjonssikkerhetssjef har ifølge ansatt også kommet med andre krav til personvern i kravspesifikasjonen. Det er laget en liten risikovurdering for selve prosjektgjennomføringen, men ikke risikovurdering for selve løsningen, noe som vil bli gjort senere i prosessen ifølge ansatt.

PPT anskaffet et nytt digitalt journalsystem, Visma Flyt, i 2020. Visma Flyt er et journalsystem som flere andre PPT-tjenester bruker og har derfor de innebygde sikkerhetstiltak som trengs for å utføre lovpålagte tjenester. Systemet har to-faktor pålogging med bankID. Som en forbedring fra forrige journalsystem er det forbedret tilgangskontroll, hvor saksbehandlere kun har tilgang til de sakene de behandler. Det er heller ikke mulig lenger å hente ut f.eks. lister over elever med navn. Ifølge virksomhetsleder ble det i stilt krav til personvern i kravspesifikasjonen. I anskaffelsesprosessen ble systemet registrert i Draftit og det ble gjennomført ROS-analyse. Det foreligger også databehandleravtale

Informasjonssikkerhetssjef sier at skolene har anskaffet en del systemer hvor det ikke er kartlagt og vurdert personkonsekvenser og informasjonssikkerhet. Et eksempel er innføring av Google Suite Education hvor skolene fikk avvik for at det ikke var gjennomført en grundig nok konsekvensutredning før anskaffelsen. Avviket ble varslet til kommunen via Datatilsynet av foresatt ved en barneskole. Kommunen har nå gjennomført ROS-analyse og DPIA, slik Datatilsynet har bedt om, og avviket er nå lukket av Datatilsynet.

Velferdsteknologi

Sandnes har en egen *Strategi velferdsteknologi (2015 – 2020)*[17]. En av strategiene er at *«IT enheten skal involveres tidlig i prosessen ved vurdering av nye teknologiske løsninger. Alle IKT løsninger som vurderes anskaffet, må i henhold til Sandnes kommunes digitale strategi meldes til*

[16] Normen - ehelse

[17] strategivelferdsteknologi2015_2020.pdf (sandnes.kommune.no)

IKT-råd for vurdering. Tverrfaglige ROS analyser skal utføres, både som en del av anskaffelsesprosessen og i evalueringsfasen.». For helse- og omsorgstjenestene er det også laget en helhelhetlig tjenestemodell (vedlagt) som ifølge informasjon på intranett skal *«sørge for tydelig rolle- og ansvarfordeling på tvers av sektorene i kommunen»*. Modellen lister blant annet opp ti oppgaver for vedlikehold av tjenesten, hvorav en er å *«forvalte rutiner for personvern og informasjonssikkerhet»*.

Innen velferdsteknologi har kommunen, ifølge intranett, tatt i bruk digitale stasjonære trygghetsalarmer, mobile trygghetsalarmer med GPS funksjon og elektronisk medisineringsstøtte. Revisjonen har undersøkt registreringer i Draftit for disse tre systemene. Alle tre ble registrert i 2019 og sist endret i 2020.

2.10 VURDERING

Kommunen tar stadig i bruk nye digitale løsninger, og har blant annet anskaffet flere fagsystemer. Nye systemer er med på å høyne kvaliteten med tanke på personvern, ved at de fra leverandørsiden har oppdaterte løsninger som sterkere ivaretar krav til personvernet. Nye løsninger har også gjort det mulig å koble kontaktinformasjon til folkeregisteret, noe som sikrer at kontaktinformasjon er oppdatert.

Kommunen har egen mal for risikovurdering og databehandleravtale. Databehandleravtalen er en lokal tilpasning av mal fra rettsdata. Databehandlermalen ivaretar krav til personvern på en tilfredsstillende måte, ved at den inneholder krav satt av Datatilsynet og DFØ. Samtidig er det positivt at kommunen jobber med ny mal som skal bygge på mal vedtatt av Datatilsynsmyndighetene i EØS.

Større digitale løsninger gjøres som en anskaffelse. I denne prosessen involveres bestillende enhet og anskaffelsesavdelingen. I tillegg kobles det på ulike støtte/rådgiverfunksjoner fra ulike enheter. Det er bestillende enhet som er ansvarlig for å ivareta systemeierkravene til personvern. De intervjuede synes derimot, at personvern er noe alle involverte i anskaffelsesprosessen tar opp som tema. For eksempel settes det krav til leverandører at de skal ivareta spesifikke personvernkrav og bruke kommunens egen databehandleravtale. De intervjuede forteller det er etablert praksis for involvering av faglig støtte innen personvern og informasjonssikkerhet, men at dette ikke skrevet i egen rutine. De faglige støttene som brukes er digitaliseringsenheten, informasjonssikkerhetssjef, personvernombud og dokumentsenteret. Kommunen har egne arkitekturprinsipper for digitalisering som sammen med informasjonssikkerhetshåndboken lister opp konkrete krav som bruk av risikovurdering og databehandleravtale.

Ved anskaffelse av digitale systemer gjennomføres det risikovurderinger som et samarbeid mellom systemeier, brukerutvalg og faglig ekspertise på IT, informasjonssikkerhet og personvern. Slikt tverrfaglig arbeid sikrer god identifisering av risiko og treffsikre vurderinger. Retningslinjene til kommunen er klare på at systemeier er ansvarlig for registrering av systemer i Draftit. I anskaffelsesprosessen bidrar også andre deltakere med at nye systemer registreres her. Det synes å være god praksis for Draftit-registreringer i nyanskaffete systemer.

Kommunens enheter tar også i bruk digitale løsninger som ikke trenger å behandles som en anskaffelse. I slike prosesser er bestillende enhet mer alene om å ivareta personvernkrav, som å registrere systemet i Draftit, gjøre risikovurdering og skrive databehandleravtale. Ifølge de vi har intervjuet, har det blitt jobbet med å bevisstgjøre ledere på hvilket ansvar de har med bruk av nye digitale løsninger. Vår vurdering er at det er ut i enhetene at personvernkrav lett kan glippe. For eksempel tok skolene i bruk Google Suite Education uten å gjøre risikovurdering i forkant, noe som resulterte i avvik meldt til Datatilsynet.

3 KJENNSKAP TIL HÅNDTERING AV PERSONOPPLYSNINGER

Problemstilling: «I hvilken grad sikrer kommunen at ansatte er kjent med hvordan personopplysninger skal håndteres?»

3.1 REVISJONSKRITERIER

Etter personvernforordningen artikkel 24 skal kommunen ha organisatoriske tiltak for å ivareta informasjonssikkerhet og personvern. Ifølge Datatilsynets veileder for internkontroll skal kommunen lage rutiner som beskriver hvordan informasjon skal behandles for å oppfylle lovkrav [18]. Veilederen peker på at opplæring er viktig for å etterleve lovkravene: *«Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.»*.

I arbeidet med å etterleve personopplysningsloven inklusiv GDPR-forordningen skal personvernombudet bistå den enkelte virksomhet. Etter artikkel 39 skal personvernombudet; *«informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning, […]»*. Personvernombudet skal sørge for opplæring av personell som utfører behandlingsaktiviteter og gjennomføre holdningsskapende tiltak.

For å styrke de ansattes kjennskap til lovkravene knyttet til informasjonssikkerhet har Sandnes kommune valgt å utarbeide en egen informasjonssikkerhetshåndbok. Her står sentrale regler og retningslinjer beskrevet, nærmere bestemt regler som for behandling av informasjon for å vareta krav til personvern.

Ut fra disse føringene har vi utledet følgende revisjonskriterium (krav eller forventninger til kommunens arbeid):

Revisjonskriterier:

- Kommunen skal sørge for at de ansatte får opplæring i informasjonssikkerhet og personvern.

[18] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

3.2 OPPLÆRING

Personopplysningsloven av 15. juni 2018 innebærer en styrking av personvernet. Reglene gir kommunen en rekke plikter, samtidig som den gir enkeltpersoner en rekke rettigheter. I tråd med artikkel 37 i GDPR-forordningen (som igjen er en del av personopplysningsloven), har Sandnes kommune utnevnt et personvernombud. Ombudet i Sandnes kommune har som oppgave å:

- Informere om hvilke personopplysninger som blir samlet inn og hvorfor.
- Holde oversikt over opplysningene som behandles.
- Gi innsyn til den opplysningene gjelder.
- Kontrollere tilgangen til opplysningene.
- Be om samtykke fra de opplysningene gjelder før opplysningene blir behandlet.
- Beskytte informasjonen slik at den ikke kommer på avveier
- Vurdere risiko for sikkerhetsbrudd og konsekvenser.
- Slette personopplysninger det ikke lenger er behov for.

Personvernombudet mottar også henvendelser knyttet til personvern og informasjonssikkerhet. Dette gjelder både fra ledere, ansatte og innbyggere. Spørsmål fra ansatte kan være hvorvidt kommunen har lov til å hente inn opplysninger, hvor lenge kommunen skal sitte på disse og om behandlingen er sikker nok. Spørsmål fra innbyggerne handler ofte om innsyn i personopplysninger. Ifølge en av de intervjuede blir spørsmål om innsyn håndtert i tråd med kommunens rutiner for innsyn, og i praksis håndtert av Dokumentsenteret og den aktuelle enheten i kommunen, enten det er barneverntjenesten, byggesaksavdelingen eller andre instanser. De vi har intervjuet forteller at kommunens utnevnelse av et eget personvernombud har gjort det enklere å få svar på eventuelle spørsmål en enkelte måtte ha.

I kommunens spørreundersøkelse om informasjonssikkerhet ble ansatte og ledere spurt om de vet hvem som kan kontaktes ved spørsmål knyttet til informasjonssikkerhet og behandling av personopplysninger. Kun syv av de totalt 325 som svarte på undersøkelsen, oppgav at de ikke vet hvem som kan kontaktes. De aller fleste svarte nærmeste leder, mens 36 prosent av lederne og 23 av ansatte oppgav at de ville kontaktet personvernombudet.

Opplæring blant de ansatte ses på som et viktig tiltak for å sikre trygg håndtering av personinformasjon. I 2020 satte Sandnes kommune i gang e-læring innen informasjonssikkerhet for alle ansatte via KS læring, - et arbeid som har fortsatt inn i 2021. I henhold til kommunen er det et obligatorisk krav til alle ansatte om å gjennomføre dette e-læringskurset. Status for gjennomføring per 06.10.2021 er som følger:

- 2784 (34%) har gjennomført e-læringskurs og fått det godkjent/signert
- 356 (4%) har påbegynt eller venter på signering
- 5132 (62%) har ikke begynt på e-læringskurset

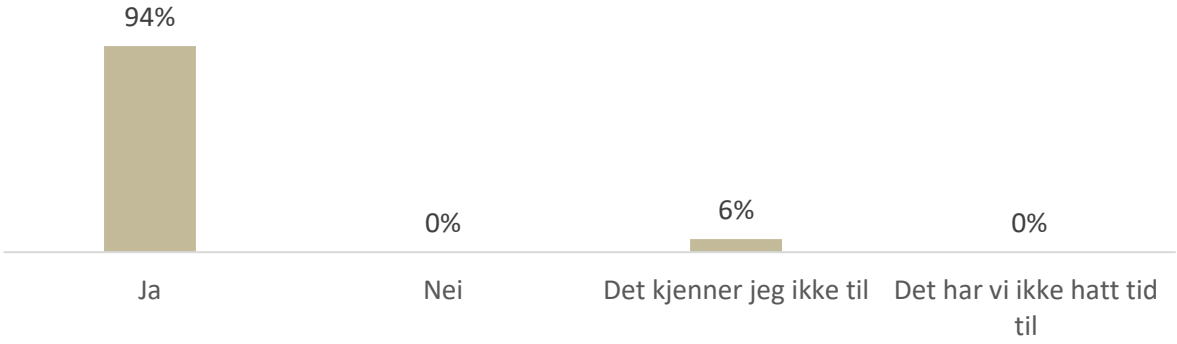
Alle ansatte er omfattet av prosentoversikten, inklusivt deltidsstillinger. Ambisjonsnivået er ikke 100 prosent, men informasjonssikkerhetssjef sier at kommunen jobber for å øke prosentandelen.

Kommunens opplæringsprogram, som er obligatorisk for alle nyansatte, har en egen modul for personvern og informasjonssikkerhet. Rutinen er at nyansatte skal gjennomføre e-læringskurs i informasjonssikkerhet, og at den nyansatte må skrive under på en egen sikkerhetsinstruks. Sistnevnte skal for øvrig også signeres av eksterne konsulenter og andre som gis tilgang til IT-relatert utstyr og systemer. Personvern er også et tema som gjennomgås årlig i kommunedirektørens ledergruppe.

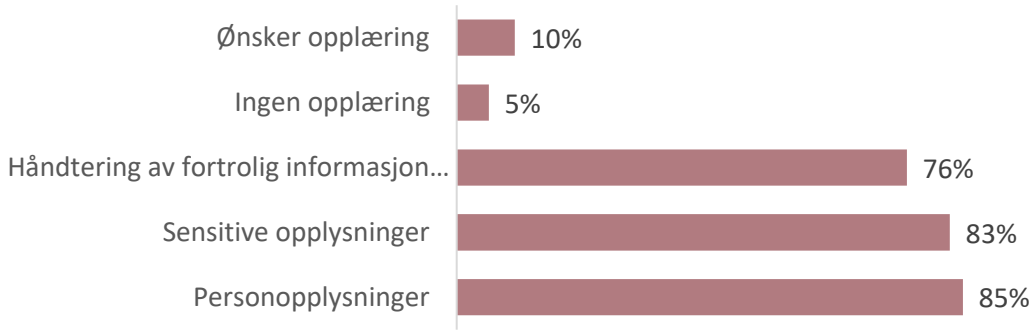
I tillegg til e-læringskurs har kommunen også andre opplæringstiltak i informasjonssikkerhet og personvern. Ved alle enhetene i kommunen, som for eksempel skoler og barnehager, er det utnevnt IKT-ansvarlige som skal ivareta opplæringen i enheten, sammen med ledelsen.

I kommunens spørreundersøkelse ble ansatte spurt om hva de har fått opplæring i, samtidig som lederne ble spurt om de har tilbudt ansatte opplæring. Både ledere og ansatte svarer i stor grad at det er gitt opplæring, mens ti prosent av de ansatte svarer at de ønsker opplæring.

Figur 2. Har dine ansatte fått opplæring i personvern og informasjonssikkerhet? N=50 (ledere) (Kilde: Sandnes kommune)



Figur 3. Har du fått opplæring i håndtering av: (flervalgspørsmål). N=275 (ansatte) (Kilde: Sandnes kommune)



Som nevnt har Sandnes kommune valgt å utarbeide en egen informasjonssikkerhetshåndbok, hvor gjeldende rutiner står beskrevet. Denne ligger tilgjengelig på kommunens hjemmeside[19]. I tillegg har kommunen utarbeidet et «Kompetanseprogram innen informasjonssikkerhet for alle ansatte», som skal være med å bidra til at ansatte får kjennskap til informasjonssikkerhetssystemet.

Den enkelte leder er gitt ansvaret for å sikre at ansatte er kjent med kommunens rutiner for informasjonssikkerhet. Lederne på alle nivå er bedt om å ha dette som tema på møter med sine ansatte. Informasjonssikkerhet er også et spørsmål i den årlige medarbeidersamtalen. Kommunen har utarbeidet en generell personvernerklæring som gjelder alle enhetene i kommunen, samt egne personvernerklæringer for skoler og barnehager.

De intervjuede forteller at de er kjent med informasjonssikkerhetshåndboken, som de som nevnt finner tilgjengelig på intranettet (kalt Pulsen). Kommunens spørreundersøkelse bekrefter at informasjonssikkerhetshåndboken er noe de fleste er relativt godt kjent med; 86 prosent av ansatte og 98 prosent av lederne svarer at de er kjent med håndboken. Spørreundersøkelsen viser også til at nesten alle (90-100 prosent) kjenner til kommunens passordregler og retningslinjer for bruk av e-post.

Tabell 3. Andel som har svart «ja», ansatte (N=275) og ledere (N=50) (Kilde:Sandnes kommune)

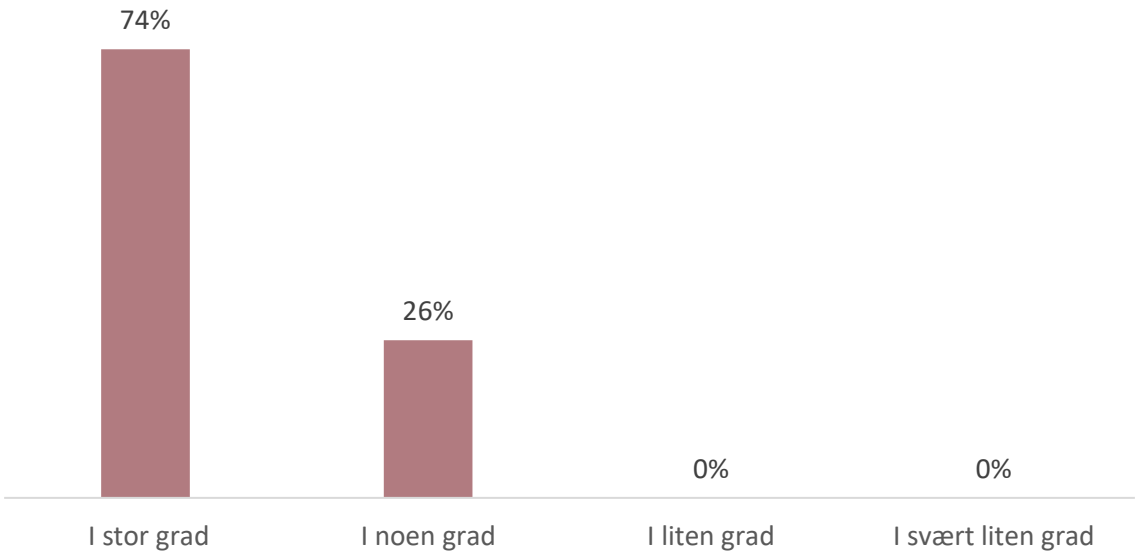
	Ansatt	Ledere
Er kjent med informasjonssikkerhetshåndboka	86 %	98 %
Kjenner til kommunens regler for passord og beskyttelse av ditt passord	93 %	100 %
Kjenner til kommunens retningslinjer for bruk av e-post	92 %	98 %

De generelle inntrykket fra intervjuer, er at ansatte opplever at kommunen i større grad enn tidligere retter sin oppmerksomhet mot personvern og informasjonssikkerhet etter innføringen av GDPR-forordningen. Utnevnelse av personvernombud og informasjonssikkerhetssjef har også bidratt til ekstra oppmerksomhet. Personvern og informasjonssikkerhet er tema som settes på agendaen på personal- og ledermøter med jevne mellomrom, fremheves det.

[19] https://www.sandnes.kommune.no/politikk-og-administrasjon/styringsdokumenter-og-planer/planer-a-a/informasjonssikkerhetshandbok/

I kommunens spørreundersøkelse ble lederne spurt om i hvilken grad det er klart hvilket person- og informasjonssikkerhetsansvar som ligger i stillingen. I undersøkelsen svarte 74 prosent at de i stor grad synes at ansvaret er klart. Ingen av de femti lederne svarte «i liten grad» eller i «svært liten grad» på dette spørsmålet.

Figur 4. Svar på spørsmål: «Er det klart for deg hvilket person- og informasjonssikkerhetsansvar som ligger til din stilling/rolle?» N=50 (ledere) (Kilde: Sandnes kommune)



3.3 VURDERING

For å sikre riktig behandling av personopplysninger, er det nødvendig å gi ansatte tilstrekkelig informasjon og opplæring. Kommunen har en oversiktlig informasjonssikkerhetshåndbok som er tilgjengelig på kommunens nettsider, og på intranett. Håndboken gir konkret beskrivelse av hvilke krav til personvern både ansatte og ledere har. Inntrykket fra intervju og resultat fra kommunes egen spørreundersøkelse, er at informasjonssikkerhetshåndboken er godt kjent.

De intervjuede forteller om en økende bevissthet om personvern etter innføringen av GDPR, noe som vurderes som positivt.

Spørreundersøkelsen viser at det i stor grad er gitt opplæring i personvern og informasjonssikkerhet i enhetene Oppvekst barn/unge, Oppvekst skole og Organisasjon. I intervju med ansatte og ledere fra andre enheter, får vi samme inntrykk. Opplæringen har blitt gjort på ulike måter; på skolene har IKT-ansvarlig eget opplegg, og andre enheter har deltatt på eksterne kurs.

En del enheter har også brukt e-læringskurset som ble igangsatt i 2020 gjennom KS læring. Gjennomføring av kurset er obligatorisk for alle ansatte, og deltakelse blir registrert. Vi vurderer det som positivt å innføre felles, obligatorisk kurs, som sikrer lik kompetanseheving for hele organisasjonen. Status per oktober 2021 er at kun 34 prosent av de ansatte har gjennomført

kurset. Etter vår vurdering er denne prosentandelen lav, og kommunen bør vurdere tiltak for å få denne andelen opp.

Det er også positivt at kommunen gjennomfører spørreundersøkelser, som gir oversikt over kompetansenivået innen informasjonssikkerhet og personvern. På denne måten kan kommunen avdekke områder som ansatte trenger mer informasjon eller opplæring i.

Revisjonen kommer med følgende anbefalinger til kommunen:

- Kommunen bør øke gjennomføringsgraden for e-læringskurset for personvern og informasjonssikkerhet

4 ETTERLEVELSE AV PERSONVERNREGLER

Problemstilling: «I hvilken grad oppbevarer, behandler og sletter virksomhetene personopplysninger i henhold til regelverket?»

4.1 REVISJONSKRITERIER

Lov om behandling av personopplysninger med personvernforordningen (GDPR) gir virksomhetene juridiske forpliktelser ved behandling av personopplysninger[20]. Kommunen skal etter artikkel 6 ha et grunnlag for behandling av personopplysninger. Behandlingsgrunnlaget kan være å innhente samtykke fra den registrerte person. Ved bruk av samtykke, skal behandlingsansvarlig kunne dokumentere at samtykke er gitt. I henhold til artikkel 7 har den registrerte rett til å trekke tilbake sitt samtykke. Uten samtykke må det vises til andre lovlige grunnlag som f.eks. at behandling er nødvendig av hensyn til viktige allmenne interesser. I tillegg må kommunen fastsette formålet med behandling av personopplysninger (artikkel 6). Formålet med behandlingen er for øvrig styrende for hvor lenge opplysningene kan oppbevares.

Behandling av personopplysninger skal skje på en åpen måte, noe som innebærer at de registrerte personene skal informeres om deres rettigheter (artikkel 12-14). De registrerte har som hovedregel rett til innsyn, retting og sletting av personopplysninger (artikkel 15-17). Og kommunen skal senest innen én måned behandle henvendelser som gjelder registrertes rettigheter (artikkel 12).

Ansvaret for å etterleve disse kravene er lagt til behandlingsansvarlig i virksomheten. I henhold til GDPR-forordningen artikkel 30 skal behandlingsansvarlig også føre protokoll over behandlingsaktiviteter for personopplysninger.

Revisjonskriterier:

- Kommunen skal føre oppdatert protokoll over behandling av personopplysninger
- Kommunen skal gjennomføre risikovurderinger
- Kommunen skal ha rutiner for sletting
- Behandling av personopplysninger skal loggføres
- Offentlig journal skal ikke inneholde sensitiv informasjon

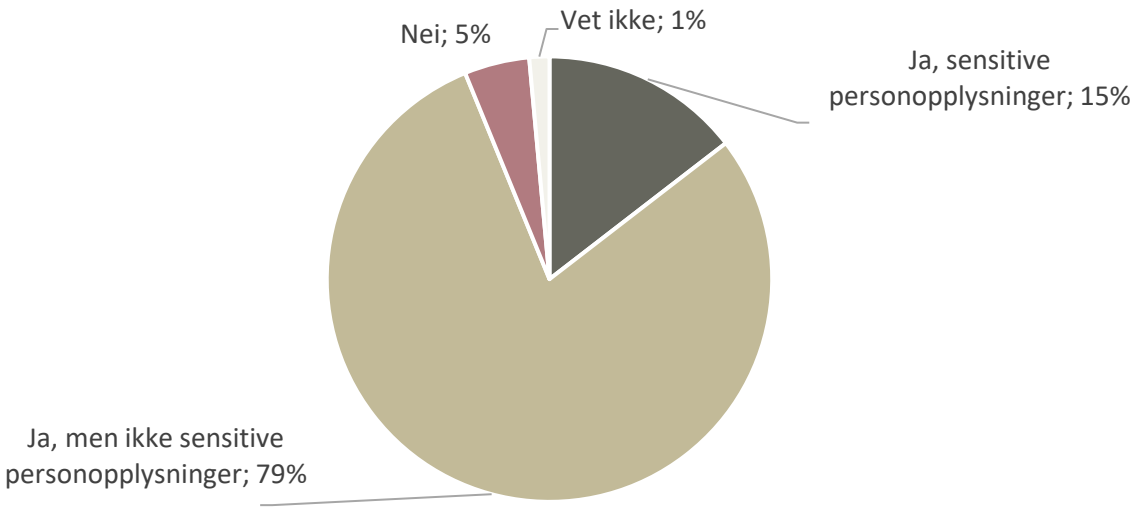
[20] Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata

- Taushetsbelagte opplysninger skal ikke sendes på e-post, såfremt disse ikke er avpersonifisert eller sendes kryptert.

4.2 KOMMUNENS OVERSIKT OVER OPPBEVARING, BEHANDLING OG SLETTING AV PERSONOPPLYSNINGER

Ansatte i kommunen behandler i stor grad personopplysninger som en del av sitt arbeid. Kommunens egen undersøkelse viser at 79 prosent av de ansatte behandler personopplysninger som ikke er sensitive, mens 16 prosent behandler sensitive personopplysninger.

Figur 5. Svar på spørsmål: «Behandler du personopplysninger i arbeidet ditt?». N=275 (ansatte) (Kilde: Sandnes kommune)



I 2018 tok Sandnes kommune i bruk systemet Draftit, som er et verktøy for å få en samlet oversikt over hvilke personopplysninger kommunen behandler, og hvilke datasystemer kommunen har som inneholder personsensitive opplysninger. Behandlingsansvaret for Draftit er lagt til kommunens informasjonssikkerhetssjef og personvernombud.

Sistnevnte skal blant annet kontrollere at kommunens systemer blir registrert i Draftit, noe som gjøres overfor ansatte med lederansvar. Per oktober 2021 er ikke alle systemene kommunen bruker registrert i Draftit. Dette gjelder blant annet enkelte skytjenester som benyttes ute på skolene.

Med Draftit er det mulig å holde oversikten over hvorvidt det er gjennomført en risikovurdering av det enkelte datasystem, og hvor risikovurderingen eventuelt ligger lagret. Selve risikovurderingen legges ikke i Draftit ettersom det ikke skal lagres sensitive opplysninger i en skyløsing.

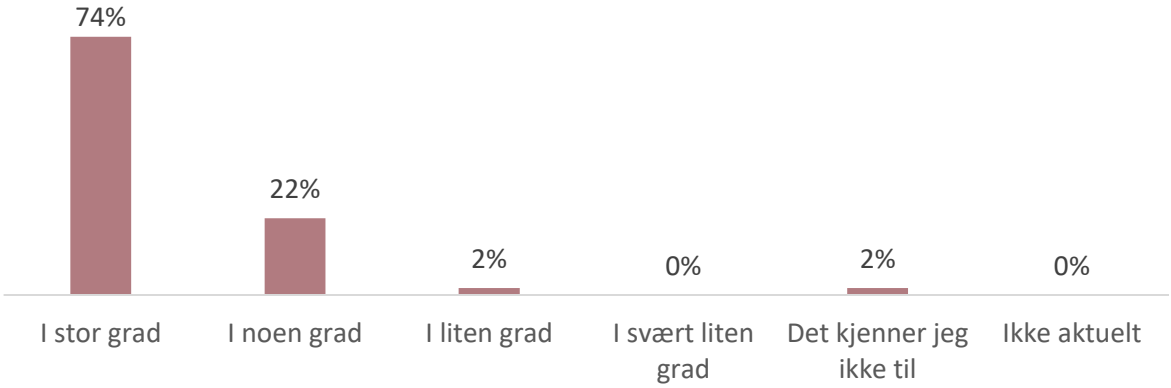
I Compilo finner vi maler for utarbeidelse av risikovurderinger, men disse benyttes i varierende grad. Siden malen for risikovurdering i Compilo krever noe kunnskap om dette programmet, og således har vist seg å være vanskelig å bruke, har informasjonssikkerhetssjef utarbeidet en alternativ mal i programmet Excel. På spørsmål om hvorfor kommunen har to ulike maler for utarbeidelse av risikovurderinger, forteller informasjonssikkerhetssjefen at malen i Excel er enklere å bruke, og at det er flere ansatte som er kjent med dette programmet. For kommunen er det viktigere at risikovurderinger blir gjennomført, enn at de ansatte benytter samme mal, poengterer informasjonssikkerhetssjefen.

Personvernombudet fremhever at Draftit gir muligheter til å kvalitetssikre kommunens arbeid med personvern og informasjonssikkerhet i større grad enn hva som er tilfelle per i dag. Eksempelvis vil det være mulig å sjekke hvorvidt det er utarbeidet risikovurderinger eller DPIA'er for det enkelte fagsystem. Dette er kontroller som ikke utføres per i dag.

I kommunens overordnede risiko- og sårbarhetsanalyse fra 2020 er risiko for en informasjonssikkerhetshendelse ett av flere punkter. Her er risikoen satt til «gult» nivå. Foreslåtte tiltak i ROS-analysen er blant annet kompetanseheving for nøkkelpersonell som arbeider mye med informasjon/sensitive data. Ifølge ROS-analysen er det laget en oppfølgingsplan for å sikre at tiltak blir gjennomført, og for å sikre fremdrift. Oppfølgingsplanen evalueres hvert år.

På spørsmål om hvilke barrierer som eventuelt forhindrer ansatte å følge rutiner og praksis svarer flere av de intervjuede «en travel hverdag». De intervjuede fremhever at det er viktig å bli minnet om personvernreglene og rutiner for overholdelse av disse med jevne mellomrom «for å få disse inn i ryggmargsrefleksen». Dersom systemer blir for tungvinte, kan man fort bli fristet til å velge den letteste veien, fremheves det.

Figur 6. Svar på spørsmål: «Har du som leder oversikt over din virksomhets behandling av personopplysninger?» N=50 (ledere) (Kilde: Sandnes kommune)

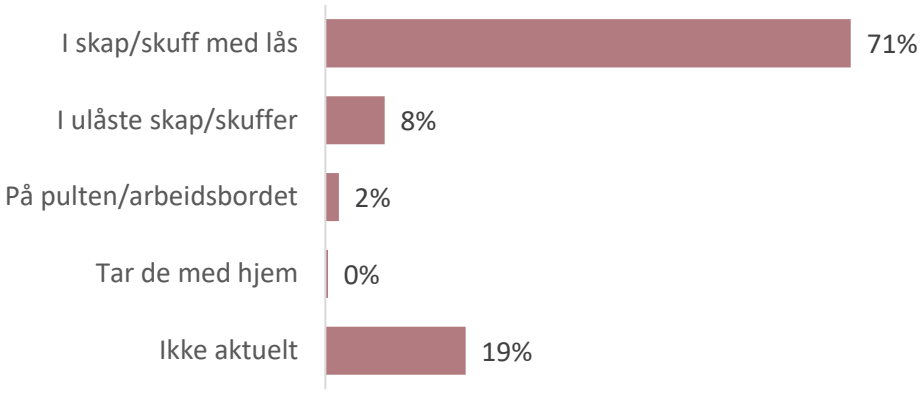


Av de femti lederne som har svart på kommunens spørreundersøkelse, svarer 74 prosent at «de i stor grad»- og 22 prosent «i noen grad», har oversikt over virksomhetens behandling av personopplysninger.

Et annet spørsmål lederne ble spurt om var «hvilke IT-systemer er din virksomhet ansvarlig for /systemeier for». Av de 50 lederne som svarte på undersøkelsen, svarer halvparten at de har systemeieransvar, og lister opp systemer i eget fritekstfelt. Elleve av lederne har listet opp system de har et overordnet eieransvar for (dette gjelder for eksempel Microsoft, Visma Enterprise, Public 360), selv om det i dette spørsmålet ble presisert at IT-systemer med overordnet eieransvar ikke skulle inkluderes.

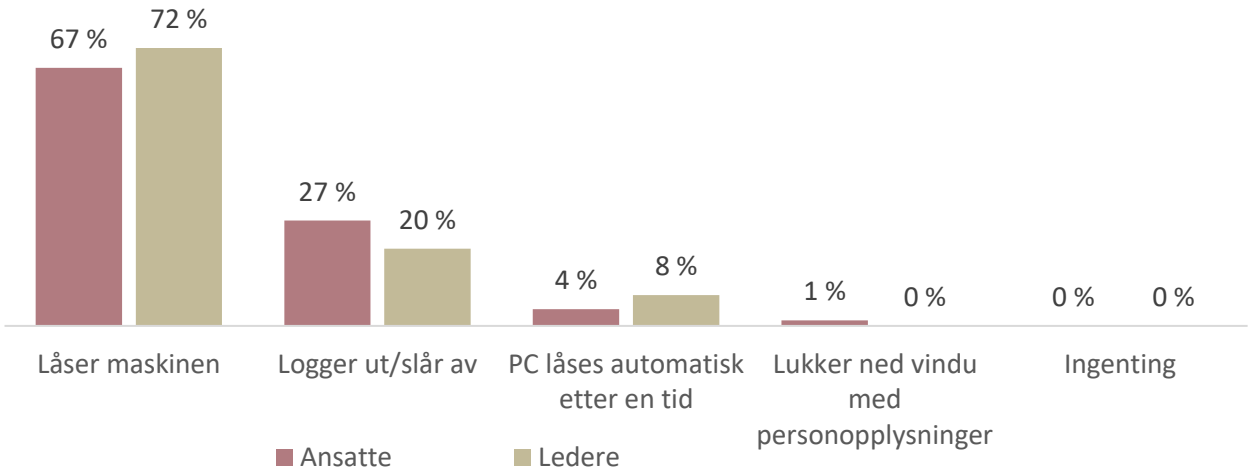
Flere av de intervjuede forteller at de oppbevarer opplysninger i papirform, men at de har rutiner som sikrer at disse oppbevares trygt. Blant de intervjuede er det flere som forteller at de benytter papirdokumenter i en kortere fase i behandlingen av den sak, men at dokumentene blir makulert. I det daglige blir dokumentene låst inne, og de ansatte forteller at de ikke lar disse dokumentene ligge åpent på pulten dersom man forlater kontoret. Spørreundersøkelsen bekrefter også at de fleste oppbevarer sensitive papirdokumenter på sikker måte i låsbare skap eller skuffer.

Figur 7. Svar på spørsmål: «Hvordan oppbevarer du papirdokumenter med fortrolig informasjon?». N=275 (ansatte) (Kilde: Sandnes kommune)



I informasjonssikkerhetshåndboken slås det fast at *«Når ansatte forlater PC-en, nettbrett, mobiltelefon m.m., skal skjermen låses»*. Spørreundersøkelsen viser også at de aller fleste ansatte og ledere låser eller slår av maskinen når de forlater arbeidsplassen (jamfør figur 8).

Figur 8. Svar på spørsmål: «Hva gjør du når du forlater PC' en din?» ansatte (N=275) og ledere (N=50) (Kilde: Sandnes kommune)



Rutiner for kommunikasjon av sensitive opplysninger

Ved behov for å kommunisere taushetsbelagte opplysninger internt benyttes saks- og arkivsystemet Public 360. For å kunne kommunisere kreves det her at begge parter har tilgang.

I henhold til kommunens informasjonssikkerhetshåndbok skal ikke epost benyttes til å sende taushetsbelagte opplysninger. Det hender at kommunen mottar e-post med personopplysninger, som kommunen ønsker å besvare. De intervjuede forteller at i slike tilfeller blir eventuelle kjennetegn fjernet fra eposten før den sendes, slik at det ikke skal være mulig å koble opplysningene til bestemte personer. Personvernombudet opplyser at kommunen er på utkikk etter løsninger som kan erstatte bruken av epost når behovet for utveksling av personopplysninger melder seg.

Kommuneadvokaten forteller at når de jobber med en sak, henter de opplysningene direkte fra den aktuelle virksomhetens fagsystem, enten det gjelder barnevern, skole, helse eller andre tjenesteområder. At kommuneadvokaten selv går inn og henter opplysningene, etter tillatelse fra virksomheten, reduserer behovet for å sende taushetsbelagte opplysninger mellom instanser internt. Når det gjelder kommunikasjonen mellom kommunen/ kommuneadvokaten og statlige instanser foregår denne stort sett gjennom statlige, digitale portaler. Dette gjelder for eksempel domstolene og fylkesnemnda.

Loggføring

All aktivitet i kommunens saks- og arkivsystem blir loggført. Loggen gir oversikt over hvilke ansatte som har, lest, endret eller slettet opplysninger, og i hvilke saker. Store fagsystemer som blir benyttet innenfor de ulike tjenesteområdene har også slik funksjonalitet. Dette gjelder blant annet fagsystem fra Visma innenfor oppvekst og helse. En av de intervjuede forteller at de foretar stikkprøver av loggen i kommunens fagsystem innenfor helsesektoren. Men det er også flere av de intervjuede som forteller at de ikke har rutiner eller praksis for å foreta kontroll av logg.

Etterlevelse på virksomhetsnivå

I forbindelse med prosjektet har vi intervjuet virksomhetsledere innenfor Helse og velferd, samt Oppvekst skole og Oppvekst barn og unge. Blant de intervjuede er oppfatningen at kommunens datasystemer ivaretar personvernet og informasjonssikkerheten på en god måte. Samtidig er opplæring av de ansatte noe må ha et kontinuerlig fokus på, ifølge dem vi har snakket med.

Leder for Barne- og familieenheten er systemeier for fagsystemene «VISMA Familia» og «VISMA Flyt". Den enkelte virksomhetsleder ved kommunens sykehjem er ikke systemeier eller behandlingsansvarlig for noen datasystemer. Her benyttes Visma Profil, og systemansvaret er lagt til kommunaldirektørnivå. Den enkelte virksomhet har utnevnt superbrukere som skal bistå andre ansatte i spørsmål knyttet til informasjonssikkerhet og personvern.

De ansatte behandler opplysninger som det kreves samtykke for å behandle. Selve samtykket innhentes på søknadstidspunktet. Dette skjer ved at i skjemaet som fylles ut ved søknad om tjenesten, skriver søker under på at kommunen kan innhente personopplysninger. Innhenting av samtykke anses som helt nødvendig for å kunne gi forsvarlige tjenester.

PP-tjenesten og barneverntjenesten har nylig satt i gang et arbeid for å få skannet inn/ overførte fysiske arkiv til elektronisk arkiv. Innenfor andre deler av kommunens tjenesteapparat er det flere som oppgir at de fremdeles oppbevarer personopplysninger/fortrolig informasjon i papirform. Noe av grunnen til dette er at det fremdeles er mulig å fylle ut søknader om tjenester på papir. Dessuten er flere av journalsystemene/ fagsystemene, som for eksempel Profil, ikke å regne som et godkjent, fullverdig elektronisk arkivsystem. Ved den enkelte virksomhet, som for eksempel kommunens sykehjem, finnes det derfor ennå arkiv hvor journaler blir oppbevart i papirform.

De intervjuede forteller at fysiske mapper med personopplysninger oppbevares i låste rom. Mens noe informasjon er lagret *både* i papirform og elektronisk, ligger annet kun elektronisk. Vi får opplyst at kommunen har satt i gang et arbeid for å redusere omfanget av dokumenter på papir, men så lenge kommunen mottar søknader på papir, er dette utfordrende å få til. Kommunen har i dette satt i gang et arbeid med å få implementert en løsning for mottak av ikke- elektroniske søknader, som vil gjøre det mulig å redusere omfanget av papirdokument.

Virksomhetslederne vi har intervjuet forteller at de har utarbeidet egne rutiner for sletting. Ved dødsfall blir fysiske mapper overført til kommunens sentralarkiv, hvor disse blir oppbevart i ti år, i tråd med arkivlovens bestemmelser. Ved dødsfall, blir tilgangene de ansatte har, slettet[21]. Skulle det vise seg å være behov for å hente ut opplysninger i etterkant, eksempelvis etter forespørsel fra pårørende, vil det kun være ansatte med utvidede fullmakter som fortsatt har tilgang.

[21] Det er kun tilgangene som blir slettet, ikke dokumentasjonen.

På spørsmål om hvilke risikoområder som gjør seg gjeldende på et sykehjem, nevner virksomhetsleder et par eksempler. Besøkende på sykehjem kan gjerne spørre personal om hvordan det går med vedkommende. Med mindre den besøkende er pårørende, skal det ikke gis informasjon om helsetilstand. Da er det viktig at den ansatte ikke oppgir personopplysninger, men samtidig ivaretar forespørselen på en høflig måte. I alle tilfeller er det viktig at den ansatte sjekker hvem som er oppgitt som pårørende.

Tabell 4. Resultat fra spørreundersøkelse etter enhet. N=50 (ledere) (Kilde: Sandnes kommune)

Spørsmål	Svaralternativ	Oppvekst barn og unge	Oppvekst skole	Organisasjon	Totalsum
Registrerer dere behandlinger/ protokoll over personopplysninger i Draftit?	Ja	80 %	0 %	83 %	**50 %**
	Nei	12 %	32 %	0 %	**18 %**
	Det kjenner jeg ikke til	8 %	68 %	17 %	**32 %**
	Totalsum	100 %	100 %	100 %	**100 %**
Har dere databehandler-avtaler for de IT-systemene hvor dette er et behov?	Ja	52 %	37 %	33 %	**44 %**
	Nei	16 %	11 %	0 %	**12 %**
	Vet ikke	16 %	26 %	50 %	**24 %**
	Annet	16 %	26 %	17 %	**20 %**
	Totalsum	100 %	100 %	100 %	**100 %**
Gjennomfører dere risikovurderinger av personvern-konsekvenser for IT-systemer dere er eiere av?	Alle	24 %	5 %	0 %	**14 %**
	De fleste	12 %	11 %	17 %	**12 %**
	Noen	16 %	21 %	17 %	**18 %**
	Ingen	32 %	26 %	17 %	**28 %**
	Ønsker veiledning	16 %	37 %	50 %	**28 %**
	Totalsum	100 %	100 %	100 %	**100 %**

I spørreundersøkelsen ble ledere spurt om de hadde registrert fagsystemene de benytter i Draftit, hvorvidt det foreligger en databehandleravtale og om det er utarbeidet risikovurdering. Undersøkelsen viser at Oppvekst skole i liten grad har fulgt opp systemeieransvaret. Ingen av de 19 lederne i skolen hadde gjort registreringer i Draftit på tidspunktet for undersøkelsen.

I tillegg til skole svarer også de seks lederne fra Organisasjon at det i liten grad er inngått databehandleravtale. Av de 22 lederne som svarer at de har databehandleravtale, svarer 19 at de vet hvor databehandleravtalen ligger lagret; i Public 360, i fagsystemet eller hos enhet for anskaffelser. Tre ledere er usikre på hvor databehandleravtalen ligger lagret.

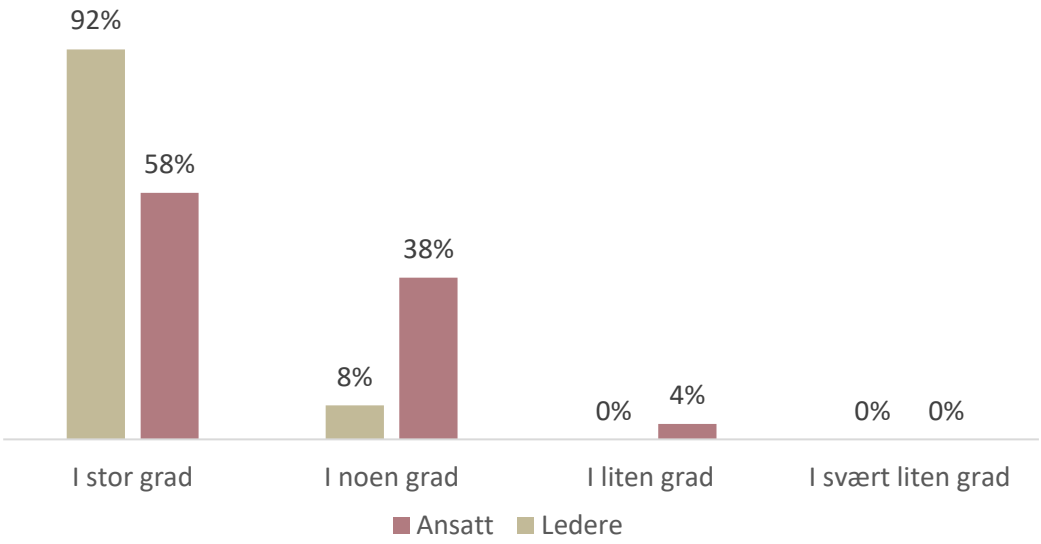
På spørsmål om gjennomføring av risikovurdering av personvernkonsekvenser ser vi at en del, nærmere bestemt 28 prosent, ikke har gjort dette. Samtidig er det om lag samme antall som ønsker veiledning om hvordan man gjennomfører en risikovurdering.

Grad av gjennomføring av oppgaver knyttet til systemeieransvar kan si noe om det generelle fokuset på behandling av personopplysninger i enhetene. De 275 ansatte som svarte på undersøkelsen sier i stor grad at behandling av personopplysninger er tema i medarbeidersamtaler, avdelingsmøter eller lignende. Men her ser vi større forskjeller mellom de tre enhetene som var med i undersøkelsen; ansatte i Oppvekst barn og unge svarer i større grad «ja» på spørsmålet enn Oppvekst skole. De intervjuede forteller om økt fokus på personvern i barnehagene, mens skolene har vært mer bakpå.

Figur 9. Svar på spørsmål: «Er behandling av personopplysninger et tema i medarbeidersamtaler, avdelingsmøter eller lignende?». N=275 (Ansatte) (Kilde: Sandnes kommune)

På spørsmål om det er fokus på personvern i kommunen, svarer hovedvekten av ledere og ansatte at det i stor grad er det. Ledere i større grad enn ansatte. Også på dette spørsmålet peker ansatte i Oppvekst skole seg ut, ved at det er flere her som svarer at det i liten grad er fokus på personvern, enn ansatte på andre avdelinger.

Figur 10. Svar på spørsmål: «Er det et godt fokus på personvern i kommunen?» ansatte (N=275) og ledere (N=50) (Kilde: Sandnes kommune)



4.3 BEHANDLINGSPROTOKOLL

I forbindelse med forvaltningsrevisjonen har vi foretatt kontroll av fire tilfeldig valgte fagsystem registrert Draftit. Dette er gjort i samråd med informasjonssikkerhetsjef. De fire fagsystemene er;

- VISMA Flyt (PP-tjenesten),
- VISMA profil (Helse & velferd),
- Familia (barneverntjenesten)
- LOGOS (grunnskolene og PP-tjenesten).

Disse fagsystemene ble valgt ut på bakgrunn av omfanget av personopplysninger som finnes i dem. Kontrollen ble utført 23.09.2021 og omfattet følgende forhold i det enkelte fagsystem:

- Inneholder fagsystemet kontaktopplysninger til fagansvarlig for dette aktuelle systemet?
- Er formålet med fagsystemets behandling av personopplysninger registrert?[22].
- Er det gitt en beskrivelse av kategoriene av registrerte personopplysninger? Dette kan være navn, personnummer, helseopplysninger etc.
- Foreligger en databehandleravtale knyttet til det aktuelle fagsystemet?
- Er det utarbeidet en risikovurdering for det aktuelle fagsystemet?

[22] Formålet er for eksempel å utføre lovpålagte tjenester som tilpasset opplæring. I dette tilfellet er det opplæringsloven som er rettslig grunnlag for behandlingen.

Tabell 5. Oversikt over resultater etter kontroll av fire fagsystem i Draftit. Utført 23.09.2021

	VismaFlyt (PPT)	Visma Profil (Helse/velferd)	Familia (barnevern)	Logos (PPT/Skole)
Kontaktopplysninger til behandlingsansvarlig	Ja	Ja	Ja	Ja
Beskrivelse av formålet med behandlingen	Ja	Ja	Ja	Ja
Beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger	Ja	Ja	Ja	Ja
Databehandleravtale	Ja	Ja	Ikke aktuelt[23]	Se punkt under
Risikovurdering og/eller DPIA	Ja	Ja	Ja	Nei

Kontrollen avdekker følgende:

- Hver enhet (PP-tjenesten og den enkelte skole) har egne databehandleravtaler med LOGOS. For å få oversikt over databehandleravtaler og eventuelle risikovurderinger og/eller DPIAer som er gjennomført her, må dette undersøkes med den enkelte skole.

4.4 ARKIVERING OG OFFENTLIGGJØRING

Som nevnt innledningsvis gjennomførte Rogaland revisjon en forvaltningsrevisjon om informasjonssikkerhet, drift og sårbarhet i 2018/19. Her ble både arkivplan, rutiner rundt arkivering og praksis rundt arkivering og offentliggjøring av dokumenter med

[23] Databehandleravtale er ikke nødvendig siden systemet er en installasjon på kommunes lokale servere.

personopplysninger og sensitiv informasjon, vurdert. Revisjonen skrev da følgende: *«Arkivplanen til Sandnes kommune er blitt oppdatert etter tilsynsrapport fra Arkivverket. De systemansvarlige i Sandnes kommune har høy kunnskap om hva som regnes som arkivverdig materiale og mener praktiseringen av dokumentbehandling og arkivering i enhetene i stor grad er tilfredsstillende.»*[24]

Leder for Dokumentsenteret forteller i intervju at all publisering på offentlige postlister gjøres av Dokumentsenteret. Dokumenter som skal publiseres går gjennom to kvalitetssjekker for å hindre at sensitiv informasjon kommer ut på postlisten. Det hender at manglende skjerming oppdages under kvalitetskontroll, men i slike tilfeller rettes feilen opp før dokumentet publiseres.

Kontroll av postliste

Revisjonen har foretatt en kontroll av postlisten på tolv små og store barnehager og skoler i kommunen. I kontrollen sjekket vi hvorvidt saker i en utvalgt uke inneholdt sensitive opplysninger, som for eksempel navn, fødselsdato eller personnummer.

Tabell 6. Kontroll postliste for et utvalg barnehager og skoler i Sandnes kommune

Enhet	Antall saker på postlisten i en utvalgt uke	Antall saker med manglende skjerming
Tre barnehager	13	0
Fire barneskoler	27	0
Tre kombinerte 1-10. trinn skoler	22	0
To ungdomsskoler	5	0

Som det fremgår av tabellen, foretok revisjonen en kontroll av totalt 67 saker. Revisjonen fant ingen personopplysninger eller sensitive opplysninger i disse sakene.

I dette prosjektet har vi ikke foretatt noen kontroll for innsynsbegjæringer, men i tidligere revisjon ble det i spørreundersøkelsen spurt om dette. I denne svarte 26 prosent at de hadde mottatt innsynsbegjæringer og 56 prosent at de hadde rutiner for dette i fagsystemet (27 systemansvarlige svarte på undersøkelsen). I kommentarfeltet til spørreundersøkelsen svarte flere

[24] Rapport Rogaland Revisjon IKS (rogaland-revisjon.no)

at innsynsbegjæringer blir håndtert tilfredsstillende, og at kommuneadvokaten kan kontaktes dersom man er usikker.

Fra leder av Barne- og familieenheten blir det i dette forvaltningsrevisjonsprosjektet meldt om et omfattende arbeid knyttet til innsynsbegjæringer. Ved ønske om innsyn, må enheten ta stilling til hva som skal slettes før utlevering. Leder tar til orde for å styrke kommunens kompetanse når det gjelder hva som skal fjernes og hva som skal bli stående ved innsynsbegjæringer. Per i dag har enheten dedikerte ansatte som arbeider med dette, for å kvalitetssikre arbeidet i størst mulig grad. Omfanget av innsynsbegjæringer har de senere årene økt, og høsten 2021 er 2,5 årsverk knyttet til arbeidet med innsynsbegjæringer.

4.5 TILGANGSKONTROLL

Rutiner for bestilling og endring av tilganger er beskrevet på kommunens intranettside. Nyansatte får automatisk tilgang til fellessystemer og standard-tilganger i enheten ved registrering i Human Resource Management (HRM) – systemet. Mens tilganger til fagsystemer ordnes via «IDM-portalen». I denne portalen legger ansatte selv inn forespørsel om tilgang, som så må godkjennes av leder før tilgang blir gitt.

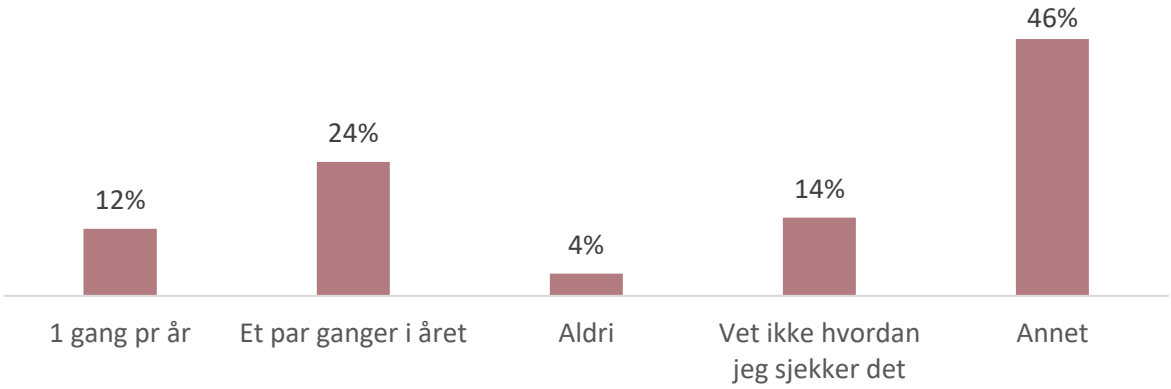
De intervjuede opplever at tilgangskontrollen i kommunen fungerer godt. Både PP-tjenesten, barnevernet og sykehjemmene har fagsystem driftet av kommunens IKT-avdeling, noe som skaper trygghet. I den enkelte virksomhet er det utnevnt superbrukere, som regel lederne, som skal ha et særskilt ansvar for tilgangskontrollen.

Fra informasjonssikkerhetssjef blir det imidlertid påpekt at kommunen ikke har kontroll på tilganger til tjenester som for eksempel Altinn. Dette er en statlig driftet tjeneste som ligger ute på Internett, hvor kommunen ikke har oversikt over hvem som har tilgang. Dette er en utfordring også i andre kommuner. I praksis betyr dette at de ansatte i hvert fall må ha kjennskap tilganger for denne tjenesten.

På spørsmål om ansattes tilganger er begrenset til det de trenger for å kunne utøve sin stilling, svarer informasjonssikkerhetssjef at dette er vanskelig å gi et klart svar på. Kommunen har ikke utarbeidet noen systematisk oversikt over dette. Dette er heller ikke en del av kommunens årlige internkontroll, og IT-avdelingen foretar heller ingen kontroller av de ansattes samlede tilganger.

I kommunens spørreundersøkelse ble ledere spurt om hvor ofte de sjekker at ansatte har riktige tilganger til IT-systemer;

Figur 11. Svar på spørsmål: «Hvor ofte sjekker du at dine ansatte har riktige tilganger i IT-systemene de bruker?» N=50 (ledere) (Kilde: Sandnes kommune)



Rundt en fjerdedel sjekker dette et par ganger i året, mens 14 prosent svarer at de ikke vet hvordan de gjør dette. Av de 23 lederne som svarer «annet», forklarer de aller fleste i kommentarfeltet at tilganger sjekkes ved ansettelse, avslutning eller endring av stilling.

Kommunen benytter også digitale løsninger som ikke har sentral tilgangsstyring. Dette gjelder for eksempel skolefaglige apper eller programmer som Aski Raski og LOGOS. Her har gjerne elever og ansatte egne brukernavn og passord, noe som er vanskelig å fange opp sentralt i kommunen. Hva som ligger av opplysninger i slike programmer opplyses å variere.

4.6 PERSONVERNERKLÆRINGER

På kommunens hjemmesider er det lagt ut en generell personvernerklæring som gjelder for alle enhetene. I tillegg er det utarbeidet egne personvernerklæringer for barnehagene, skolene og for bestilling av covid-19 vaksine. Alle personvernerklæringene inneholder følgende informasjon:

- Personvernombudets kontaktdetaljer
- Hvilke personopplysninger behandles
- Formål og behandlingsgrunnlag for behandling av personopplysninger
- Rettigheter til innsyn, retting, sletting, begrensning, dataportabilitet og tilbaketrekking av samtykke
- Retten til å klage til Datatilsynet

Den generelle personvernerklæringen gjelder for alle som mottar tjenester av kommunen. Erklæring beskriver ikke spesifikt hvilke personopplysninger som behandles, men henviser til den aktuelle tjenesten eller enheten for utøvelse av retten til innsyn, sletting etc.

Kommunen behandler også ansattes personinformasjon, for eksempel kontaktinformasjon for å gi lønn. Men kommunen har ikke egen personvernerklæring for ansatte.

4.7 SÆRSKILT OM SKOLENE

For å sikre etterlevelse av personvernreglene på skolene har kommunen utarbeidet en egen personvernerklæring for disse. I tillegg er det utnevnt systemansvarlige (pedagogiske IKT-veiledere) ved hver enkelt skole som sammen med ledelsen har som oppgave å påse at regelverket blir fulgt. Nylig er det også innført to faktor-autentifisering for tilgang til datasystemene.

Med Korona-pandemien har lærer i hele landet fått behov for flere digitale verktøy, samtidig som skolene har fått tilbud om flere programmer fra forlag og andre aktører, som skal bidra til heldigital undervisning. For den enkelte lærer vil det være fristende å ta i bruk eksternt driftede programmer, og i praksis står både skoleeier og lærere i en skvis mellom å gi best mulig opplæring og samtidig ivareta elevenes personvern. Bruk av eksterne verktøy innebærer en risiko for at opplysninger om elevene kommer på avveie, eller at elevenes e-postadresser blir brukt til svindelforsøk[25].

Under Korona-pandemien har skolesjefen satt som krav at det blir gjennomført risikovurderinger for samtlige programmer som skal tas i bruk. Skolesjefen fremhever i intervju at det ikke er optimalt at hver enkelt skole skal måtte gjøre dette. Hun ser behovet for flere *felles* digitale verktøy og programmer, som eies av skoleeier. Ulempen er at lærerne i mindre grad kan velge programmer selv, noe som utfordrer metodefriheten lærerne har. Men her må hensynet til personvernet og personvernlovgivningen veie tyngst.

Per oktober 2021 er skolesjefen systemeier for følgende systemer:

- OAS – oppvekst administrativt system som heter IST -everyday
- Google Suite Education – her registreres også personopplysninger. Datatilsynet har gitt oss en del avvik som nå er lukket.
- Visma Flyt (PPT)
- Transponder – meldingsbok med kommunikasjon mellom skole og foresatte
- Bibliofil – oversikt over utlån av bøker, hvor vi finner fødselsnummer etc.
- Ulike pedagogiske læringsressurser, som blant annet Wevideo. Det er inngått en kommuneavtale med pedagogisk læringssystem (Soundtrap, Creaza, TV2 elevkanalen, Into Words)

I tillegg benyttes saks- og arkivsystemet Public 360 hvor alle elevmappene ligger lagret. Dette er informasjon knyttet til enkeltvedtak, personlige forhold og samtykke fra foresatte. Tilgangskontrollen til opplysningene skjer gjennom en to-faktor-autentisering, hvor tilgangsstyringen er lagt til Dokumentsenteret. Fra kommunen får vi opplyst at Dokumentsenteret foretar kontroller av loggene til elevmappene, og i tråd med kommunens personvernerklæring er

[25] Konsekvenser av kræsjdigitaliseringen i norsk skole oppsummeres i rapport fra Bouvet

samtlige registrert i Draftit. I tillegg foreligger databehandleravtale og risikovurdering for saks- og arkivsystemet. I intervju får vi opplyst at lærere har tilgang til elevmapper for alle elever på sin skole. Det opplyses også at slike store tilganger er problematiske, og at et fremtidig nytt system bør ha bedre funksjonalitet for strengere tilgangsstyring.

På spørsmål om hva som eventuelt oppleves som en barriere for å følge rutiner og praksis, fremhever skolesjefen at utarbeidelse av egne risikovurderinger og databehandleravtaler er tids- og ressurskrevende. Hun ser som nevnt behovet for en mer effektiv organisering, slik at arbeidet med informasjonssikkerhet og personvern ikke blir for tidkrevende for den enkelte skole. I forbindelse med den nylig gjennomførte omorganiseringen til ett, felles oppvekstområde har dette vært oppe på agendaen. Kommunen har så langt startet med OAS[26], og forsøker i større grad å få til felles verktøy, med felles risikovurderinger på overordnet nivå.

Som avdekket i vår kontroll av programmet LOGOS i Draftit, har hver enkelt skole hittil hatt ansvaret for å skrive en databehandleravtale med LOGOS, og eventuelt gjennomføre egne risikovurderinger. Per oktober 2021 er kommunen imidlertid i gang med å anskaffe en felles utgave av dette programmet, som skal gjelde for hele kommunen[27].

Mer bruk av felles programmer støttes også av en landsomfattende rapport publisert av Bouvet høsten 2021. I rapporten kalt «Digitalisering i skolen – har vi glemt personvernet?» anbefales bedre opplæring og utnyttelse av digitale læringsressurser for å sikre personvernet. Det bør ikke være slik at hver enkelt kommune skal sitte med hele oppgaven med å vurdere hvilke verktøy som egner seg best i de ulike fagene. Rapporten anbefaler mer bruk av felles programmer, og arbeidet med risikoanalyser og databehandleravtaler bør samordnes og effektiviseres. Dette vil bidra til å sikre personvernet og bidra til bedre utnyttelse av digitale læringsressurser, heter det i rapporten.

Bouvet-rapporten anbefaler for øvrig også at det utarbeides en felles tjenestekatalog for digitale læringsressurser, noe regjeringen allerede har foreslått i sin handlingsplan for digitalisering av grunnopplæringen. Med en slik katalog vil elever og lærere få tilgang til bedre verktøy, og verktøy som er dårlig på personvern vi kunne holdes utenfor norsk skole.

4.8 VURDERING

Kommunen behandler personopplysninger for å levere kommunale tjenester. Opplysninger som behandles varierer fra enkle kontaktopplysninger til sensitive helseopplysninger. Behandlingen av personopplysninger foregår på ulike måter; skriftlige dokumenter til internt bruk, per brevpost og i e-poster fra privatpersoner. Men hovedvekten av behandling ligger i de ulike digitale fagsystemene i kommunen.

[26] OAS – oppvekst administrativsystem som heter IST-everyday

[27] Eventuelt et tilsvarende program.

Sensitive opplysninger skal ikke sendes per e-post. Dette har kommunen egne rutiner for i informasjonssikkerhetshåndboken. Kommunisering av sensitive opplysninger mellom andre enheter og innbyggere skjer også i større grad via fagsystemer og sikre digitale kommunikasjonsløsninger enn tidligere, noe som reduserer sannsynligheten for at slike opplysninger sendes per e-post. Henvendelser fra innbyggerne kan inneholde sensitive opplysninger, for eksempel helseopplysninger knyttet til kommunens tjenester. Dersom ansatte svarer innbyggeren per e-post, skal sensitive opplysninger slettes før svaret sendes. Kommunen har rutiner på dette og flere av de vi har intervjuet bekrefter at rutinene blir fulgt. Vi vurderer derfor at kommunen har tilfredsstillende rutiner og god praksis som hindrer e-poster med sensitive opplysninger.

Kommunens digitale løsninger som behandler personopplysninger registreres i eget system (Draftit). Systemet fungerer som protokoll over behandling av personopplysninger ved at det blant annet beskriver behandlingsgrunnlag, kategorier av personopplysninger osv. Det er systemeier i den enkelte enhet som er ansvarlig for å registrere enhetens systemer i Draftit. Det er positivt at kommunen har eget, og «levende» system for slik registrering.

Personvernombudet er gitt oppgaven med å kontrollere at systemene blir registrert i Draftit. Status per november 2021 er at det er registrert 319 behandlinger, derav 270 systemer i Draftit. Ikke alle systemer ligger per november registrert, og her gjenstår et arbeid i skolene. I vår kontroll av fire utvalgte fagsystem fant vi at alle systemene var registrert i Draftit, men at ett av systemene manglet dokumentasjon på risikovurdering og databehandleravtale. Kommunens spørreundersøkelse avdekker at en større andel av lederne ikke gjennomfører risikovurderinger, og at de ønsker veiledning om hvordan man gjør dette. For å sikre personvernet i systemer er det viktig at kommunen øker bruk av risikovurderinger.

Rutiner for sletting av personopplysninger er forskjellig ut fra behandlingen. Behandling av personopplysninger etter arkivloven skal for eksempel ikke slettes i utgangspunktet. Rutinene for sletting beskrives i Draftit og følges opp på enhetsnivå. Det generelle inntrykket vi har fra intervjuene er at kommunen har god kontroll på rutiner rundt sletting av opplysninger.

For å hindre at uautoriserte får tilgang til personopplysninger fastsetter personvernlovgivningen krav om tilgangskontroll. Hvilke tilganger ansatte trenger, bestemmes av leder og styres sentralt av IKT-avdelingen. Dette gjelder fellessystemer og større fagsystemer. Oppfølging av tilganger er ikke formalisert i kommunen, med unntak av ved avslutning av arbeidsforhold. Det er opp til den enkelte leder å kontrollere at ansatte har de riktige tilgangene. På bakgrunn av informasjon fra kommunens spørreundersøkelse og intervjuer vi har foretatt, kommer det fram at tilganger i liten grad sjekkes, utover ved endring eller avslutning av arbeidsforhold. I spørreundersøkelsen svarer 14 prosent av lederne at de ikke vet hvordan tilganger skal sjekkes.

Kommunens saks- og arkivsystem, foruten fagsystemer på enheter vi har inkludert i våre intervjuer, har logger som viser hvilke ansatte som har sett, endret eller slettet noe i fagsystemet, noe som vi vurder er tilfredsstillende. Ved noen av enhetene gjennomføres stikkontroller for å

sjekke at ansatte ikke har vært inne på saker de ikke har et formålstjenlig behov for å åpne, men det generelle inntrykket er enhetene ikke har formalisert sin kontroll av aktivitetsloggen.

Hva som publiseres på offentlig postliste styres fra kommunen sentralt. I prosjektet har vi sjekket publiserte saker ved et utvalg skoler og barnehager, men vi fant ingen saker med personopplysninger. Dette må sies å være positivt. Kommunen synes å ha godt innarbeidet kvalitetskontroll av offentlig postliste som forhindrer feilpubliseringer.

Revisjonen kommer med følgende anbefalinger til kommunen:

- Kommunen bør registrere alle systemer som behandler personopplysninger i Draftit
- Kommunen bør sikre at det gjennomføres risikovurderinger ved bruk av digitale løsninger.

5 BRUDD PÅ PERSONVERNREGLENE

Problemstilling: «Hvordan håndterer kommunen brudd på personvernreglene og hvordan følges dette opp?»

5.1 REVISJONSKRITERIER

Fylkeskommunen skal etter kommuneloven § 25-1 punkt c «avdekke og følge opp avvik for risiko for avvik». Hvis avviket gjelder personopplysninger, skal den behandlingsansvarlige etter personvernforordningen artikkel 33 melde bruddet på personopplysningsplikten til tilsynsmyndighet innen 72 timer. Kort forklart skal avviksmeldingen beskrive hva som har skjedd, hvilke konsekvenser avviket kan gi og hvilke tiltak som har eller skal iverksettes.

Artikkel 34 sier at *«Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet.»*. Rutiner for behandling av avvik skal være beskrevet i internkontrollen.

Revisjonskriterier:

- Kommunen skal ha rutiner for å håndtere avvik knyttet til brudd på personopplysningsloven
- Avvik bør følges opp med tiltak i etterkant

5.2 RUTINER FOR AVVIKSHÅNDTERING

Kommunen benytter seg av eget avvikssystem, Compilo, for behandling av avvik. Generell informasjon om avvik og link til Compilo er tilgjengelig på intranettområdet «Helse, Miljø og Sikkerhet – HMS». Intranettet er delt opp i seks hovedområder, HMS-siden er tilknyttet området «Hjelp i jobben». På intranettet beskrives følgende kategorier for avvik:

1. HMS som gjelder hendelser og situasjoner knyttet til helsen, miljøet eller sikkerheten til de ansatte. Videre også hendelser som vedgår det indre eller ytre miljø på arbeidsplassen. For eksempel skade på ansatt, utstyr, miljøutslipp osv.
2. Organisasjon/internt som gjelder hendelser og situasjoner knyttet til interne forhold på arbeidsplassen. Dette kan være samarbeid, organisering, avtaler osv.
3. Tjeneste/Bruker som gjelder hendelser og situasjoner som angår tjenestemottaker. For eksempel elever, pasienter og lignende.

Intranettsiden henviser til kapittel i HMS-håndboken for mer informasjon om avvikshåndtering. I HMS-håndboken beskrives de samme tre kategoriene for avvik. I tillegg står det i HMS-håndboken at avvik defineres etter alvorlighetsgrad (lav, middels, høy) og beskriver følgende roller og oppgavefordeling:

Figur 12. Beskrivelse roller knyttet til avviksbehandling. Hentet fra kommunens HMS-håndbok

Oppfølging av avvik

Nærmeste leder vil som hovedregel være avviksbehandler med ansvar for å lukke avviket innen tidsfrist. Avvik som ikke lukkes innen tidsfrist vil bli videresendt i linjen til nest ledernivå. Leder som har mottatt et avvik har og muligheter for å videresende avvik i linjen hvis det vurderes som nødvendig.

Lokalt verneombud vil være kopimottaker og har lesetilgang og kan gi kommentarer til HMS-avvik for eget ansvarsområde.

Hovedverneombud vil være kopimottaker og har lesetilgang og kan gi kommentarer til HMS-avvik innenfor eget ansvarsområde.

Hvis leder ønsker å endre på alvorlighetsgrad som avviksmelder har satt, bør leder informere og avklare dette med avviksmelder. Hvis dette gjelder HMS-avvik bør det vurderes om verneombud skal være med for å avklare alvorlighetsgraden.

Fra intranettet er det også tilgang til flere brukerveiledninger for Compilo.

Avvik på personvernreglene er ikke spesifikt nevnt på intranettområdet for HMS. Under området «Om kommunen» som er en annen av de seks hovedområdene, er det en egen side for informasjonssikkerhet. På denne siden er det informasjon om avvik som skal sendes til Datatilsynet:

> *«Avviksmeldinger som skal til Datatilsynet må fylles ut på vedlagt skjema, "melding om avvik". Utfylt skjema sendes på e-post til personvernombud Sigrun Homleid (sigrun.homleid@sandnes.kommune.no). Fristen er 72 timer for melding til datatilsynet. Meldingen må sendes Sigrun umiddelbart etter at avviket er oppdaget.*
>
> *Du finner "avvik til Datatilsynet" til høyre på denne nettsiden. Last ned skjemaet og lagre det lokalt, slik at ikke opplysningene du fyller inn blir liggende i malen.»*

Informasjonssikkerhetshåndboken har også eget avsnitt for avvikshåndtering (se vedlegg).

5.3 AVVIK REGISTRERT I COMPILO 2017-2021

I Compilo er det hentet ut statistikk for avvik i kategori «Informasjonssikkerhet og personvern». Denne kategorien har også følgende underkategorier med følgende beskrivelse i Compilo:

- Brudd på taushetsplikt (eksempel: informasjon (inkludert samtaler) gitt til uvedkommende. Snoking i data utenfor ansattes arbeidsoppgaver. Utskrift på avveie. Feilsendt post. Deling av brukernavn og/eller passord. Feil/manglende skjerming av dokumenter i fagsystemer. Publisering av bilder, film og lydopptak uten samtykk.
- Uautorisert endring av data. (Manipulering, sletting eller endring av data. Det kan være bevisste handlinger, brukerfeil, systemfeil eller liknende)
- Feil behandling av personopplysninger. (Behandling av personopplysninger som ikke er i henhold til lovverk og prosedyrer. Eksempel: Innsamling eller lagring av informasjon uten tillatelse. Ikke saklig grunn for behandlingen. Manglende vurdering av behandlingens lovlighet. Utilstrekkelig eller manglende rutiner og prosedyrer. Mangler databehandleravtale. Behandlingen ikke registrert i Draftit)
- IT-utstyr. (Eksempel: Uautorisert utstyr kobles til kommunens nettverk. Uautoriserte systemendringer. Funksjonsfeil i programvarer eller maskinvare.)
- Datainnbrudd. (Forsøk på eller tilfeller av hacking, phising, virus og liknende.)

*Tabell 7. Antall registrerte avvik etter kategori. *Til og med 01.11.21. (Kilde: Compilo).*

Kategorier	2017	2018	2019	2020	2021*
Brudd på taushetsplikt	13	17	20	75	66
Datainnbrudd	0	0	0	3	1
Feil behandling av personopplysninger	0	0	1	23	68
IT-utstyr	9	15	70	30	15
Uautorisert endring av data	32	29	43	1	2
Ikke kategorisert	8	18	17	17	6
Totalt	**62**	**79**	**151**	**149**	**158**

De siste årene har det blitt meldt inn rundt 150 avvik årlig innen informasjonssikkerhet og personvern. Fram til 1. november 2021 er det meldt inn 158 avvik. Hvilke typer avvik som dominerer, varierer. I 2019 ble det meldt inn mange avvik på IT-utstyr, mens i 2020 ble det meldt inn 75 brudd på taushetsplikt. I 2021 er det meldt inn flere saker på «feil behandling av personopplysninger» enn tidligere år. En gjennomgang av avvik meldt inn i 2021 har følgende tema som går igjen:

Internpost med personsensitive opplysninger: Slike opplysninger skal legges inn i egen hvit konvolutt som legges inn i internpostkonvolutt. Avvikene gjelder opplysninger som er lagt direkte i internpostkonvolutt. Alvorlighetsgraden er stort sett middels og havner innenfor kategoriene «feil behandling av personopplysninger» og noen under «brudd på taushetsplikt».

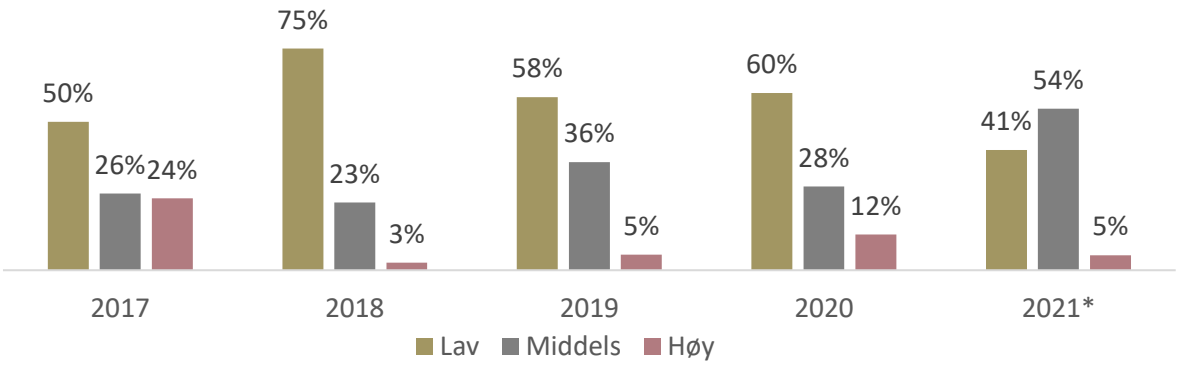
Avdelinger i kommunen som har gjentatte ganger meldt inn denne type avvik er helse og velferd, sykehjem, barn og unge og skole.

Gjenglemt personopplysninger: Typiske avvik er ark med navn, gjenglemt hos bruker. De fleste avvik er meldt inn under «brudd på taushetsplikt».

Feil i digitale systemer/feilsending: Her er det flere ulike avvik som handler om teknisk feil eller svakheter, eller feil bruk av systemer. Eksempler på avvik som er meldt inn, er manglende nullstilling av jobbtelefon, dokumenter fra sikker sone som har havnet i åpen sone, utsending av felles SMS hvor mottaker fikk se opplysninger fra andre mottakere og ansatt som har endret jobb-epostadresse.

Annet – Rollebrudd: Her finner vi brudd på taushetsplikt. Eksempelvis er hendelser hvor taushetsbelagt informasjon har blitt diskutert av ansatte foran andre brukere og hjemmetjeneste som har ringt på feil dør. Av andre avvik er det også fysiske skader, HMS-avvik, som er lagt under feil kategori i Compilo.

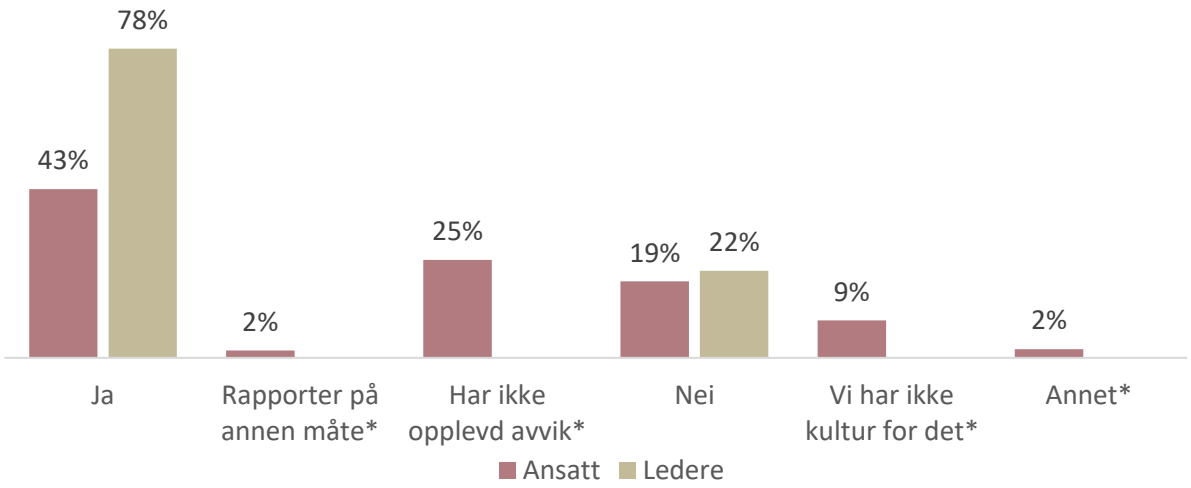
*Figur 13. Alvorlighetsgrad etter antall avvik per år. N= se Tabell 7). *Til og med 01.11.21. (Kilde: Compilo).*



De fleste avvik som meldes inn er av lav eller middels alvorlighet. I 2021 er det meldt inn flere middels alvorlige saker, men samtidig færre med høy alvorlighetsgrad.

I kommunens spørreundersøkelse ble ansatte og ledere spurt hvorvidt de rapporterer avvik i Compilo. 78 prosent av lederne svarer at de gjør det. De ansatte svarer i mindre grad at de melder avvik (43 prosent), men her svarer også en fjerdedel at de ikke har opplevd avvik. Noen ansatte har også svar at avvik rapporteres på annen måte og de fleste forklarer at det er nærmeste leder en har rapportert til.

Figur 14. Svar på spørsmål: «Rapporterer du avvik eller brudd på personvern/informasjonssikkerhet i Compilo?» N= 274 (Ansatte), N=50 (ledere) (Kilde: Sandnes kommune)[28]

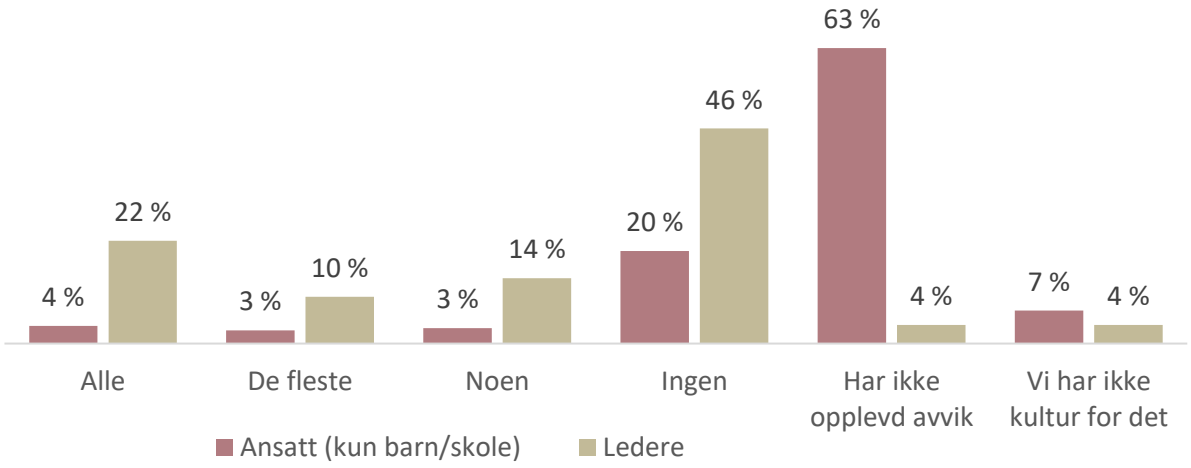


Ansatte (utenom ansatte i Organisasjon) og ledere ble også spurt hvor mange avvik som har blitt registrert i Compilo. Her ser vi at en stor del av lederne (46 prosent) svarer ingen, mens 63 prosent av ansatte svarer «Har ikke opplevd avvik». En av de vi intervjuet bekrefter at det hender at avvik ikke blir meldt inn i Compilo og utdyper at dette gjerne har med kunnskap å gjøre, at avviksregistreringen oppleves som tungvint. Det vises også til at enheter som bruker Compilo for andre typer avvik gjerne også er flinkere til å melde inn avvik på informasjonssikkerhet og personvern.

En virksomhetsleder innen Oppvekst barn og unge forteller i intervju at avvik står høyt på agendaen i ledergruppa og i møte med ansatte. Lederen oppfordrer alle ansatte til å melde inn avvik i Compilo og opplever at det er kultur for det. En annen virksomhetsleder forteller at det kan være ulike oppfatninger rundt hvordan en definerer avvik, og forteller at det på enheten har blitt gjort arbeid med å øke oppmerksomhet og kunnskap rundt hva avvik er og hvordan dette meldes.

[28] Ledere hadde i spørreskjemaet kun svaralternativ ja/nei. Ansatte hadde i tillegg svaralternativ «Vi har ikke kultur for det», også fritekstsvar. En stor del ansatte har skrevet svar i fritekst. På bakgrunn av disse svarene har revisjonen laget nye kategorier merket med *.

Figur 15. Svar på spørsmål: «Hvis du har opplevd avvik i informasjonssikkerhet, hvor mange har du registrert i Compilo?» N= 212 (Ansatte i enhet Oppvekst barn/unge og enhet Oppvekst skole), N=50 (ledere) (Kilde: Sandnes kommune)



5.4 AVVIK TIL DATATILSYNET 2018-2021

Avvik som legges inn i Compilo i kategori «informasjonssikkerhet og personvern» får automatisk følgende melding:

«For avvik knyttet til personvern skal det alltid vurderes om det er behov for å melde avviket til datatilsynet. Er din vurdering at dette avviket skal rapporteres til Datatilsynet, skal dette videresendes til ansvarlig i Sandnes kommune for innrapportering til Datatilsynet. Det er 72 timers meldeplikt til datatilsynet, så dette må håndteres raskt».

Kommunen bruker eget skjema for avvik til Datatilsynet, som er basert på Datatilsynets mal i Altinn. Skjemaet sendes inn av den som oppdager avviket, og personvernombud og informasjonssikkerhetssjef følger opp behandlingen i Datatilsynet.

Fra 2018 til og med oktober 2021 har kommunen sendt inn 18 avvik til Datatilsynet. Per 22.10.2021 var alle saker, unntatt to nylige, avsluttet av Datatilsynet. Tidligere i rapporten er det beskrevet fire av avvikene som ble sendt til Datatilsynet; to av avvikene var fra skolene og gjaldt manglende etterlevelse av personvern for digitale løsning er (Google Suite Education og Beat the Street). De andre avvikene som er sendt gjelder ulike temaer; fødselsnummer på offentlig postliste, gjenglemte papirlister med helseopplysninger og feilsending av brev. Noen avvik gjelder også problemer hos leverandører, som for eksempel dataangrep hos vann og avløpsleverandør og feil i ID-porten.

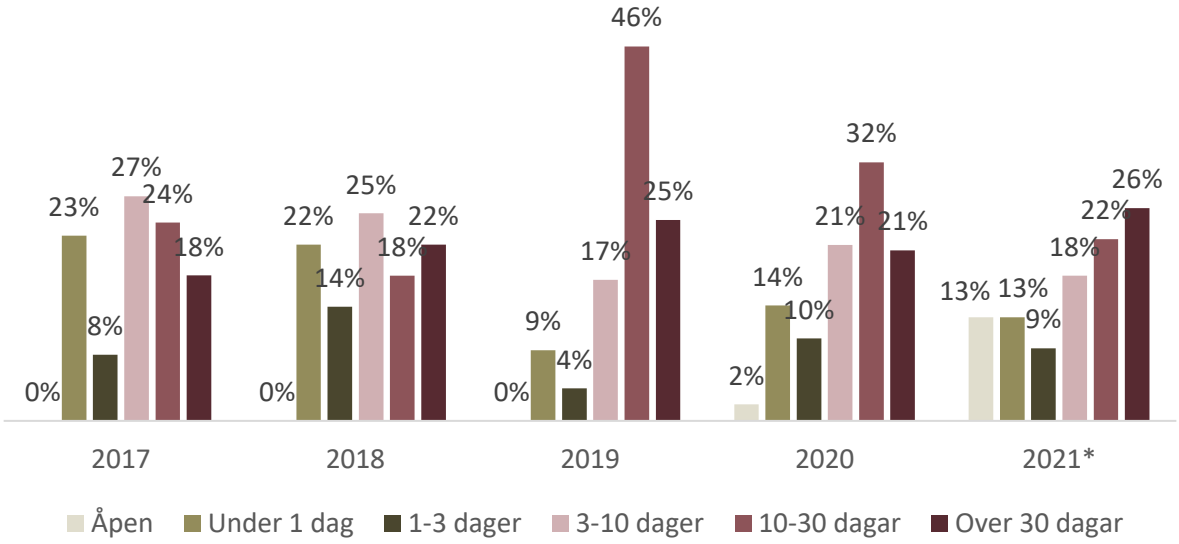
5.5 OPPFØLGING AV AVVIK

I forbindelse med årsrapport rapporterer kommunen årlig på arbeid med informasjonssikkerhet og personvern. I årsrapport for 2020 står det at det er registrert «149 avvik som har blitt behandlet av

ledere i linjen, i tillegg blir avvikene kontrollerte av kommunens informasjonssikkerhetssjef og personvernombud». Årsrapporten beskriver også at det i 2020 har vært arbeidet med å øke bevissthet, eierskap og kunnskap om personvern og viser deriblant til igangsatt e-læring innen informasjonssikkerhet.

Avvik som registreres i Compilo registreres med lukketid, som er antall dager fra første registrering til avvik blir lukket av nærmeste leder. Per 01.11.21 er det 17 avvik som ikke er lukket, to fra 2020 og 15 fra 2021. De siste to årene har rundt en fjerdedel av avvikene hatt en lukketid på mer enn 30 dager. En virksomhetsleder forklarer at det gjøres tiltak internt før avviket markeres som lukket.

*Figur 16. Lukketid etter antall avvik per år. N= se Tabell 7). *Til og med 01.11.21. (Kilde: Compilo).*



Avvik som meldes inn i Compilo blir kontrollert av personvernombud og informasjonssikkerhetssjef. Personvernombudet holder også kontakten med Datatilsynet og forteller i intervju at hun sjekker at anbefalinger og pålegg fra Datatilsynet blir fulgt opp i enhetene. Personvernombudet forteller i intervju at hun sammen med informasjonssikkerhetssjef går gjennom avvik i Compilo for blant annet å se om noen avvik går igjen og om det er noe som kan forbedres. En del av dette er å se om avvikene er på system eller individnivå, for eksempel om enkelte avdelinger skiller seg ut. Det vises til at avvik knyttet til internpostkonvolutter gjerne går igjen, noe som også bekreftes av andre vi har snakket med. En av de intervjuede viser også til at økende praksis med digital post reduserer risiko med feil håndtering av papirdokumenter.

Et vanlig avvik er at brukernavn og passord kommer på avveie. En av de vi intervjuet forteller at dette er et kjent problem, men at det gjerne kan være utgåtte passord knyttet til skolene. Kommunen jobber med å erstatte eksisterende pålogging med to-faktor pålogging. Bruk av to-faktor pålogging høyner sikkerhetsnivået. En slik løsning gir liten risiko for misbruk av tilganger når brukernavn og passord kommer på avveie.

En virksomhetsleder forteller om håndteringen av to avvik som ble meldt til Datatilsynet. Det ene avviket gjaldt publisering av navn knyttet til journalsystem i arkiv, noe som også var en nyhetssak[29]. Det andre avviket handlet om personopplysninger som ble gjort tilgjengelig for uvedkommende. Årsaken var både manglende retningslinjer og manglende tekniske funksjoner i innhenting av kontaktopplysninger fra folkeregisteret. Virksomhetslederen forteller at avvikene ble fulgt opp i kommunen på en god måte, og rutinene rundt avviksbehandling ble fulgt. I sakene ble alle involverte samlet til felles møter og virksomhetsleder opplevde at det ble gitt fortløpende informasjon i sakene. Det ene avviket ble fulgt opp med ROS-analyse og nye retningslinjer på enheten.

En annen virksomhetsleder viser til at det i Compilo legges inn dokumentasjon på vurderinger a avviket, og at det gjennomføres kvartalsvis gjennomgang av avvik i ledergruppen. Dette gjøres for å informere om hva som er viktig å rette oppmerksomheten mot, for å unngå flere avvik.

5.6 VURDERING

Kommunen har eget system, Compilo, for kvalitetsarbeid og avviksoppfølging. Dette har alle ansatte tilgang til via intranett. Systemet brukes til behandling av ulike typer avvik, hvor informasjonssikkerhet og personvern er en egen kategori. Rutiner for avviksbehandling er beskrevet i informasjonssikkerhetshåndboken. Vi vurderer at rutinene på en tilfredsstillende måte beskriver hva ansatte og ledere skal gjøre i avvikshåndtering. Alle som oppdager avvik, har ansvar for å melde dette i Compilo. I Compilo sendes avviket til nærmeste leder. Personvernombudet og informasjonssikkerhetssjef får også kopi av avvik som gjelder GDPR-personvern. Nærmeste leder behandler og lukker avviket. Avvik som meldes til Datatilsynet behandles også av personvernombudet.

De siste årene er det årlig meldt inn rundt 150 avvik innen informasjonssikkerhet og personvern. Brudd på taushetsplikt og feil behandling av personopplysninger er gjengangertemaer.

Siden 2018 har kommunen meldt inn 18 avvik til Datatilsynet. Flere avvik er fra skolene og gjelder manglende etterlevelse av personvernkrav, som risikovurderinger, ved bruk av digitale løsninger. Kommunen har også opplevd dataangrep og teknisk feil hos ulike leverandører som har resultert i avviksmelding til Datatilsynet.

I kommunens spørreundersøkelse svarer ansatte i Oppvekst barn og unge og Oppvekst skole at det ikke er kultur for å melde avvik i informasjonssikkerhet. De vi intervjuet bekrefter at det hender avvik ikke meldes inn i Compilo. Enheter som benytter Compilo til andre typer avvik er gjerne flinkere til å melde inn avvik innen informasjonssikkerhet og personvern ifølge de

[29] Nesten 2200 navn knyttet til PPT-journaler fra Sandnes lå søkbare i arkivportal (aftenbladet.no)

intervjuede. Dette gjelder for eksempel enheter i helsetjenester som har praksis for melding av HMS-avvik i Compilo.

Kommunen har system for oppfølging av avvik i Compilo. Avvik som legges inn må registreres med tiltak før de kan formelt lukkes av linjeleder. Et flertall av avvikene de siste årene har en lukketid på enten 10-30 dager eller over 30 dager. Avvikene innen informasjonssikkerhet og personvern blir også kontrollert av personvernombud og informasjonssikkerhet. Vanlig praksis er å identifisere om det er avvik som går igjen eller om det er enheter som skiller seg ut. På denne måten blir det identifisert forbedringspunkter for kommunen, noe vi vurderer som svært positivt. En virksomhetsleder at avvik jevnlig blir gjennomgått i ledergruppe som tiltak for å unngå nye avvik.

Revisjonen kommer med følgende anbefaling til kommunen:

- Kommunen bør skape mer kultur for å melde inn avvik på informasjonssikkerhet og personvern

VEDLEGG

Skriftlige kilder

Anskaffelsespolitikk for Sandnes kommune (2018)
Arkitekturprinsipper for digitalisering
Strategi for anskaffelser 2018-2022
Sandnes – Helt enkelt – Metodikk for arbeid med digitalisering, smartby og innovasjon
Strategi velferdsteknologi 2015 – 2020
Årsrapport 2020 -Kommuneplan - Måloppnåelse for tjenesteområdene
Informasjonssikkerhetshåndbok
Informasjonssikkerhetsinstruks
HMS-håndbok
Helhetlig risiko- og sårbarhetsanalyse (Revidert 20.05.2020)
Mal for databehandleravtale
Mal for avviksmelding Datatilsynet
Risiko og sårbarhetsanalyse for Public 360°
Avvik meldt inn i Compilo 2018-2021

Muntlige kilder

Personvernombud
Informasjonssikkerhetssjef
Leder dokumentsenter
Skolesjef
Digitaliseringsleder
Rådgiver i anskaffelsesavdelingen
Kommuneadvokat
Fire virksomhetsledere innen oppvekst barn og unge, og helse og velferd

Informasjonssikkerhetshåndboken – «Livsløp for informasjonsinnholdet i IT-løsninger»

Livsløp for informasjonsinnholdet i IT-løsninger -

Informasjon i IT-løsninger går gjennom et livsløp, gjennom anskaffelse, drift, arkivering og avvikling.

Anskaffelse av nytt IT-system

I anskaffelsesprosessen skal det stilles krav om innebygd personvern og personvern som standardinnstilling. Det er viktig å sikre at personopplysninger ikke kommer på avveie, derfor må det stilles krav til løsninger hvor personvern har høy prioritet.

Det skal utnevnes en systemeier som er behandlingsansvarlig for systemet og har ansvaret for at oppgavene rundt forvaltningen og risikoanalyse. Systemeieren rådfører seg med personvernombud i alle spørsmål knyttet til personvern og behandling av personopplysninger.

Systemeier sammen med informasjonssikkerhetssjef er ansvarlig for å gjennomføre ROS analyse der formålet med behandlingen av systemets behandling av personopplysninger blir gjennomført og personopplysningene blir redegjort for. Det skal alltid vurderes om en DPIA skal utarbeides.

Forvaltning av IT-systemet

Det skal gjennomføres årlig informasjonssikkerhetsgjennomgang med oppdatering av risikovurderingen. Det er systemeier som er ansvarlig for gjennomføring av årlig informasjonssikkerhetsgjennomgang, og informasjonssikkerhetsanavarlig og/eller personvernrådgiver samt representant fra IT-drift skal delta.

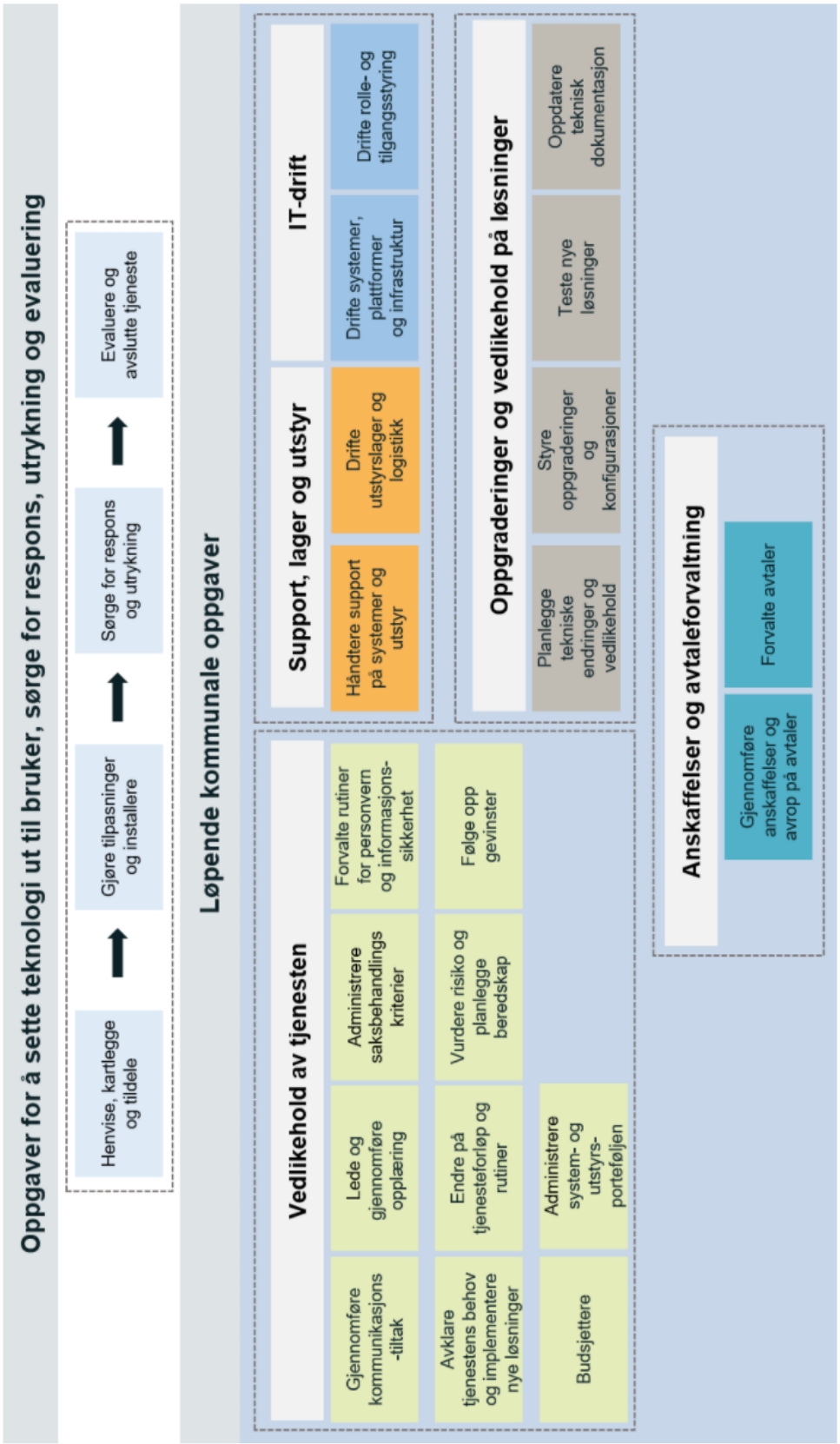
Databehandleravtaler skal gjennomgås og fornyes ved behov.

Avhending av IT-system

Når et IT-system ikke lenger skal brukes, skal data som ligger i systemet sikres med hensyn til konfidensialitet, integritet og tilgjengelighet. Informasjonen skal arkiveres i hht lovverket, og det skal være mulig å videreføre bruk i andre systemer.

Systemeier er ansvarlig for at informasjonen blir ivaretatt på en trygg måte når systemet ikke lenger skal tas i bruk. Dokumentsenter bistår sammen med systemeier for å sikre rett forvaring.

Helhetlig tjenestemodell for helse- og omsorgstjenestene (fra intranett)



Informasjonssikkerhetshåndboken - internkontroll

Internkontroll

Avviksbehandling +

Formålet med avviksbehandlingen er å få kunnskap om hendelser slik at kommunen samlet kan begrense skadene, lære av hendelsene og endre rutiner og implementere gode løsninger. Dette for å hindre at vi unngår at liknende hendelser skjer igjen samt sikre at vi til enhver tid ivaretar våre innbyggeres personvern.

Hendelser som skal meldes som avvik kan være enkeltepisoder, gjentakende episoder, overtredelser, svikt i rutiner, funksjonsfeil i fagsystemet eller liknende, der personopplysninger har kommet på avveie, ikke lenger er korrekte eller oppdaterte, eller har gått tapt. Også personopplysninger som er kryptert kan gå tapt eller komme på avveie, og de skal også meldes til datatilsynet. Det er viktig at de registrerte også får beskjed så tidlig som mulig slik at de kan gjøre nødvendige tiltak.

Alle som oppdager et avvik har ansvar for å melde dette i avvikssystemet Compilo. Alvorlige brudd vil bli varslet personvernombud.

Mottak og behandling av avviksmelding

Personvernombud kan motta avviksmeldingen som en muntlig henvendelse, tekstmelding, telefon eller som et avviksmeldingsskjema. En melding om avvik til personvernombudet skjer i fortrolighet, og personvernombudet har taushetsplikt og ivaretar melderens anonymitet. Personvernombudet vil også kunne igangsette avviksbehandling på eget initiativ, uten at en formell avviksmelding er mottatt.

1. Avvik registreres i Compilo. Dersom avviket er av en slik karakter at det er fare for personopplysninger har kommet på avveie, blitt urettmessig endret eller gått tapt skal avviket meldes datatilsynet
2. Følg instruksene i Compilo for melding til datatilsynet.
3. En egen enhet «Personvern GDPR» som består av fire personer håndterer melding om avviket til datatilsynet. Meldingen sendes uten ugrunnet opphold og senest 72 timer etter at avviket er oppdaget. Melding til Datatilsynet skal ikke unntas offentligheten
4. På bakgrunn av opplysninger oppgitt i avviksmelding vil personvernombudet kontakte aktuelle ressurser, f. eks systemansvarlig, behandler eller leder for å avklare realiteten i og omfang av avviket, og finne forslag til tiltak for å lukke avviket og begrense skaden
5. Personvernombudet, Informasjonssikkerhetssjef, behandlingsansvarlig og systemeier vurderer avvikets omfang, alvorlighetsgrad og allerede igangsatte tiltak.
   - Har personopplysninger kommet på avveie, blitt urettmessig endret eller slettet slik at Datatilsynet skal varsles?
   - Har det allerede blitt igangsatt tilstrekkelig gode tiltak for å lukke avviket og hindre nye avvik kan avvikssaken lukkes?
   - Ved behov kontakter personvernombudet Datatilsynet om spørsmål ved hendelsen.
6. Personvernombudet utformer og sender melding til de registrerte på vegne av behandlingsansvarlig og systemeieren i de tilfeller der personopplysninger har kommet på avveie, blitt urettmessig endret eller gått tapt. Meldingen til de registrerte signeres av behandlingsansvarlig og skal sendes uten ugrunnet opphold. Den kan være i form av e-post, pressemelding eller annen skriftlig melding som vil nås alle berørte.
7. Dokumentbehandlingen skal skje i saksmappen personvernombud [årstall] i sak/arkivsystemet, der de i utgangspunktet unntas i offentlighet.
8. Personvernombudet utformer notat for avvikssaken. Ved avvik der tilstrekkelige tiltak for å lukke og hindre nye avvik er igangsatt, kan avvikssaken foreslås lukket. Avviksmelding til Datatilsynet og melding til de registrerte legges ved der dette er aktuelt. Notatet med vedlegg sendes til behandlingsansvarlig som beslutter om avvikssaken kan lukkes.