Rogaland Revisjon

Forvaltningsrevisjon

Informasjonssikkerhet

Stavanger kommune, 2023

INNHOLD

OPPDRAGET

Bestilling:

Kontrollutvalget i Stavanger kommune vedtok 28.03.22 en forvaltningsrevisjon av Informasjonssikkerhet.

Formål:

Formålet med prosjektet er å vurdere i hvilken grad kommunen sikrer tilstrekkelig opplæring, kompetanse og praksis for å ivareta informasjonssikkerhetskrav.

Problemstillinger:

- I hvilken grad har de ansatte, på alle nivå, kjennskap til retningslinjer og rutiner for informasjonssikkerhet? [1]
- I hvilken grad etterlever kommunen kravene til informasjonssikkerhet?
- Hvordan kommuniseres arbeidet med informasjonssikkerhet ut i organisasjonen?
- I hvilken grad bruker kommunen avvikssystemet til læring og forbedring?

Prosjektleder for prosjektet har vært forvaltningsrevisor Guro Tjøstheim. Rapporten er kvalitetssikret av leder for forvaltningsrevisjon Silje Nygård og gjennomgått av revisjonsdirektør Rune Haukaas.

[1] Kontrollutvalget la til «*på alle nivå*» i første problemstilling i møte 28.03.22 (16/22)

SAMMENDRAG

På oppdrag fra kontrollutvalget har Rogaland Revisjon utført forvaltningsrevisjon av kommunens håndtering av informasjonssikkerhet. Formålet med prosjektet er å vurdere i hvilken grad kommunen sikrer tilstrekkelig opplæring, kompetanse og praksis for å ivareta informasjonssikkerhetskrav. De viktigste datakildene i prosjektet er spørreundersøkelse (til alle ansatte i kommunen), gjennomgang av dokument, rutiner og protokoll, samt intervju.

Hovedinntrykk

Informasjonssikkerhet handler om vern av alle typer informasjon slik at informasjonen ikke blir gjort kjent for uvedkommende, ikke blir endret utilsiktet og er tilgjengelig ved behov. Vårt hovedinntrykk er at:

- Kommunen har et gjennomgående styringssystem for informasjonssikkerhet, men ansattes kjennskap til retningslinjer og rutiner svekker kommunens ivaretakelse av krav knyttet til informasjonssikkerhet.
- Informasjon og opplæringsmateriell om informasjonssikkerhet er tilgjengelige gjennom ulike kanaler, og kommunens opplæringsplan inneholder viktig informasjon om informasjonssikkerhet.
- Det er få som gjennomfører obligatorisk opplæring i informasjonssikkerhet. Kun 8% av ansatte i Oppvekst og utdanning har gjennomført minst ett av syv krav i planen.

Hvordan kommuniseres arbeidet med informasjonssikkerhet ut i organisasjonen?

Kommunen har flere kanaler som brukes til å kommunisere arbeidet med informasjonssikkerhet ut i organisasjonen. Dette fra informasjonssikkerhetsrådet på kommunedirektørnivå til gruppevirksomhet og funksjoner på driftsnivå. Også intranett, opplæringsplaner tildelt den enkelte ansatt og andre e-kurs blir brukt for å gjøre informasjonssikkerhetsarbeidet kjent i organisasjonen.

Kjennskap til retningslinjer og rutiner for informasjonssikkerhet

Kommunens sentraladministrasjon oppfattes å ha god kjennskap til det overordnede styringssystemet for informasjonssikkerhet, men kjennskapen reduseres i takt med nivået den ansatte befinner seg på. Dette er ikke unaturlig. Det viktige er derimot at ansatte er kjent med bestemmelser og rutiner som inngår i deres utøvelse av faktisk arbeid. Spørreundersøkelsen avdekker at flere ansatte ikke kjenner til rutinene og at de ønsker mer opplæring. Obligatoriske opplæringsplaner i informasjonssikkerhet er i liten grad gjennomført, og funn tyder på at dette ikke blir identifisert og fulgt opp av leder. Vår konklusjon er at ansatte i virksomhetene ikke har så god kjennskap til retningslinjer og rutiner knyttet til informasjonssikkerhet, og at kommunen derfor bør sikre at flere får opplæring i informasjonssikkerhet.

Etterlevelse av kravene til informasjonssikkerhet?

Kommunen har et gjennomgående styringssystem for informasjonssikkerhet, og vurderes i stor grad å legge til rette for at informasjonssikkerheten kan ivaretas. Ansattes manglende kjennskap til retningslinjer og rutiner svekker derimot etterlevelse og kommunens ivaretakelse av kravene, og viser derav behov for tiltak.

Kommunens praksis knyttet til utsendelse av sikkerhetsinstruksen ved ansettelse sikrer ansattes signering av sikkerhetsinstruksen. Det er derimot en vei å gå fra signering til etterlevelse, noe både spørreundersøkelse, protokollføring og intervju gir et innblikk i. Også gjennomført kontroll av sikker sone, avdekker avvik knyttet til skjerming av sensitiv informasjon både i papir- og elektronisk form. Gjennomgangen tyder på at skolenes etterlevelse av krav til personvern utfordres når henvendelser kommer per epost og SMS, noe som utgjør en risiko mht. dokumentasjon av denne type korrespondanse. Det vurderes derfor som hensiktsmessig at skolene har en jevnlig gjennomgang av rutiner og praksis knyttet til dette.

Arbeidet knyttet til protokollføring er omfattende og krever fortløpende oppfølging, samt god kjennskap til rutiner og krav. Systemet oppfattes som både sårbart og komplekst, og både intervju og spørreundersøkelse tyder på usikkerhet knyttet til hvem som skal protokollføre. Dette mener vi utgjør en sårbarhet gjeldende ivaretakelse av krav om behandlingsoversikt.

Kommunen er kjent med at deres protokoll for behandlingsaktivitet[2] av personopplysninger er ufullstendig. At det nå arbeides med å få på plass en protokoll og oversikt som er lettere å følge opp er bra, men også det vil kreve at ansatte som skal være involvert i systemregistrering og protokollføringen er kjent med sitt ansvar. Her tyder funn på at flere systemansavelige ikke er kjent med oppgaver som ligger til rollen. Vi mener derfor at det er viktig å sikre at systemansvarlige er kjent med ansvaret knyttet protokollføring og systemregistrering, og at dette blir kommunisert til ansatte i virksomhetene.

I hvilken grad bruker kommunen avvikssystemet til læring og forbedring?

Kommunen har rutiner og retningslinjer for å oppdage og rapportere avvik, men undersøkelsen viser behov for å øke oppmerksomheten omkring avvikshåndtering, som en del av læring og forbedring i organisasjonen. Det er positivt at avviksrapporteringen har økt jevnlig de siste årene, men det ser fortsatt ut til å være en underrapportering, noe som kan skyldes meldingskulturen.

Vi vurderes et behov for å gjøre rutiner knyttet til melding av avvik mer kjent og at det i større grad kan legges til rette for rapportering av avvik. Avviksmeldinger som danner grunnlag for endring og forbedring bør også synliggjøres. Vi anbefaler derfor at det etableres forventninger og

[2] Alle virksomheter som behandler personopplysninger, skal føre en protokoll over behandlingsaktivitetene de har ansvar for.

rutiner for gjennomgang av avvik på virksomhetsnivå, slik at systematiske problem/feil kan identifisere og videre bidra til læring og forbedring i praksisfeltet.

Anbefalinger

Samlet sett anbefales kommunen å:

- øke gjennomføringsgraden av den obligatoriske opplæringsplan om informasjonssikkerhet
- vurdere tiltak som kan sikre at ledere nyttiggjør seg funksjoner som gir oversikt på gjennomførte/ikke gjennomførte planer, slik at dette følges opp.
- sikre at systemansvarlige er kjent med hva rollen innebærer av ansvar knyttet til protokollføring av behandlingsaktivitet, slik at dette blir gjennomført ihht. krav.
- vurdere om det skal stilles krav til virksomhetene/skolene om jevnlig gjennomgang av rutiner og praksis knyttet til behandling av henvendelser per epost og sms
- legge til rette for en åpen å støttende meldingskultur
- vurdere om det skal iverksettes bevisstgjørende tiltak/ytterlig opplæring knyttet til rapportering av avvik som omhandler informasjonssikkerhet og personvern
- sikre systematisk oppfølging av avvik også på virksomhetsnivå

KOMMUNEDIREKTØRENS KOMMENTAR

Kommunedirektørens kommentar mottatt 05.05.2023:

Kommunedirektøren takker Rogaland Revisjon for arbeidet med avlagt rapport om Stavanger kommunes håndtering av informasjonssikkerhet. Anbefalingene rapporten peker på vil inngå som et ledd i vårt kontinuerlige forbedringsarbeid.

Kommunedirektøren har over tid arbeidet strukturert med tematikken informasjonssikkerhet og personvern. Kommunedirektøren har blant annet løftet frem informasjonssikkerhet og personvern som ett av fem satsningsområder i inneværende handlings- og økonomiplan. Ivaretakelse av informasjonssikkerhet og personvern er blitt løftet frem som et viktig satsningsområde i den nylig vedtatte digitaliseringsstrategien.

Som et ledd i dette arbeidet ble seksjon for informasjonssikkerhet og personvern opprettet i august 2022. En del av denne seksjonens ansvarsområde er å videreutvikle og kontinuerlig forbedre den styrende dokumentasjonen innen informasjonssikkerhet og personvern, som i sum utgjør kommunens styringssystem for informasjonssikkerhet og personvern.

Denne forvaltningsrevisjonen hadde oppstart i juni 2022, og har pågått lenge. Dette innebærer at det har skjedd mye godt arbeid innen dette fagfeltet mens forvaltningsrevisjonen har pågått.

Kommunedirektøren deler Rogaland revisjons vurdering om at «kommunen har et gjennomgående styringssystem for informasjonssikkerhet, og vurderes i stor grad å legge til rette for at informasjonssikkerheten kan ivaretas».

Kommunedirektøren registrerer at rapporten har et stort fokus på skolesektoren. Dette er forståelig, gitt oppmerksomheten det har vært rundt personvernet i skolen. Likevel ønsker kommunedirektøren å påpeke at det hadde vært en styrke for rapporten om Rogaland Revisjon hadde gjennomført intervjuer med representanter fra større deler av kommunens organisasjon.

Rapporten inneholder gode lærlingspunkter som vil bli adressert og fulgt opp. Kommunedirektøren ønsker særlig å trekke frem behovet for å gjøre informasjon om rutiner og retningslinjer innen informasjonssikkerhet og personvern bedre kjent i organisasjonen, herunder det å øke svarprosenten for de obligatoriske opplæringsplanene. Vi er avhengige av årvåkne og kompetente ansatte for å ivareta informasjonssikkerheten og personvernet i tjenesteleveransene våre, og for å legge til rette for trygg digitalisering.

1 INNLEDNING

1.1 BAKGRUNN

Nasjonal sikkhetsmyndighet (NSM) viktigste budskap inn i 2022 var at toppledere måtte prioritere å beskytte seg og samfunnet enda bedre i tiden fremover[3]. Dette var før krigen i Ukraina startet. I kjølvannet av dette melder SINTEF[4]og Datatilsynet om økt risiko for cyber- og nettverksangrep[5].

Kontrollutvalget i Stavanger kommune vedtok 28.03.2022 en forvaltningsrevisjon av Informasjonssikkerhet.

1.2 REVISJONSKRITERIER

Revisjonskriterier er elementer som inneholder krav eller forventninger, og vil bli brukt til å vurdere funn i de undersøkelser som gjennomføres. Kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. I dette prosjektet legges følgende kilder til grunn for utvikling av revisjonskriterier:

- Kommuneloven
- eForvaltningsforskriften
- Krav til informasjonssikkerhet i personopplysningsloven med forskrifter
- Føringer og veiledere for informasjonssikkerhet fra nasjonale veiledningsaktører
- Politiske vedtak, mål og føringer
- Administrative retningslinjer, mål, føringer o.l.

En nærmere beskrivelse av bakgrunn og utledning av revisjonskriterier kommer frem i faktadelen.

1.3 METODE

I prosjektet har vi gjennomgått relevante dokumenter, planer, rutiner, retningslinjer, veiledere, interne kontroller og systembeskrivelser fra kommunen. Også tidligere gjennomførte revisjoner og Sikker sone kontroller er tatt som vurderingsgrunnlag. Noen av skolene som var del av Sikker sone kontrollen er også del av denne forvaltningsrevisjonen.

[3] NSM Risiko 2022
[4] SINTEF er et av Europas største uavhengige forskningsinstitutter.
[5] 12 ting du må vite om cybersikkerhet (sintef.no) Økt risiko for nettverksangrep | Datatilsynet

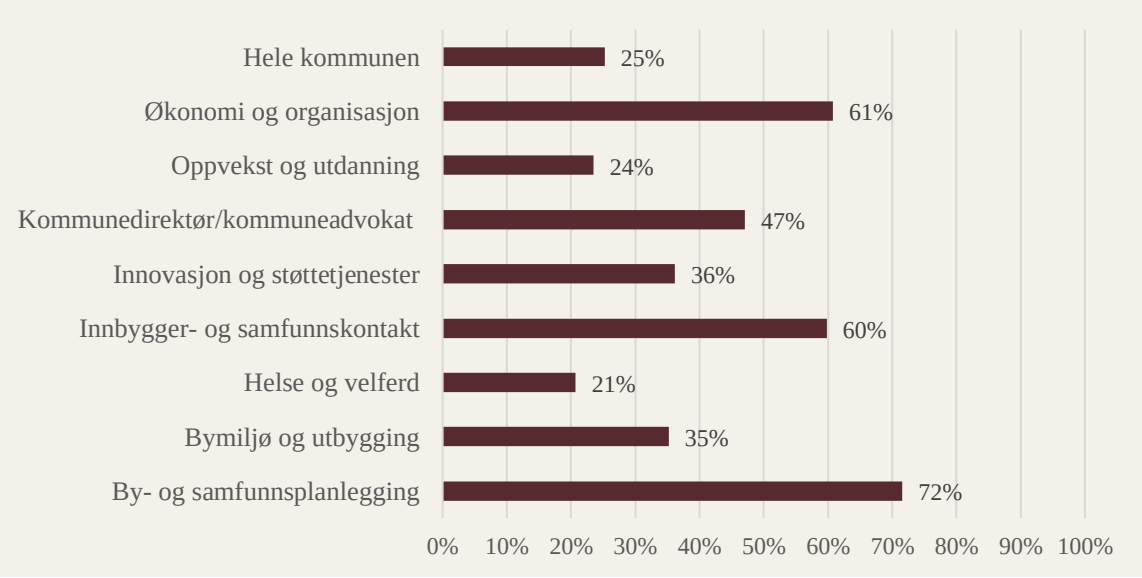
Vi har intervjuet totalt 25 personer i kommunen, hvorav 19 er fra skole. Øvrige intervjuede fra Oppvekst og utdanning er Leder for forvaltning, samt rådgiver for personvern- og informasjonssikkerhet. Fra direktørområde Innovasjon og støttetjenester er Seksjonssjef IT-systemforvaltning, seksjonssjef Informasjonssikkerhet og personvern, rådgiver/ prosjektleder for Vigilo[6]) og personvernombud intervjuet. Det er gjennomført gruppeintervju med rektor, avdelingsleder og miljøveileder ved to av skolene. Øvrige intervju er gjennomført individuelt. Alle intervju er verifisert.

Utvalg av skoler er gjort i samarbeid med kommunen, blant annet basert på tjenesteområdets størrelse (størst) og geografisk beliggenhet/spredning.

Det er også gjennomført en spørreundersøkelse om informasjonssikkerhet. Denne ble sendt ut til 11 560 ansatte, og omfatter alle ansatte i kommunen med stilling over 0 prosent. Nærmere 3000 har besvart spørreundersøkelsen, noe som gir en svarprosent på 25. Svarprosenten varierer mellom tjenesteområdene, fra 21 prosent til 72 som vist i figuren under. Tjenesteområdene med lavest svarprosent er de som i mindre grad bruker PC eller mobil i arbeidshverdagen. I de tilfeller det i rapporten blir vist til spørreundersøkelsen, omhandler dette svar fra hele organisasjonen, ikke utelukkende Oppvekst og utdanning eller skolesektoren.

Selv om svarprosenten kun utgjør ¼ del av kommunens ansatte, er likevel antallet respondenter høyt. Dette mener vi gir et tilstrekkelig grunnlag til å danne oss et bilde av de kommuneansattes synspunkter omkring informasjonssikkerhet.

Figur 1: Svarprosent på spørreundersøkelse om informasjonssikkerhet



Kilde: Rogaland Revisjon IKS

[6] Fagsystem for skole, barnehage og SFO

Kommunens egen undersøkelse i internkontroll kalt Leders sjekkliste, samt statistikk for gjennomføring av e-læring er også med i vurderingsgrunnlaget. Nærmere om datagrunnlaget i de ulike kapitlene.

Vår vurdering er at metodebruk og kildetilfang har gitt et tilstrekkelig grunnlag til å besvare prosjektets formål og de problemstillinger kontrollutvalget vedtok.

1.4 AVGRENSNING

Denne forvaltningsrevisjonen retter søkelyset på hvordan kommunen arbeider med organisatoriske tiltak for å ivareta informasjonssikkerhet, med noe ekstra oppmerksomhet rettet mot skolesektor.

1.5 TIDLIGERE REVISJONER OG KONTROLLER

Her følger en kort oppsummering av tidligere gjennomført revisjoner og kontroller som omhandler informasjonssikkerhet.

1.5.1 FORVALTNINGSREVISJON

Rogaland Revisjon gjennomførte i 2018/2019 en forvaltningsrevisjon av informasjonssikkerhet, drift, og sårbarhet.[7] Revisjonen vurderte kommunens systemer og rutiner forinformasjonssikkerhet, med spesielt henblikk på kommunens organisatoriske tiltak. Revisjonens hovedinntrykk var at kommunen i stor grad hadde system og prosedyrer som ivaretok informasjonssikkerhet, og at det var flere tekniske løsninger implementert/planlagt gjennomført, som ville overvåke systemet og varsle mulige trusler. Det kom frem at flere av kommunens egne rutiner for årlige gjennomganger og revisjoner ikke ble overholdt. Det var dermed en risiko for at kommunen ikke fanget opp viktige endringer i sine mål og strategier.

Revisjonen kom med fem anbefalinger som kommunen har arbeidet med:

- Prioritere en full gjennomgang av informasjonen som ligger på intranett
- Revidere katastrofeplanen for IT årlig, og gjennomføre årlige katastrofeøvelser basert på katastrofeplanen
- Gjennomgå kommunens rutiner for avviksbehandling ved innføring av nytt avvikssystem for å sikre at IT-sjef og sikkerhetsansvarlig er informert om avvik som omhandler brudd på

[7] Forvaltningsrevisjon Informasjonssikkerhet, drift og sårbarhet, Rogaland Revisjon 2019

informasjonssikkerhet. Ved årlig gjennomgang av sikkerhetsmål og -strategi bør gjennomgang av avvik også være en del.
- Gjennomgang og oppdatering av arkivplanen slik at den er i henhold til forskrift
- Registreringer av behandlinger av personopplysninger i Draftit kontrolleres mot tidligere liste over behandlinger som krevde konsesjon og meldeplikt. Behandlingene bør ha en overordnet risikovurdering og status.

Kort oppsummert har kommunen gjort følgende arbeid i etterkant av forrige revisjon[8] :

- Revidert rutiner og ferdigstilt nytt styringssystem for informasjonssikkerhet
- Revidert katastrofeplan for IKT
- Innført nytt avvikssystem (TQM) og etablert system for rapportering til ledelsen
- Oppdatert arkivplan
- Forenklet registrering av behandlinger av personopplysninger (protokollføring)

1.5.2 SIKKER SONE KONTROLL[9]

Rogaland Revisjon gjennomfører årlige en sikker sone-kontroller i kommunen. Frem til 2020 ble virksomheter innen Helse og velferd kontrollert, mens det fra 2021 er gjennomført kontroller i virksomheter under Oppvekst og utdanning. Siden 2017 er rundt 150 virksomheter kontrollert med spørreundersøkelse, fysisk besøk og intervju. Funn avdekker blant annet behov for veiledning i systemer, manglende rutiner ved behandling av sensitive data/opplysninger, og etterlevelse av personopplysningsloven og forskrifter med tilhørende krav. Sikker sone kontroll ble sist utført 23.11.2022. Denne konkluderer med at skolene i all hovedsak etterlevde regelverket for informasjonssikkerhet, men det registreres noen avvik. Kommunen er anbefalt å:

- Jevnlig gjennomgang av taushetsplikt og sikkerhetsreglement med forskjellige eksempler innen informasjonssikkerhet, som er tilpasset skolene
- Tilgjengelige veiledninger innen rutiner og systemer for informasjonssikkerhet, tydelig plassering hvor man finner dette
- Kurs tilpasset skolens bruk av systemer
- Mal for notat på fremvist politiattest i Public 360, som inkluderer felt for navn, dato fremvist, dato på attest og eventuelle kommentarer
- Fokus på hvem som rapporterer, hva som rapporteres og korrekt bruk av hendelsestyper i Si ifra, samt tiltak, oppfølging og tilbakemelding på rapporterte avvik

[8] Kilde: Oppfølging av rapporten «Informasjonssikkerhet, drift og sårbarhet» arkivsak-dok. 17/00014-8. Møtedato 22.10.2019

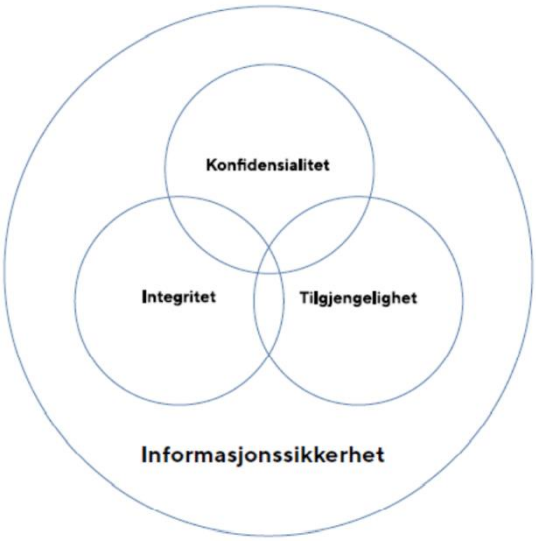
[9] Gjennomføres årlig av Rogaland Revisjon

- Skolekonsulent som arkivansvarlig ved skolene, med full tilgang, inkludert å kunne opprette saker i Public Oppvekst
- Varslingssystem for skarpe situasjoner eller utagering ved skolene

1.6 HVA ER INFORMASJONSSIKKERHET?

Informasjonssikkerhet handler om vern av alle typer informasjon slik at informasjonen ikke blir gjort kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet (integritet) og er tilgjengelig ved behov (tilgjengelighet)[10], se fFigur 22.

Figur 2: Illustrasjon av begreper innen informasjonssikkerhet



Kilde: Stavanger kommune

Det er vanlig å dele inn det praktiske informasjonssikkerhetsarbeidet i to kategorier; *organisatoriske tiltak* og *tekniske tiltak*. På den tekniske siden har Stavanger kommune en IT-avdeling som skal jobbe systematisk med sikkerhet. Inkludert i tekniske tiltak har kommunen varslingssystem for digital infrastruktur gjennom Nasjonal sikkerhetsmyndighet (NSM)[11]. Organisatoriske tiltak innebærer strukturer, tydelige rolle- og ansvarsbeskrivelser, og relevante rutiner og retningslinjer i kommunen. Operativt krever dette nødvendig dokumentasjon, som ROS- analyser, DPIA-analyser[12], databehandleravtaler, samt kontinuitetsplaner for systemer. I organisatoriske tiltak inngår også utvikling og forbedring av styringssystemet for informasjonssikkerhet og personvern, og kompetansehevende tiltak for alle ansatte.

[10] DIGDIR – En forutsetning for å nå virksomhetens mål
[11] Varslingssystem (VDI) - Nasjonal sikkerhetsmyndighet (nsm.no)
[12] Data Protection Impact Assessment (DPIA)– En vurdering av personvernkonsekvenser som skal sikre at personvernet til de som er registrert i løsningen ivaretas.

2 ER INFORMASJON TILGJENGELIG OG KJENT?

I dette kapittelet vil vi se nærmere på hvordan arbeidet med informasjonssikkerhet kommuniseres ut i organisasjonen og i hvilken grad ansatte, på alle nivå, har kjennskap til retningslinjer og rutiner for informasjonssikkerhet.

2.1 REVISJONSKRITERIER

Kommunen skal, etter personvernforordningen artikkel 24, gjøre organisatoriske tiltak for å ivareta krav knyttet til informasjonssikkerhet og personvern. Tiltakene skal gjennomgås jevnlig og skal oppdateres ved behov. Ifølge Datatilsynets veileder for internkontroll[13] vil dette i praksis bety å lage rutiner som beskriver hvordan informasjon skal behandles for å oppfylle lovkrav. Veilederen peker også på at opplæring er viktig for å kunne etterleve lovkrav: *«Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.»*.

Ifølge kommunens rollebeskrivelser skal alle ansatte kjenne til kommunens retningslinje og rutiner for informasjonssikkerhet. Ansatte må ha tilstrekkelig kunnskap for å utføre sine arbeidsoppgaver på en god måte, og med økt bruk av digitale verktøy kreves det også opplæring i disse. Utilstrekkelig opplæring gir økt risiko for brukerfeil som kan gi konsekvenser for informasjonssikkerheten. Digitalisering introduserer også virksomheten for nye trusler. Tekniske barrierer hindrer de fleste angrep, men ikke alle. Det er derfor viktig at ansatte har kunnskap om sårbarheter i digital sikkerhet. Tilstrekkelig og relevant opplæring innen informasjonssikkerhet er et eget krav i standard for administrasjon av informasjonssikkerhet (ISO 27002).

I Stavanger kommunes «*Retningslinje for informasjonssikkerhet*» påpekes at alle ledere og ansatte skal få tilstrekkelig opplæring. Digitaliseringsdirektoratet fremhever kompetanseutvikling som en viktig del av internkontroll for informasjonssikkerhet. Felles forståelse og praksis bygger en god sikkerhetskultur, som bidrar til at sikkerhetstiltak ivaretas. Kommunikasjon er en annen internkontrollaktivitet og forutsetning for god kontroll. For eksempel skal nye føringer kommuniseres nedover i organisasjonen. Kommunikasjon oppover er også viktig for å gi godt beslutningsgrunnlag, som å informere om etterlevelse av tiltak, innspill til forbedringer, status for risikovurderinger osv.

Veileder for informasjonssikkerhet har et eget punkt for kommunikasjon som gjelder alle ledere, som «*har ansvar for å jevnlig kommunisere viktigheten av å følge opp det systematiske*

[13] Virksomhetenes plikter, informasjonssikkerhet og internkontroll

informasjonssikkerhetsarbeidet.» Veilederen sier også at informasjonssikkerhetsansvarlige har *«et særskilt ansvar for å sørge for at viktigheten av informasjonssikkerhetsarbeidet er på agendaen i de ulike tjenesteområdene, og at relevant informasjon flyter ut i linjeorganisasjonen»*. Videre stilles det krav til ledere på alle nivå om å kontinuerlig identifisere behov for kompetanse og kulturutvikling, samt systematisk følge opp disse behovene.

I kommunens rollebeskrivelse for ansatte står det at *alle har ansvar for å gjennomføre den tildelte individuelle opplæringsplanen*. Videre at opplæringsplanen skal gjennomføres for å sikre tilstrekkelig kompetanse på alle systemer som brukes i arbeidet. Den grunnleggende opplæringsplanen som gjeldende for alle ansatte inneholder tre moduler som gir grunnleggende kunnskap om informasjonssikkerhet. Ansatte som bruker IKT mye i arbeidet, har i tillegg fire ekstra moduler om informasjonssikkerhet, som går mer i dybden på å sikre informasjon i arbeidet.

Videre heter det i brosjyren «Informasjonssikkerhet i Stavanger» 2021 at alle ansatte må «*kjenne til Stavanger kommunes retningslinjer for informasjonssikkerhet, herunder rutiner for varsling av informasjonssikkerhetshendelser i «Si ifra!»*».

På bakgrunn av dette er følgende revisjonskriterier utledet:

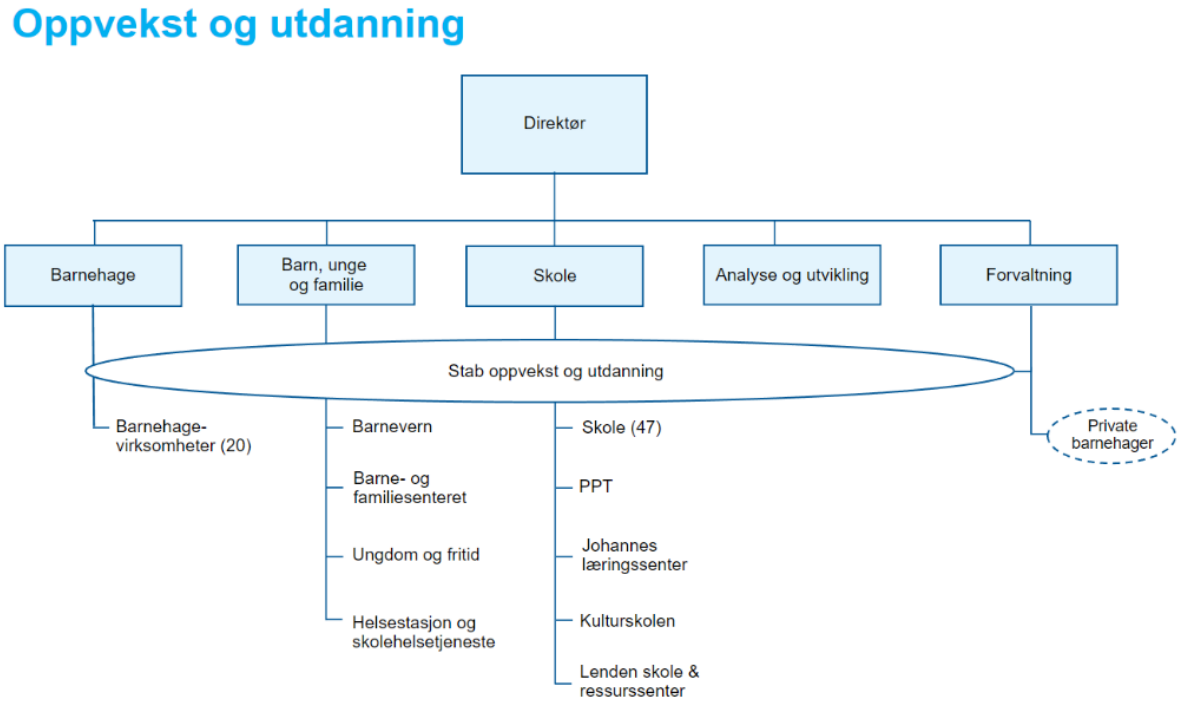
- Ansatte kjenner til rutiner, retningslinjer og riktig bruk av informasjonssystemer
- Ansatte gjennomfører tildelt opplæringsplan
- Ledere identifisere og følge opp behov for opplæring

2.2 ORGANISERING AV INFORMASJONSSIKKERHETSARBEIDET

Stavanger kommune har syv tjenesteområder. I dette prosjektet rettet vi oppmerksomheten mot Oppvekst og utdanning, som inkluderer direktørens stab[14] (markert med blått) og fire skoler.

[14] Staben er tjenesteuavhengig. Det betyr at de ansatte kan jobbe innenfor flere fagområder.

Figur 3: Organisasjonskart Oppvekst og utdanning



Kilde: Stavanger kommune

Organisasjonsstrategien i Stavanger kommune bygger på helhetlig ledelsesprinsipp, som betyr at hver enkelt leder har ansvar for det som skjer innenfor sitt område. Dette inkluderer internkontroll innen informasjonssikkerhet og at arbeidet skal være tilpasset helheten i organisasjonen.

2.2.1 ROLLER OG ANSVAR I INFORMASJONSSIKKERHETSARBEIDET

Direktør i Innovasjon og støttetjenester har et delegert ansvar som informasjonssikkerhetsleder for hele Stavanger kommune. Det innebærer et overordnede ansvar for det strategiske informasjonssikkerhetsarbeidet og et ansvar for at arbeidet understøtter kommunens retningslinjer for informasjonssikkerhet. Hver direktør er i tillegg informasjonssikkerhetsansvarlig for sitt tjenesteområde, som blant annet betyr å sikre at en hensiktsmessig organisering som understøtter kommunens retningslinjer for informasjonssikkerhet.

Tjenesteområdet Innovasjon og støttetjenester har ansvar for å sette rammer og legge føringer for informasjonssikkerhetsarbeidet. I tjenesteområdet finner vi seksjon for informasjonssikkerhet, som blant annet utarbeider rutiner og retningslinjer, gir råd, støtte og veiledning til hele organisasjonen, samt legger til rette for kompetansehevende tiltak. Vi finner også kommunens personvernombud i dette tjenesteområdet. Personvernombudet har derimot en selvstendig og uavhengig rolle i kommunen. Gjeldende informasjonssikkerhetsarbeid har ombudet hovedsakelig en rådgivende og kontrollerende funksjon i forhold til personvern.

Informasjonssikkerhetsrådet er «*…et rådgivende organ, hvor medlemmene støtter opp om, og følger opp vedtak*»[15]. Rådet skal sørge for helhetlig styring og kontroll av informasjonssikkerhetsarbeidet i kommunen. Rådets medlemmer er direktørene, IT-sjef, rådgiver informasjonssikkerhet fra IT og personvernombud. Disse skal sikre en god forankring, koordinering på tvers- og etterlevelse av retningslinjer i de ulike tjenesteområdene. Som saksforberedende organ for kommunedirektørens ledergruppe (KLG) utarbeider rådet et årlig saksnotat for gjennomgang av informasjonssikkerhetsarbeidet.

Ressursgruppe personvern skal bidra til at kommunen behandler personvernopplysninger iht. regelverket. Formålet er erfaringsutveksling relatert til praktisk arbeid med personvern i kommunen og samhandling på tvers av tjenesteområdene. Rådet skal være representert med minst ett medlem med en form for personvernansvar, fra hvert tjenesteområde. Det er informasjonssikkerhetsrådet (det vil si direktørene, IT-sjef, rådgiver informasjonssikkerhet fra IT og personvernombud) som bestemmer medlemmene i denne gruppen. Møtehyppighet er minimum annenhver måned.

Flere av kommunens ansatte har arbeidsoppgaver som helt eller delvis handler om ivaretakelse av informasjonssikkerhet. Disse er underlagt ordinær linjeledelse, og har gjennom sine arbeidsoppgaver et særlig ansvar for å støtte de informasjonssikkerhetsansvarlige innen sitt ansvarsområde. Oppgavene til disse rollene varierer ut fra hvor i organisasjonen de er ansatt. Januar 2022 fikk Oppvekst og utdanning en rådgiver dedikert til informasjonssikkerhetsarbeid i tjenesteområdet. Vi får opplyst at det er planlagt å øke rådgiverressursen med ytterligere én stilling i 2023.

2.2.2 RUTINER FOR INFORMASJONSSIKKERHET

Retningslinjene for informasjonssikkerhet og personvern gjelder alle ansatte i kommunen, og er utarbeidet etter Digitaliseringsdirektoratet, Datatilsynet og NSM sitt veiledningsmateriell. I forbindelse med revidering av kommunens styringsdokument i 2021, blir tjenesteområdenes informasjonssikkerhetsansvar presisert og tydeliggjort. Det blir også opprettet egne temasiden for informasjonssikkerhet og personvern på intranett. Dette for å sette rammer og retning for det videre arbeidet.

Brosjyren[16] «*Informasjonssikkerhet i Stavanger kommune*» fra 2021 sier blant annet at:

> *Alle ansatte i Stavanger kommune har et ansvar for å bidra til at kommunen når informasjonssikkerhetsmålet. Dette betyr at alle ansatte må ha kunnskap om hvilken betydning informasjonssikkerhet har for deres arbeidsoppgaver, og hvordan de kan utføre arbeidet sitt på en måte som ivaretar informasjons-sikkerheten. Alle ansatte må blant*

[15] Mandat Informasjonssikkerhetsrådet, Stavanger kommune
[16] Tilgjengelig både fysisk og på intranett

annet ha forståelse for trusler og risiko tilknyttet sine arbeidsoppgaver, og ha forståelse for hvordan uønskede hendelser kan hindre måloppnåelse, eller få konsekvenser for andre parter. Alle ansatte må i tillegg kjenne til Stavanger kommunes retningslinjer for informasjonssikkerhet, herunder rutiner for varsling av informasjonssikkerhetshendelser i «Si ifra!».

Flere av kommunens rutiner og retningslinjene, som er tilgjengelige på intranett, inneholder ansvarsfordeling, begrepsforklaringer, lovgivning, samt konkretiserer arbeidet med informasjonssikkerhet i kommunen.

I kommunens overordnede Sikkerhetsreglement[17] står blant annet:

- Være varsom med å kommunisere med brukere og pårørende på e-post og SMS ved fare for å røpe klientforhold, samt at korrespondanse skal slettes når kommunikasjonen er dokumentert i relevant fagsystem eller når man har besvart meldingen.
- Sosiale medier og andre direktemeldinger/chat skal ikke brukes til formidling av taushetsbelagt informasjon.
- Taushetsbelagte personopplysninger skal lagres i aktuelt fagsystem, ikke på PC, minnepenn, «skyen»[18] eller kommunenes nettverk.
- Man skal ikke oppsøke tilgang til taushetsbelagt informasjon man ikke har behov for, eller opptre på en måte som gjør disse tilgjengelige for uvedkommende.
- Skjermbeskytter skal aktiveres hver gang man forlater arbeidsplassen.
- Ingen skal låne ut brukernavn eller passord, eventuelt bytt passord dersom noen kan ha fått tilgang til dette.
- Kommunens avvikssystem skal benyttes til å rapportere sikkerhetsbrudd til nærmeste leder.

Neste tabell gir en oppsummert oversikt over kommunens interne retningslinjer/rutiner for informasjonssikkerhet:

Tabell 1: Interne styringsdokumenter for informasjonssikkerhet

Dokument(er)	Sist endret/godkjent	Innhold
Sikkerhetsreglement	Oktober 2022	Generelle og konkrete føringer for kommunens sikkerhetsarbeid, inkludert informasjonssikkerhet
Retningslinje for informasjonssikkerhet	27.10.2022	Generelle retningslinjer for kommunens informasjonssikkerhet
Retningslinjer og rutiner for avvik	27.06.2022	Oversikt av rapportering og rutine for arkivering av avvik

[17] Sikkerhetsreglementet er et sentralt og overordnet styringsdokument, sist endret oktober 2021.
[18] «Skyen» er kallenavn for nettsky eller skytjenester. Dette refererer til datalagring via programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett (Skytjenester | Datatilsynet)

Sjekkliste	22.11.2022	Definisjoner, behandlingsgrunnlag, aktivitet
Veileder for informasjonssikkerhetsarbeidet	24.10.2022	Oversikt av ansvarsområder, informasjonssikkerhetsarbeid og rutiner
Rollebeskrivelser	22.11.2021 12.10.2022	Beskrivelser av system- og appforvaltning Rutine for bruker/ansatte
Regelverk for internkontroll og risikostyring	23.02.2021	Regelverk gjeldende for kommunens administrasjon

Kilde: Stavanger kommune

2.3 INFORMASJONSKANALER OG RESSURSER

Kommunen har ulike informasjonskanaler og ressurser som tas i bruk ved formidling av informasjon til ansatte. Vi skal her se nærmere på noen av dem.

2.3.1 RESSURSER PÅ SYSTEMNIVÅ

Ledergruppen

På overordnet nivå er kommunedirektørens ledergruppe (KLG) en viktig arena for kommunenes informasjonssikkerhetsarbeid. Informasjonssikkerhetsleder har en årlig gjennomgang med KLG, av systemrisiko og andre alvorlige hendelser som krever tiltak eller handling på overordnet nivå. Flere av de som er intervjuet viser til gjennomgangen som viktig i forståelse og oppfatning av status for informasjonssikkerhet det siste året.

Informasjonssikkerhetsrådet

Kommunens informasjonssikkerhetsråd «*er et rådgivende organ, hvor medlemmene støtter opp om, og følger opp vedtak*».[19] Digitalisering og økt sårbarhet samt trusselbildet for 2021 danner grunnlaget for mandatet til Informasjonssikkerhetsrådet. Rådet skal gi støtte og oppfølgning i

[19] Mandat Informasjonssikkerhetsrådet, Stavanger kommune

saker og vedtak. Som saksforberedende organ for Kommunedirektørens ledergruppe skal det årlig utarbeides et saksnotat for gjennomgang av informasjonssikkerhetsarbeidet.

Rådet er sammensatt av direktørene, som også er informasjonssikkerhetsansvarlig for sitt tjenesteområde, og ledet av informasjonssikkerhetsleder. Direktørene har mulighet for å delegere bort medlemskapet, men dersom denne ikke har mulighet til å møte oppfordres direktør til å delta. Andre medlemmer av rådet er IT-sjef, rådgiver informasjonssikkerhet fra IT og personvernombud. Andre aktører kan også inviteres med dersom hensiktsmessig i forhold til møteagenda.

Rådet har i oppgave å påse at informasjonssikkerhetsarbeidet er i tråd med gjeldende lover og forskrifter, og helhetsprinsippet. Det skal sikres etterlevelse og kontinuerlig forbedring, nødvendig fokus og engasjement i organisasjonen, samt nødvendig kompetanse hos ansatte. Medlemmene har ansvar for å videreformidle informasjon gitt i rådet til sitt tjenesteområde hvor de også skal sette informasjonssikkerhet på agendaen, samt løfte utfordringer og erfaringer inn til rådet.

Ressursgruppe Personvern

Personvern er del av informasjonssikkerhetsarbeidet i kommunen. Det er nedsatt en ressursgruppe for personvern[20] bestående av nøkkelpersonell som jobber med personvern og eventuelt informasjonssikkerhet i arbeidshverdagen. Disse blir utpekt av informasjonssikkerhetsrådets medlemmer. Gruppen rapporterer til Informasjonssikkerhetsrådet om aktiviteter i gruppen, saker som er drøftet og møtefrekvens. Personvernombudet er også medlem i ressursgruppen. Øvrige medlemmer er tilhørende de ulike tjenesteområdene i kommunen med minimum en deltaker per tjenesteområde.

Gruppen har som formål å dele erfaring og kompetanse, samt gi anledning til drøfting av saker og tiltak opp mot regelverk. Gruppen er i tillegg et rådgivende organ. Gruppen er tettere på og har større nærhet til tjenesteområdene enn informasjonssikkerhetsrådet. En stor del av arbeidet til gruppen består av å standardisere arbeidsmetoder for behandling av personopplysninger i kommunen.

I intervju blir gruppen beskrevet som en god arena for å drøfte og diskutere avvik og tiltak, og kunnskapsdeling på tvers av tjenesteområdene.

[20] Kilde: Mandat for Ressursgruppe personvern, Stavanger kommune.

Personvernombud

Hovedoppgavene til personvernombudet er blant annet kontroll, rådgivning, kontaktpunkt mellom tilsynsmyndigheten og kommunen, samt tilgjengelig for de registrerte.[21] Videre heter det i personvernforordningen artikkel 38 nr.1. *«Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger»*.

Personvernombudet har hele kommunen som sitt virkeområde og bistår i flere ulike aktiviteter som omhandler personopplysninger. Ved anskaffelse av nye systemer eller applikasjoner skal eksempelvis personvernombudet varsles for sikring av at systemet overholder krav til oppbevaring av personopplysninger. Personvernombud fungerer også som kontaktperson ved melding av avvik til Datatilsynet, og har en rolle i saksbehandling av brudd på personvern.

Personvernombudet har en nøkkelrolle i organisasjonen, og er som nevnt medlem i ulike grupper. Personvernombudet skal være tilgjengelig og har et opplæringsansvar overfor ansatte som behandler personvernopplysninger.

Ifølge intervju må personvernombud og ansatte med rådgivende funksjoner ifm. personvern og informasjonssikkerhet ofte nedprioritere kompetansehevende tiltak til fordel for løpende henvendelser fra virksomhetene. Dette er ofte oppgaver som haster, noe de mener legger beslag på kapasitet til gjennomføring av kompetansehevende tiltak.

Systemansvarlig

Systemansvarlige er representant for brukere av et system/program. De er ansvarlige for fagsystemets «ve og vel» noe som inkluderer den daglige driften. Kommunen har egen rollebeskrivelse for systemansvarlig, hvor det er listet alle deres oppgaver.

Tjenesteområdet Oppvekst og utdanning har en egen gruppe for systemansvarlige med formål å øke bevissthet og kompetanse i flere ledd. Kunnskapsdeling mellom systemansvarlige og mulighet for bistand fra nøkkelpersonell blir oppgitt som nyttig, da kravene til personopplysningsbehandlende systemer er mange. Informasjonssikkerhets- og personvernrådgiver bruker gruppen til å blant annet opplæring i risikovurderinger og protokollføring av behandlingsaktivitet

[21] Personvernforordningen artikkel 38 nr. 4.

2.3.2 INTRANETT

Intranett er kommunens interne nettverk, hvor kun ansatte har tilgang. Intranett brukes til å dele intern informasjon med ansatte. Her publiseres viktige saker som ansatte bør få med seg, som driftsmeldinger fra IT, aktuelle kurs for ansatte, og andre nyheter fra hele kommunen. Her finner vi blant annet kommunens organisasjonskart og de ulike tjenesteområdenes organisering. Hvert tjenesteområde har sin side, hvor de ulike virksomhetene og avdelinger kan legge til viktig informasjon om eller fra avdelingen. Vi finner at de ulike tjenesteområdene har ulik disposisjon og bruk av intranett.

Det ligger flere ulike retningslinjer, rutiner og dokumenter tilgjengelig på intranett. Gjeldende informasjonssikkerhet er noen lett tilgjengelige, mens andre må søkes etter, noe som krever at man vet hva man leter etter.

Styrende dokumentene for informasjonssikkerhet er tilgjengelig på Innovasjon og støttetjeneste sin side for Informasjonssikkerhet. Informasjonssikkerhetsseksjonen har i tillegg lagt til lenker fra Datatilsynet og Digitaliseringsdirektoratet som oppslagsverk/ ulike informasjonssider om temaet. Ved bruk av Microsoft Edge som nettleser er dette automatisk startside på nettleseren.

2.3.3 ÅRLIG SIKKERHETSKAMPANJE

Stavanger kommune tar del i den årlige *Nasjonal sikkerhetsmåned*. Dette er en kampanje som gjennomføres hver oktober, og som har som formålet å øke engasjementet, bevissthet og kunnskap om digital sikkerhet i kommunen. I løpet av kampanjen publiseres ulike innlegg og kursmoduler/nanolæring på intranettet. Det er ikke obligatorisk å delta, men ledere oppfordres til å anbefale sine ansatte til å gjennomføre kurs og lese informasjonen som legges ut.

2.3.4 ANNET

Kommunen har også ulike brosjyrer (fysiske og elektroniske), som påpeker viktigheten av at ansatte i kommunen er bevisste og kontinuerlig oppmerksom på, og ivaretar informasjonssikkerhet og personvern i sin arbeidshverdag. Det henvises også til eksterne kilder som Digitaliseringsdirektoratet og lovverk.

2.4 KUNNSKAP OG KOMPETANSE

Informasjonssikkerhetsrådet, Ressursgruppe personvern og andre grupper i kommunen har som formål å dele kunnskap og erfaring, samt å utligne forskjeller i kunnskap og kompetanse på tvers av tjenesteområder og nivå i organisasjonen. Kommunen har med andre ord flere måter å dele kunnskap og informasjon på. Hver enkelt leder har likevel et ansvar for det som skjer innenfor sin enhet, herunder internkontroll innen informasjonssikkerhet og personvern. En del av dette

ansvaret er å sørge for at den enkelte enheten arbeider i tråd med føringene som er gitt i kommunens styringssystem for informasjonssikkerhet og personvern. Det er dermed et ledelsesansvar å sikre at ansatte har tilstrekkelig kunnskap til å kunne utføre sine oppgaver på en sikker måte, også med tanke på informasjonssikkerhet. I dette delkapitlet tar vi først for oss hvilke kompetansehevingstilbud kommunen har, og gjennomføringen av disse, før vi ser nærmere på ansattes kompetanse og kjennskap til rutiner og retningslinjer.

2.4.1 KOMPETANSEHEVENDE TILTAK

I kommunens handlings- og økonomiplan 2022-2025 er informasjonssikkerhet en satsning, og det er uttrykt at både kapasitet og kompetanse i kommunen skal styrkes. Rutiner, retningslinjer, rollebeskrivelser og sjekklister er alle dokument som definerer og beskriver informasjonssikkehetsarbeidet. *Melding om informasjonssikkerhet* ble gjort tilgjengelig for alle ansatte og folkevalgte i 2021. Det finnes også en oppdatert brosjyre på intranett med tilsvarende innhold. Vi får fra kommunen opplyst at det over tid er satset på digitalisering, og at det som en del av denne prosessen er sett viktigheten av informasjonssikkerhet. Det vises også til at det er et større behov for informasjonssikkerhet og digital sikkerhet i en tid hvor nye trusler og sårbarheter oppstår kontinuerlig.[22] Kommunen har obligatorisk opplæring til ansatte, men har også iverksatt andre tiltak for å heve kompetansen i organisasjonen.

Av kommunens rollebeskrivelse framgår det at ansatte skal fullføre den obligatoriske opplæringsplanen. Denne ble tildelt alle ansatte i 2021 og er etter det tildelt nyansatte. Planen er modulbasert og inneholder informasjon i form av ulike kurs fra ulike avdelinger i kommunens administrasjon. Den kan tilpasses ulike tjenesteområde og leder kan ved gjennomgang av sitt ansvarsområde søke opp ansatte og se hvem som har fullført planen og ikke. Opplæringsplanen skal gjennomføres av den ansatte i løpet av en 12 måneders periode. Opplæringsplanen kan også tas i bruk for opplæring og oppdatering på fag/regler/prosedyrer ut over nyansettelser.

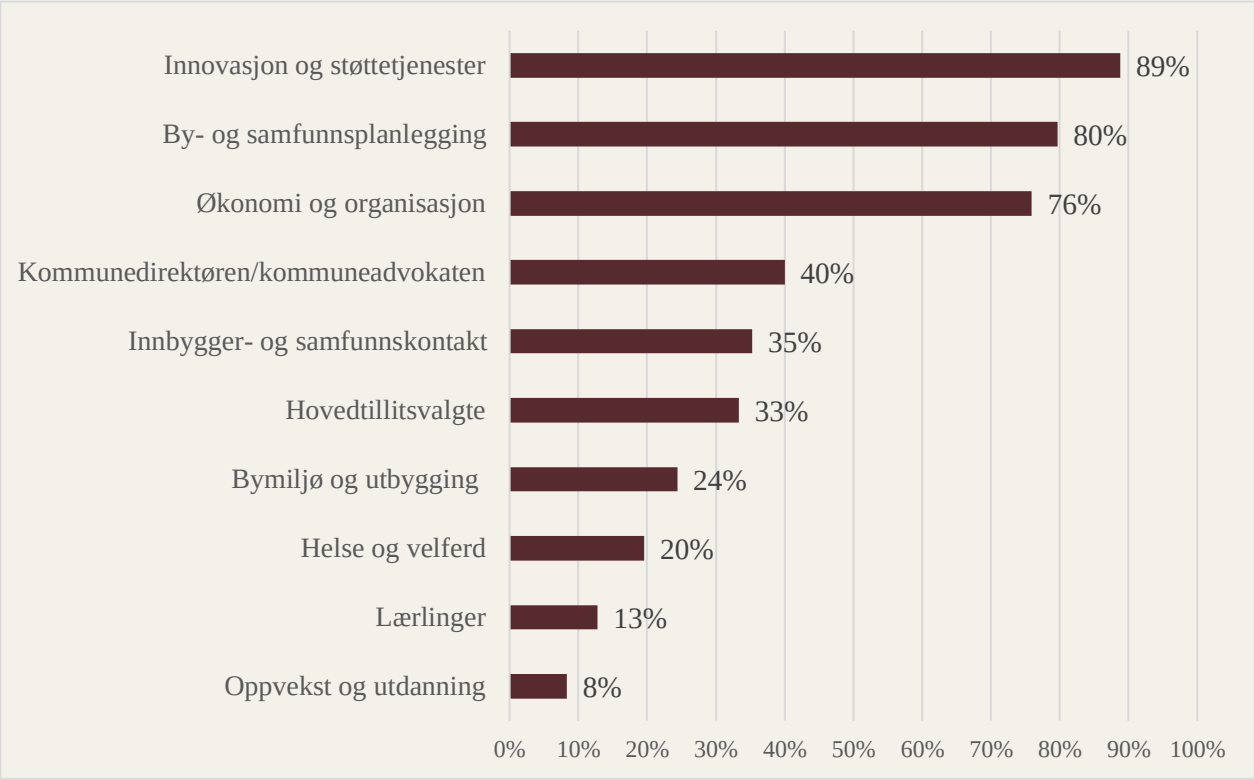
Seksjon for informasjonssikkerhet har tre av 12 moduler/e-læringskurs i opplæringsplan for alle ansatte. Modulene er grunnleggende for informasjonssikkerhet og tar for seg sikkerhet på mobil samt trusler fra IT-kriminelle. Det er også eget kurs i personvern (*Introduksjon til GDPR – personvern).* Ansatte som bruker PC/mobil mye i jobben, har i tillegg 4 e-læringskurs/moduler om fysisk sikkerhet, grunnleggende og utvidet personvern, samt håndtering av sikkerhetshendelser. Kursene skal være enkle nok til at alle ansatte som har behov for dem forstår innholdet, samtidig som de gir en innføring i hvordan ansatte skal opptre i tråd med rutiner og retningslinjer for informasjonssikkerhet.

Tall per 09.01.2023 for gjennomføring av kurs i informasjonssikkerhet og personvern viser at 40 prosent av kommunens ansatte har fullført minst ett krav fra grunnopplæringen (tre moduler). For ansatte som bruker PC og/eller mobil mye i jobben (i alt syv moduler), er tilsvarende tall 42

[22] NSM Risiko 2022, Økt risiko krever økt årvåkenhet

prosent. Prosentandelen som har fullført minst ett krav varierer mellom tjenesteområdene. Her er fullføringsgraden i Oppvekst og utdanning[23], på 8 prosent, klart lavest.

Figur 3: Prosentandel fordelt på tjenesteområde som har fullført minst ett krav i opplæringsplan (de som bruker PC/mobil mye) [24]



Kilde: Stavanger kommune

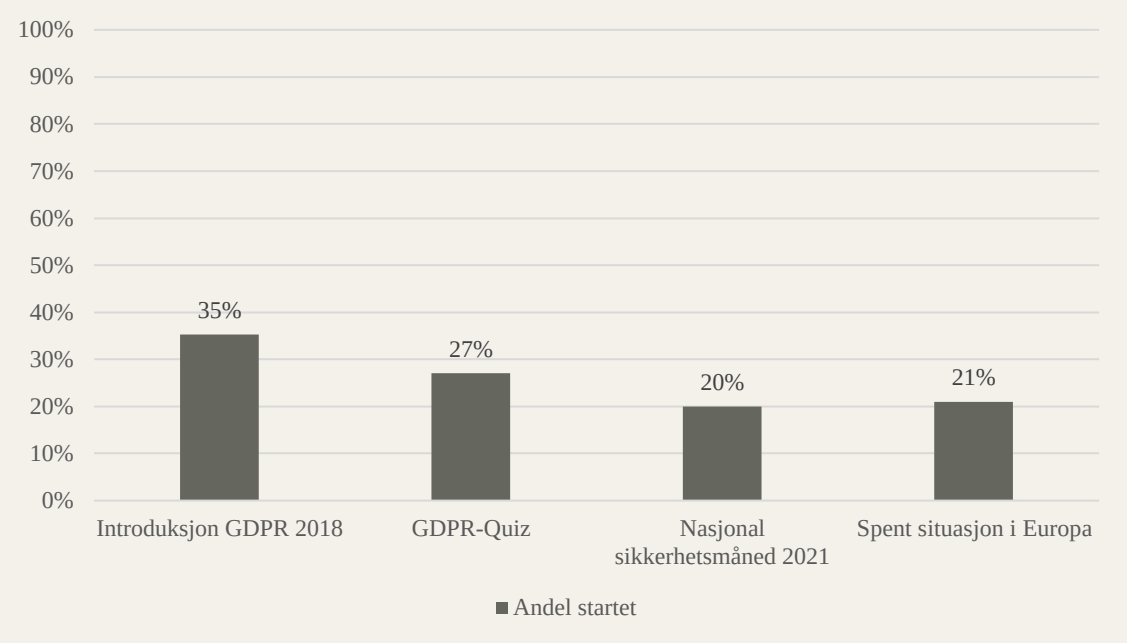
I intervju med skoleansatte mener noen at det ikke blir prioritert tid og ressurser til opplæringen, mens andre forteller at det settes av noe, men ikke nok tid til dette. Vi erfarer at opplæring ved noen skoler blir lagt til fellestid, mens det ved andre skoler er opp til den enkelte å prioritere gjeninnføring. Det blir også påpekt at opplæringen er omfattende.

Utover opplæringsplanen til hver enkelt ansatt, kan ansatte også ta enkeltkurs i form av *nanolæring*[25], som blir brukt i nasjonal sikkerhetsmåned. Disse deles og legges ut av kommunens administrasjon, og ledere blir oppfordre til å videresendes opplæringen til sin del av

[23] Det finnes ikke tall som viser hvor mange som har gjennomført alle de obligatoriske kursene.
[24] Kun kurs i informasjonssikkerhet og personvern. Andel oppgitt i prosent, for ansatte som bruker PC/mobil mye i jobben
[25] Kurs i form av nanolæring innen informasjonssikkerhet er fra KiNS (Foreningen Kommunal Informasjonssikkerhet), laget i samarbeid med Bærum kommune og KS. I intervjuene beskrives kursene som gode og tilstrekkelige.

organisasjonen. Figuren under viser en oppsummering av hvor mange som har startet nanolæring de siste årene.

Figur 4: Prosentandel av alle ansatte som har startet ulike nanolæringskurs 2018-2022



Kilde: Stavanger kommune

Av figuren ser vi at andel ansatte som har startet de ulike nanolæringskursene varierer fra 20 til 35 prosent. Av disse varierer andelen som fullfører kursene mellom 70 og 97 prosent.

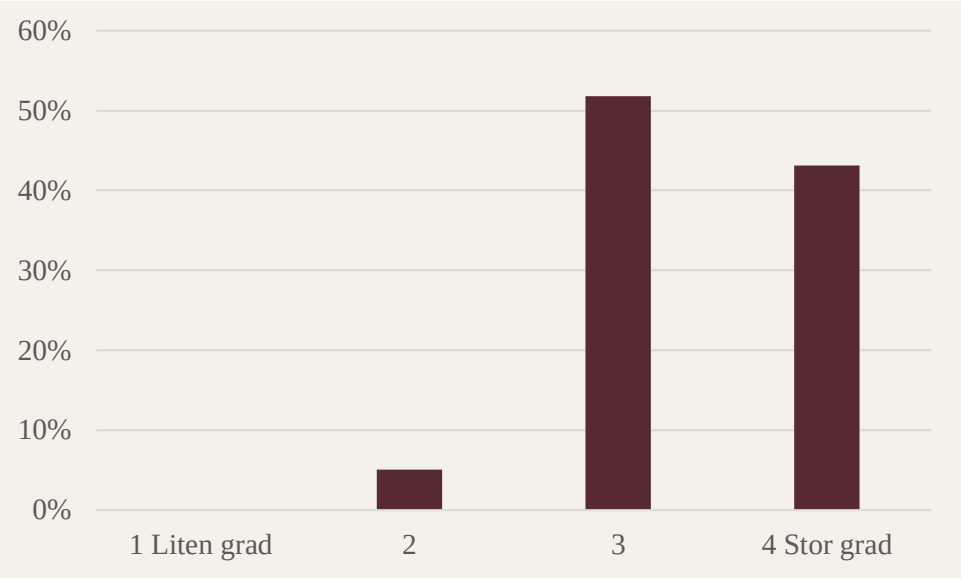
I intervju med skoleansatte sier enkelte at de har gjennomført noen av kommunens kurs i opplæringsplanen, og nanolæringskurs under nasjonal sikkerhetsmåned. Sikkerhetsmåneden er noe som refereres til som s*ikkerhets-uka*, andre er ikke klar over at det er en årlig kampanje, mens enkelte viser til at de nylig har benyttet tiltaket og synes det er en god påminnelse om informasjonssikkerhet.

I forbindelse med revisjonens utsendelse av spørreundersøkelsen, er vi gjort kjent med at direktørområdet Innovasjon og støttetjenester fikk flere henvendelser fra ansatte som lurte på om dette var en sikker link å trykke på.

2.4.2 ANSATTES KOMPETANSE

Kommunen innheter jevnlig informasjon om ansattes kompetanse, kunnskap og ferdigheter om blant annet informasjonssikkerhet og personvern gjennom Leders sjekkliste[26]. Dette som en del av kommunens internkontroll. Svarene som omfatter informasjonssikkerhet for den siste gjennomføring[27], er illustrert i figuren under.

Figur 5: Leders synspunkt på medarbeidernes kunnskap/ferdighet om informasjonssikkerhet



Kilde: Leders sjekkliste, 1. tertial 2022, Stavanger kommune

Svarene utgjør et gjennomsnitt på 3,3 (fra 1 i liten grad til 4 i stor grad). Tjenesteområdene By- og samfunnsplanlegging og Innovasjon og støttetjenester ligger begge over gjennomsnittet med 3,8. Oppvekst og utdanning er eneste tjenesteområdet som ligger under snittet, med en score på 3,2.

I kommentarfeltet pekes det på at de ansattes stillingsprosent spiller inn, og at det skal gjøres tiltak for å styrke kunnskapen. Noen ansatte mener også at e-læring er mindre effektivt enn fysiske foredrag/kurs.

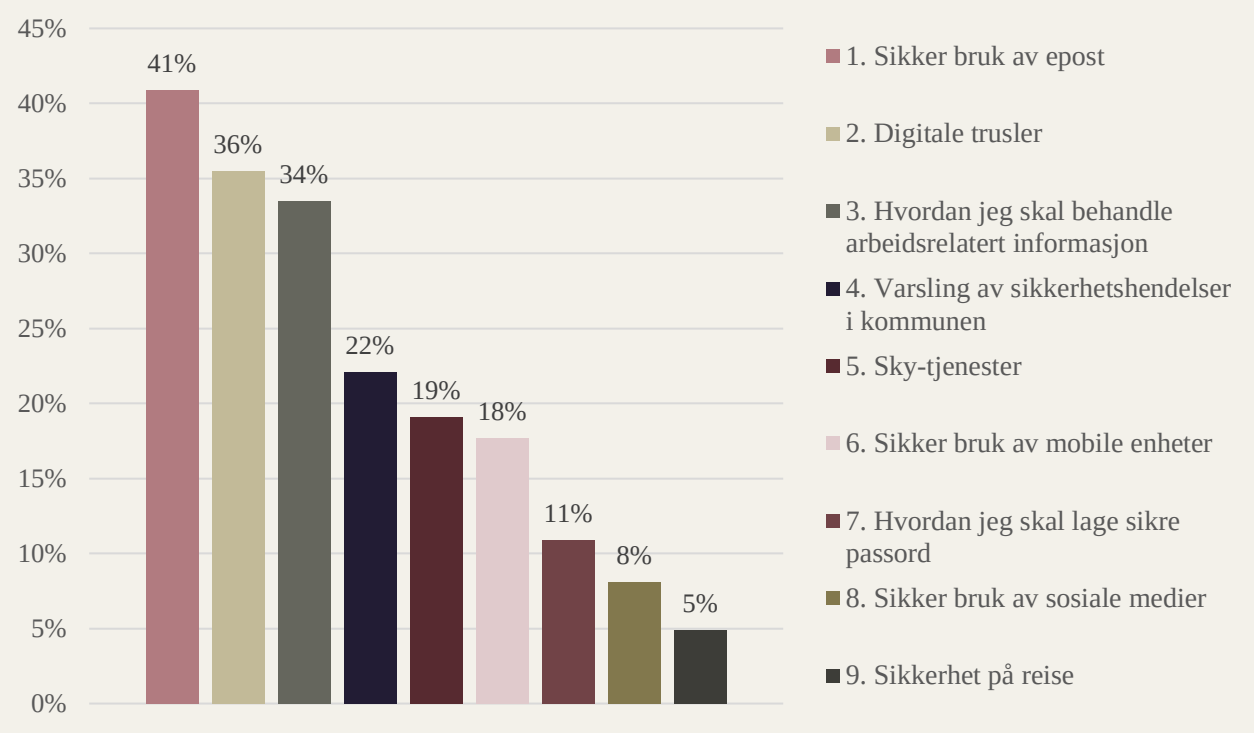
I spørreundersøkelsen finner vi variasjon i hvordan ledere og ansatte vurderer eget kunnskapsnivå. På spørsmål om kompetanse, kunnskap og ferdigheter, både om seg selv og vurdering av ansatte, svarer ledere «i stor grad» oftere enn ansatte. Ansatte vurderer med andre

[26] Leders sjekkliste er en del av virksomhetsstyringssystemet "Plattformen" og består av internkontrollområder som er felles for hele kommunen. Sjekklisten besvares to ganger i året. Punktene variere basert på hvilken periode man er i. Punktene i sjekklisten besvares av kommunalsjefer, avdelingssjefer og virksomhetsledere.
Som leder svares det for egen avdeling eller virksomhet. Som kommunalsjef svares det med bakgrunn i det ansvaret du har ovenfor underliggende enheter / virksomheter.
[27] 1. tertial 2022

ord eget kunnskapsnivå noe lavere enn sine ledere. Dette er også noe som gjenspeiles i intervju, hvor ledere på virksomhetsnivå gir uttrykk for god kompetanse innen informasjonssikkerhet. Ansatte er i større grad usikre på hva informasjonssikkerhet er, i noen tilfeller også hva det betyr i deres arbeid. Eksempelvis var det enkelte ansatte som ikke forstod hvorfor vi skulle intervjue dem om dette temaet.

I spørreundersøkelsen oppgir over halvparten (53%) av respondentene at de ønsker mer kunnskap om digital sikkerhet på jobb. Disse fikk igjen spørsmål om hvilke to områder de anså som viktigst å få mer kunnskap om. Resultatene framgår av figuren under.

Figur 6: Jeg ønsker mer kunnskap om digital sikkerhet på disse områdene (velg de to viktigste) (N=1536)



Kilde: Rogaland Revisjon

Respondentene oppgir her et ønske om mer kunnskap om sikker bruk av epost, digitale trusler og behandling av arbeidsrelatert informasjon. Her er det likevel visse forskjeller mellom ledere og medarbeidere på hva de anser som viktigst å få mer kompetanse om. For lederne og systemansvarlige er digitale trusler som oppgis som viktigst, mens medarbeiderne oppgir sikker bruk av epost som viktigst.

Gjeldende opplæringsplanen og tildelte kurs i denne, blir vi fortalt at lederne i liten grad har oversikt over hvilke kurs de ansatte har fullført. Systemet beskrives som tungvint, da kontroll av opplæring krever at leder manuelt søker opp sine ansatte. På den andre side får vi informasjon om at kompetansemodulen i lønns- og personalsystemet gir god oversikt på dette. Det hevdes at manglende oversikt handler om bevissthet og kompetanse blant respondentene, ikke systemet i

seg selv. Hvorvidt planen er gjennomført er videre et eget punkt i kommunens mal for medarbeidersamtale[28]. Vi får opplyst i intervju at én skole ikke bruker kommunens mal for medarbeidersamtaler, og derfor ikke har opplæringsplanen som et tema i samtalen.

Utover opplæringsplanen kan ledere, ved behov, uttrykke ønske om kompetanseheving fra kommunens nøkkelpersoner på området, som eksempelvis personvernombud eller informasjonssikkerhets- og personvernrådgiver. Samtidig påpeker flere at det både på virksomhetsnivå og blant støtteapparatet er utfordringer med tid og kapasitet, som medfører at kompetanseheving er vanskelig å prioritere. Intervjuene tyder dessuten på at tilbudet om kompetanseheving er lite kjent for skolelederne. Eksempelvis er det i våre intervjuer kun én leder som oppgir å ha bestilt slike kurs.

I intervju uttrykkes at mangel på kompetanse hos ansatte skaper merarbeid. Videre er det flere av de intervjuede som mener at informasjonssikkerhet i Oppvekst og utdanning først ble satt på agenda i 2022, og at det ikke har vært et prioritert arbeid i tjenesteområdet. Vi får derimot opplyst at det nylig er satt av mer ressurser til dette arbeidet på systemnivå, og at det nå arbeides med å «*standardisere arbeid med informasjonssikkerhet for virksomheter*», i forsøk på å begrense merarbeid for nøkkelpersonell.

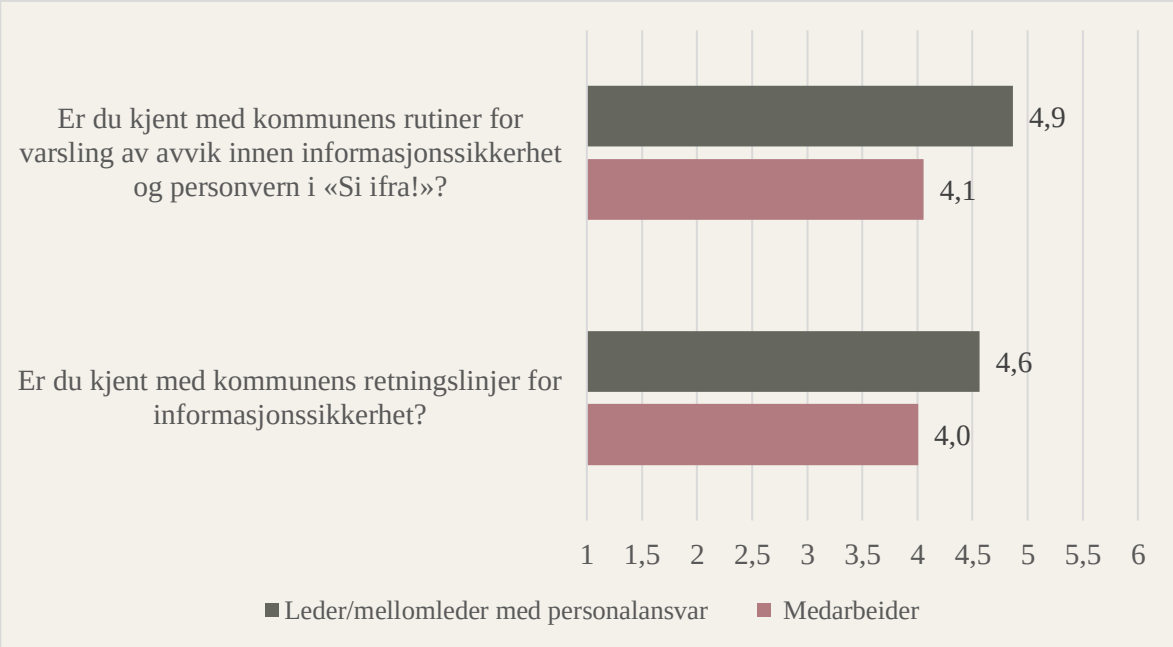
Vi får videre opplyst at informasjon om informasjonssikkerhet ikke er noe alle ansatte finner like nødvendig eller relevant, og flere forteller at informasjonssikkerhet ikke er på møteagendaen i virksomhetene. Informasjon om dette kommer som «små drypp» under møter og på e-post, og flere uttaler de at de er usikre på hva informasjonssikkerhet handler om og om det angår dem. Usikkerheten knytter de til manglende kunnskap.

2.4.3 KJENNSKAP TIL RUTINER OG RETNINGSLINJER

Tilstrekkelig opplæring er viktig del av informasjonssikkerhetsarbeidet, også når det kommer til retningslinjer og rutiner. For at ansatte skal kunne etterleve lover, regler og lokale bestemmelser må ansatte bli gjort kjent med disse. I spørreundersøkelsen ba vi respondentene ta stilling til hvorvidt de var kjent med kommunens rutiner for varsling av avvik og kommunens retningslinjer for informasjonssikkerhet:

[28] Kommunen har felles løsning for medarbeidersamtale på intranett, medarbeidersamtale skal gjøres årlig

Figur 7: Gjennomsnitt av kjennskap til retningslinjer og rutiner innen informasjonssikkerhet[29]



Kilde: Rogaland Revisjon

Av figuren ser vi at ledere er mer kjent med både varslingsrutinene og retningslinjene for informasjonssikkerhet, sammenlignet med medarbeiderne. De fleste medarbeiderne oppgir at de har god kjennskap til retningslinjene – det er likevel ca. 30% som i mindre grad er kjent med dem. Tilsvarende tall for lederne er ca. 15%, mens 12% av systemansvarlige oppgir det samme.

Videre rapporterer de fleste om god kjennskap til kommunens rutiner og retningslinjer. I intervjuene får vi derimot opplyst at de ansatte er kjent med at rutiner finnes, men at det er få som er kjent med hva de inneholder. Eksempelvis er flertallet av de intervjuede lite kjent med hva som regnes som et avvik innenfor informasjonssikkerhet og personvern, og hvor, når og hvordan dette skal rapporteres. (Mer om avvik i her)

Som tidligere nevnt er kommunens rutiner tilgjengelige på intranett. Samtidig får vi opplyst at mange ansatte ikke bruker PC til sine ordinære arbeidsoppgaver, og at ikke alle ansatte jevnlig sjekker epost eller har tid til å se gjennom det som blir tilsendt fra administrasjonen, særlig dersom dette ikke blir ansett som viktig eller relevant informasjon. Ansatte i skolen bruker dessuten en annen epostadresse enn administrasjonen, som betyr at felles eposter ikke alltid blir direkte sendt til epostadressen ansatte bruker i det daglige. Noen av de intervjuede opplyser at de har lagt inn direkte videresending til sin mest brukte epostadresse.

Det fremheves i intervju at nyansatte naturlig nok ikke har samme praksis eller kunnskap som ansatte med lenger erfaring/ansiennitet. Vi blir også gjort oppmerksom på at relevant informasjon

[29] Skala fra 1 i liten grad til 6 i stor grad, besvart av ledere og medarbeidere

om for eksempel hva som kan utleveres av elevinformasjon, ikke er tatt inn som del av opplæringen til alle ansatte i skolen. Det vises også til at ledere har uttrykt at erfaring er den beste måten man lærer å håndtere situasjoner rundt informasjonssikkerhet og personvern på, - gjennom forankret lærdom.

2.5 VURDERING

Lovverket har strenge krav knyttet til behandling av personopplysninger, og stiller høyre krav til etterlevelse av kommunens ansatte. Rutiner og retningslinjer forhindrer i stor grad brudd på krav, men dette forutsetter at disse er kjent for ansatte.

Kommunen har flere aktiviteter for kontinuerlig og systematisk forbedring av informasjonssikkerhetsarbeid. Informasjon og opplæringsmateriell knyttet til dette er også gjort kjent i ulike kanaler som intranett, rollefunksjoner, grupper/råd, opplæringsplaner og nettbaserte kurs. Dette vises også igjen i de styrende dokumentene som oppdateres, revideres og/eller godkjennes jevnlig.

Det vurderes at informasjonsflyten i sentraladministrasjonen er systematisert på en måte som sikrer at informasjon er tilgjengelig for kommunedirektørens ledergruppe. Funn kan derimot tyde på at informasjon fra dette nivå til virksomhetsnivå og ned i virksomhetene er mer utfordrende. Da intervju avdekker manglende kjennskap til retningslinjer og rutiner om informasjonssikkerhet hos ansatte, er det nærliggende å tro at informasjon/rapporteringer fra virksomhetsnivå til kommunalsjefnivå kan være mangelfull. Dette kan i verste fall føre til manglende opplæringstiltak eller at eventuelle tiltak som iverksettes ikke treffer.

Undersøkelsen viser at kjennskap til retningslinjer og rutiner for informasjonssikkerhet varierer på de ulike nivåene i kommunen. Slik vi ser det har kommunens sentraladministrasjon god kjennskap til det overordnede styringssystemet for informasjonssikkerhet, men kjennskapen ned i organisasjonen reduseres, naturlig nok, i takt med nivået den ansatte befinner seg på. At flere ansatte stiller spørsmål til link med spørreundersøkelse som ble sendt ut i dette prosjektet, vitner om en bevissthet i organisasjonen knyttet til elektronisk behandling av informasjon. Utover dette er det viktige at ansatte også er kjent med bestemmelser og rutiner som inngår i deres utøvelse av faktisk arbeid, og at de er kjent med konsekvensene av å ikke følge disse. Skolene er driftsenheter, og det er derfor forståelig at de ikke finner informasjonssikkerhet like relevant i sin hverdag. Denne undersøkelsen tyder derimot på at flere ansatte har mindre kjennskap til retningslinjer og rutiner for informasjonssikkerhet og ikke vet hvor de finner disse.

Intranett og opplæringsplanene gir de ansatte god tilgang til informasjon om informasjonssikkerhet, og den nasjonale sikkerhetsmåned (nanokurs) oppfattes som en viktig påminner og opplæringsbidrag. Ansatte har på denne måten tilgang til informasjon og opplæring i informasjonssikkerhet. Dette krever derimot tilgang til PC i arbeidshverdagen. Både svarprosent på revisjonens spørreundersøkelse og andel ansatte som har gjennomført nanolæring, kan tyde på at nettopp manglende elektronisk tilgang hindrer at nødvendig informasjon når ut til alle ansatte.

Tall fra kommunen viser også at ansatte i liten grad gjennomfører obligatoriske kurs om informasjonssikkerhet i tildelt opplæringsplan. Opplæringsplanene blir i intervju av skoleansatte vist til som omfattende og at det krever tilrettelagt tid for å kunne gjennomføre dem. Intervjuene tyder på variasjon knyttet til om og hvordan det blir lagt til rette for gjennomføringen, samt at ledere ikke er godt nok kjent med hvordan dra nytte av tilgjengelige oversiktsverktøy og dermed ikke har oversikt over hvem som har fullført og ikke. Opplæringsplanene inneholder viktig informasjon for ivaretakelse av krav til informasjonssikkerhet og personvern. Kommunen bør derfor sikre at den enkelte ansatte får anledning til å gjennomføre tildelt opplæringen, samt at leder holder seg oppdatert og følger opp i de tilfeller opplæringen ikke blir gjennomført. Utilstrekkelig opplæring gir økt risiko for brukerfeil og svekke etterlevelse, som kan gi konsekvenser for informasjonssikkerheten.

2.6 ANBEFALING

Revisjonen anbefaler:

- Kommunen bør øke gjennomføringsgraden av opplæringsplanen
- Kommunen bør vurdere tiltak som kan sikre at ledere nyttiggjør seg funksjoner som gir oversikt på gjennomførte/ikke gjennomførte planer, slik at dette kan følges opp.

3 ETTERLEVELSE

I hvilken grad etterlever kommunen kravene til informasjonssikkerhet?

3.1 REVISJONSKRITERIER

Offentlig sektor har etter arkivloven krav om arkivering av alle innsamlede dokumenter. Arkivering gjelder også dersom behovet for dokumentasjon er midlertidig eller dersom dokumentet har midlertidig virkning. Som del av arkivplan inngår systemoversikt over elektroniske systemer hvor det ligger viktig dokumentasjon for enkeltindivider og organet selv[30].

Arkivloven stiller krav til *Systemoversikt*, som innebærer en oversikt over alle program og applikasjoner mm. som kommunen bruker. Videre krever Personopplysningslovens kapittel 1 artikkel 30 at all behandlingsaktivitet[31] av personopplysninger skal protokollføres. Det betyr at

[30] Veileder for systemoversikt med beskrivelser - Arkivverket

[31] En oversikt over hvilke personopplysninger som behandles, hvilket formål dette har og hvilke hjemler kommunen har for å gjøre behandlingen. I tillegg inngår dokumentasjon som DPIA og øvrig risikovurderinger. Eksempel på

alle virksomheter som behandler personopplysninger, skal føre protokoll over gjennomførte behandlingsaktiviteter knyttet til personopplysninger.

Kommunen skal etter personvernforordningen artikkel 24 gjøre organisatoriske tiltak for å ivareta krav om informasjonssikkerhet og personvern. Tiltakene skal gjennomgås jevnlig og oppdateres ved behov. I kommunens rutiner for informasjonssikkerhet, finner vi sjekklisten «*Når jeg skal behandle personopplysninger må jeg huske på*». Denne henviser til protokoll for behandlingsaktivitet, hvor det er forklart hvilke krav og forhold som må oppfylles for at man kan behandle personopplysninger, og hva som følger med behandlingen. Sjekklisten sier blant annet at «*Hver gang vi behandler personopplysninger for et nytt formål skal dette ha egen føring i protokollen. Alle feltene skal fylles ut, og føringen skal undertegnes og dateres*». Dette innebærer at alle ansatte kan være behandlere av personopplysninger, noe som krever kjennskap til sjekklisten og protokollen, samt risikovurdering som DPIA.

Kommunens overordnede styringssystem legger krav til lagring og oppbevaring av *taushetsbelagte personopplysninger* i *relevant fagsystem*. Dette er også inntatt i *rutine for bruk av epost*. Det er også vist til at «*taushetsbelagte personopplysninger skal ikke ligge åpent tilgjengelig for uvedkommende*», følgende skal overflødig papirer makuleres.

Sikkerhetsreglene og arkivloven stiller krav til at det at dokumentasjon skal være tilstrekkelig, noe som gjør at ansatte i kommunen også må lagre elektronisk korrespondanse. *Rutine for bruk av epost* er en del av sikkerhetsreglementet og ligger tilgjengelig på intranett. Her står at epost i hovedsak skal brukes til korrespondanse med eksterne, mens Teams skal være kanal for intern kommunikasjon. Ved mottakelse av sensitiv informasjon skal dette lagres i riktig fagsystem eller arkiveres i Public 360. Videre skal epost med sensitiv informasjon *slettes* etter arkivering, noe som også innebærer å *slette papirkurven*. Sikkerhetsreglementet viser også til forsiktighet ved bruk av SMS.

Mens sikkerhetsreglement og retningslinjer er kommunens overordnet styrende systemet for informasjonssikkerhet i kommunen, gir rutiner og rollebeskrivelse mer konkret krav til praksis i enkelte situasjoner. I rollebeskrivelser er *Alle som bruker IKT som et verktøy for å utføre nødvendige arbeidsoppgaver for kommunenes innbyggere*, definert som **bruker**. [32] I dette legges ansvaret for å etterleve lover, regler og lokale bestemmelser til den enkelte ansatte.

behandlingsaktivitet kan være alt fra lagring av navn eller annen personinformasjon, karakterutskrift, chat-tjenester mellom elever, lærere eller ansatte o.a..

[32] Hentet fra kommunens dokumentasjon om rollebeskrivelser «Bruker».

Ut fra dette har vi utledet følgende revisjonskriterier:

- Ansatte er gjort kjent med sikkerhetsinstruksen
- Taushetsbelagt informasjon skal ikke lagres i skyen/skybaserte tjenester
- Behandling av epost eller sms som inneholder sensitiv informasjon behandles ihht rutiner
- Det blir ført protokoll for all behandling av personopplysninger

3.2 SYSTEMATISKE AKTIVITETER

Det vil til enhver tid eksistere risikoer utenfra som man ikke kan styre, men organisasjonen kan i større grad sikres ved å ha gode rutiner som minsker sjansene for menneskelig svik og feil. Informasjonssikkerhet inngår i kommunens internkontroll. I kommunens retningslinje for informasjonssikkerhet presiseres det at ansatte og ledere skal etterleve krav, retningslinjer, prosedyrer og rutiner som gjelder, og at det jevnlig skal oppdateres og motiveres med ny kunnskap om informasjonssikkerhet. Dette for å lykkes i arbeidet med å sikre informasjon.

Figuren under viser hvordan kommunen systematisk og kontinuerlig skal arbeide med informasjonssikkerhet:

Figur 8: Systematiske aktiviteter i informasjonssikkerhetsarbeidet

Kilde: Stavanger kommune

3.3 SYSTEMOVERSIKT OG PROTOKOLLFØRING

Kommunen har en systemoversikt og en protokoll for behandlingsaktivitet[33] av personopplysninger.

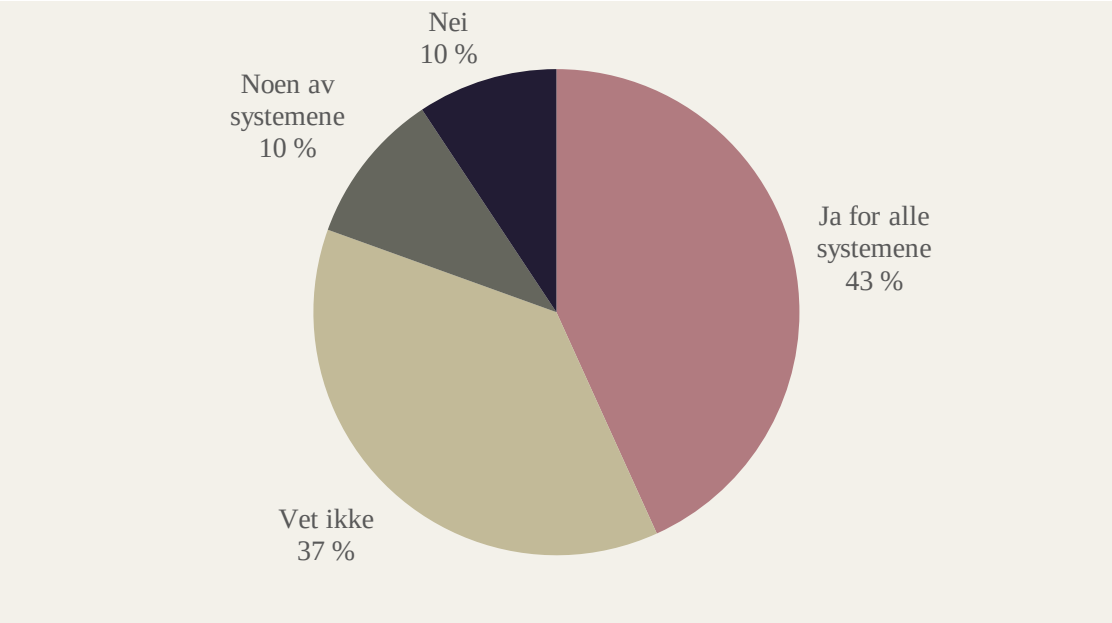
Systemoversikten gir blant annet innsikt i alle system, fagprogram, apper, mm (heretter samlebetegnelsen system) og tilhørende analyser som er i bruk i kommunen. Innføring av nye system krever dokumenterte vurderinger av bruk før det tas i bruk.

Protokollen inneholder en oversikt over krav som stilles, hjemmel til kravet, beskrivelse av kravet og utfylling av dette for alle aktivitetene/systemene. Det er nøkkelpersonell[34] som har ansvar for at behandlingsprotokollen er oppdatert. Det uttales fra flere av de intervjuede at de ikke vet hvem som har ansvaret for føringen, andre viser til at det er nøkkelpersoner i oppfølging av informasjonssikkerhet og personvern som har det endelige ansvaret. I Oppvekst og utdanning er det i hovedsak systemansvarlig som har ansvar for å protokollføre behandlingsaktivitet.

Ifølge kommunens rutiner har blant annet systemansvarlig ansvar for å holde protokollen oppdatert. Å være systemansvarlig er en tilleggsfunksjon til opprinnelige stilling. I spørreundersøkelsen oppgir 153 respondenter[35] at de er systemansvarlig for ett eller flere fagsystemer i kommune, hvorav 77% er systemansvarlige for program som behandler personopplysninger. Disse ble videre spurt om behandling av personopplysninger er registrert i protokoll for behandlingsaktiviteter:

[33] Behandlingsaktivitet er alt fra lagring av navn eller annen personinformasjon, til karakteroversikt for enkeltelever i skolen og chat tjenester mellom elever, lærere eller ansatte i kommunen.
[34] Nøkkelpersonell i denne forbindelse: systemansvarlige/-eier, rådgivere for informasjonssikkerhet og personvern eller andre som har informasjonssikkerhet som del av sitt arbeid.
[35] 56 (36,6%) respondenter er ledere med personalansvar og 97 respondenter (63,4%) er medarbeidere

Figur 9: Systemansvarliges føring i protokoll for behandlingsaktivitet av personopplysninger

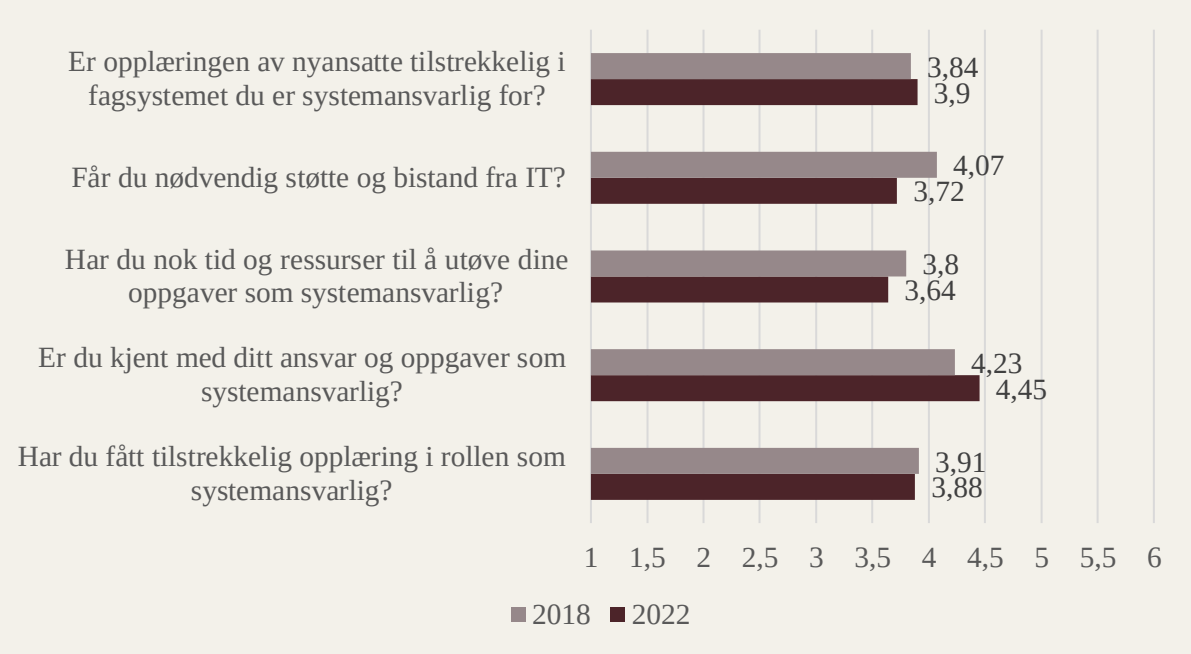


Kilde: Rogaland Revisjon

Under halvparten av respondentene svarer at behandling av personopplysninger er protokollført i alle system, 37% oppgir at de ikke vet, samtidig som det oppgis at deres system behandler personopplysninger.

I spørreundersøkelsen ba vi systemansvarlige om å ta stilling til en rekke spørsmål knyttet til deres rolle:

Figur 10: Spørsmål til systemansvarlige, sammenligning gjennomsnittsvar 2018 og 2022 (skala 1-6)



Kilde: Rogaland Revisjon

Som vist i figuren over, svarer systemansvarlige at de ligger litt over middels i alle spørsmål med unntak av *«Er du kjent med ditt ansvar og oppgaver som systemansvarlig?»*. Her er scoren godt over middels og høyere enn i 2018.

I intervju får vi opplyst at aktiviteter som normalt sett blir gjennomført av ansatte, eksempelvis uthenting av bursdagslister eller annen informasjon som i utgangspunktet ikke er arkivverdig, er utfordrende å få protokollført. Dette da ansatte ikke er kjent med kravet om protokollføringen.

Etter forrige forvaltningsrevisjon, *Informasjonssikkerhet, drift og sårbarhet (2019)*, innførte kommune et nytt system for protokollføring av behandlingsaktiviteten. Dokumentet, som er et låst og tilgangsstyrt Excel-ark, er tilgjengelig på Intranett. Vår gjennomgang av behandlingsprotokoll, viser at denne er ufullstendig og ikke oppdatert, hvor flere av registreringene mangler detaljinformasjon, mangler godkjenning, signering eller andre oppføringer. Dette bekreftes i intervju, hvor det også opplyses om at dette er noe de jobber med. Det vises til at kommunen har flere hundre system, noe som gjør protokollføringen utfordrende. Systemoversikt og protokoll er også to separate dokument, og krever i tilfeller også dobbelføringer. I tillegg er det mange ansatte som er involvert i protokollføringen. I intervju blir vi fortalt at systemet er lite oversiktlig og oppleves som en dårlig løsning. Det jobbes derfor med en løsning som gjør at systemoversikt og protokoll kan snakker sammen slik at blant annet dobbelføringer kan unngås. Vi får opplyst at en slik løsning vil være en forbedring som vil gjøre det enklere imøtegå krav.

Det blir opplyst at det i Oppvekst og utdanning er jobbet systematisk med informasjonssikkerhet og personvern de siste tre årene, hvor blant annet tre områder har hatt særlig fokus:

1) Styrke kompetanse og bevissthet hos systemansvarlige i direktørområdet.

2) Stavangerskolen: Økt styrking og kontroll på personvern i digitale læremidler og mulighet til å ta i bruk digitale løsninger. September 2022 ble det blant annet innført midlertidig stopp i godkjenning og aktiviteter av nye digitale løsninger, og fjernet tilgangen til et stort antall digitale løsninger. Dette for å redusere størrelsen på systemporteføljen som brukes av skolene. Systemporteføljen består både av *Stavangerpakken*[36] og åpne nettsider[37] som kan komplementere undervisningen. Det er videre lagt inn innholds filter som skal blokkere upassende sider/tjenester. I dag skal digitale læremidler i kommunen risikovurderes og godkjennes sentralt før de tas i bruk ute på skolene.

3) Gjennomføre ROS-analyser og DPIA for systemene som direktørområdet er mest avhengig av for å levere viktige tjenester til innbyggerne.

Flertallet av de intervjuede mener at de ikke har bruk for andre systemer enn de som ligger i Stavangerpakken, mens andre opplyser at de også benytter gratis applikasjoner eller nettsider. Enkelte ansatte oppgir at de ikke tar i bruk nye system før de har vært i kontakt med IT-avdelingen, eller IKT-veileder på skolen. Det vises også til en praksis hvor ansatte kontakter nærmeste leder, IKT-veileder eller rektor ved mistanke om avvik eller andre spørsmål innen tematikken. En lærer uttaler at ledelsen ved skolen er positive til bruk av digitale tjenester, og at lærerne er oppmuntret til å også benytte nettsider som ikke er inkludert i Stavangerpakken.

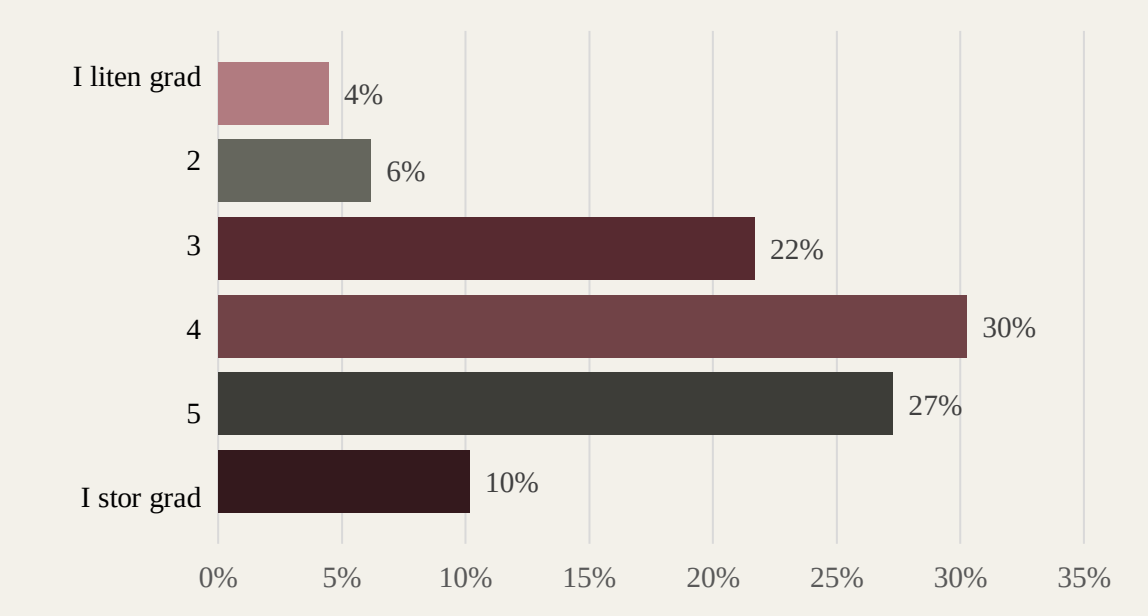
3.4 PRAKSIS OPP MOT RUTINER

Kommunen har taushetserklæring og sikkerhetsinstruks som vedlegg ved signering av arbeidskontrakt. Tall fra leders sjekkliste 1. tertial 2022 viser at alle medarbeidere ved tiltredelse i stilling på dette tidspunkt har signert disse dokumentene og antas dermed kjent med rutinene.

I spørreundersøkelsen ble respondentene bedt om å ta stilling til hvorvidt rutiner følges i det daglige.

[36] *Stavangerpakken* er Stavangerskolens godkjente læreverk, som er et sett tjenester kommunen har kjøpt tilgang til. Dette er større systemer som blir prioritert protokollført og dermed risikovurdert.
[37] Åpne nettsider; ordbøker, leksikon, nettaviser oa. som ikke krever pålogging.

Figur 11: I hvilken grad oppfattes det at rutiner for informasjonssikkerhet følges i det daglige?



Kilde: Rogaland Revisjon

Dersom vi deler skalaen i to, ser vi at flertallet mener at rutinene følges, mens ca. én av tre oppgir at rutiner følges i mindre grad. Også på disse spørsmålene gir lederne en bedre score enn medarbeidere. Intervjuene gir et tilsvarende bilde.

De intervjuede fra skolene uttrykker at det i stor grad er praksis som gir rutiner, og at de er lite kjent med det overordnede styringssystemet for informasjonssikkerhet. Flere ansatte sier at de er usikre på hvilken rutine de følger, men forteller at det er en praksis å følge «vær varsom-plakaten». Noen forteller at de gjør mye for å sikre informasjon, men at de er usikre på om det de gjør er nok. Ved en av skolene blir vi fortalt at praksis i noen tilfeller bygger på usikkerhet og forsiktighet, noe som medfører mindre dokumentasjon og tilgjengelighet. Det blir vist til at taushetsplikten er noe de ansatte i skolene setter høyt og at de grunnet det går forsiktig frem.

Vi blir i intervju fortalt at det i tilfeller ved manglende tilgang i fagsystem, samt i bruk av aktivitetsplaner[38] blir praktisert utskrift av dokumenter for å gjøre de tilgjengelig for ansatte. Ved to av skolene, får vi opplyst at dokumenter som inneholder sensitive opplysninger eller annen taushetsbelagt informasjon, ikke alltid blir skjermet/låst inn. Vi får også opplyst at loggføring knyttet til kartlegging av elever blir notert anonymisert for hånd, og ikke dokumenter i fagsystemet. Slike notater blir vist til som private og blir i hovedsak oppbevart i den ansattes låste skap eller ved deres arbeidsplass. Sikker sone kontroll avdekket at seks av de 12 skolene hadde sensitiv dokumentasjon utenfor sikret sone, arkivert på Google disk (skytjeneste). Ved én skole

[38] Skolen har etter opplæringsloven §9A-4 en aktivitetsplikt ved mistanke eller kjennskap til at en elev ikke har det trygt og godt på skolen. En aktivitetsplan skal blant annet synliggjøre tiltak som skal sikre eleven et trygt skolemiljø (kilde: www.Udir.no)

ble det funnet sensitiv dokumentasjon på minnepenn som var tilgjengelig for alle ansatte på skolen. Her ble det også påpekt at låsing av skjerm eller - kontordør ikke er like godt innarbeidet av alle, samt at flere ansatte sjelden benytter seg av fagprogram/-systemet.

I intervju blir det vist til at ansatte anonymiserer elever i møtereferat og overholder taushetsplikt ved å ikke skrive/nevne elevers navn i samtale med kollegaer og elevens foresatte, samt at sensitive opplysninger ikke sendes på epost, men heller formidles per telefon. Intervjuede forteller også at de bruker sikker print, og at dokumenter da legges i konvolutt like etter utskrift.

Epost og SMS korrespondanse oppgis som skolenes mest vanlige former for skriftlig korrespondanse. I intervju blir det vist til at noen bruker epost mye og har dette som hovedform for skriftlig kommunikasjon, både internt og til aktuelle eksterne aktører (foresatte). Vi blir fortalt at ansattes bevissthet knyttet til å slette mottatte eposter som inneholder fullt navn og informasjon om elev, for så å besvare henvendelse ved opprettelse av ny epost, varierer. Andre igjen følger hverken rutine eller praksis for sletting av epost eller annen korrespondanse med foresatte (inkludert SMS). Det blir også nevnt usikkerhet knyttet til hvorvidt epostkorrespondanser blir slettet i e-postkasse etter lagring i fagsystem. Også ansattes bevissthet knyttet behandling av sms blir oppgitt som varierende. Informasjon fra intervju viser ulike praksis knyttet til sletting av dokumenter og eposter, hvor noen sletter mens andre ikke har et like bevisst forhold til dette.

Sikker sone kontroll avdekket avvik ved mottak av sensitiv informasjon på epost ved tre av de 12 besøkte skolene. Epost ble besvart uten at historikk ble slette og arkivverdig innhold ble ikke arkivert. Generaliteten ved bruk av epost- og SMS korrespondanse blir oppgitt som begrunnelse for at rutiner eller overholdelse av arkiveringsplikt ikke blir fulgt. Det blir også pekt på at krav om arkivering av epost/SMS kun er gjeldende i tilfeller hvor det innhentes dokumentasjon, noe som opplyses å normalt skjer via skolenes fagsystem.

Fagsystemet Public Oppvekst (PO) og Public 360 blir omtalt som tungvint og tidkrevende å bruke, og blir oppgitt å være i konflikt med krav til dokumentasjon. Vi får blant annet opplyst at det er vanskelig for lærerne å loggføre og dokumentere informasjon om elever som ikke er faglig relatert, da Sikker sone, Public Oppvekst (PO)[39] og Public 360[40], er fag- og arkivsystemer hvor det må opprettes sak for å lagre dokumenter. Det fortelles at arkivering av saker er uoversiktlig og ulogisk, og det oppleves utfordrende å knytte mottakere og dokumenter til saken. Det kommer heller ingen melding eller varsel fra PO når en sak eller fil er opprettet i systemet. Den ansatte må logge seg inn i programmet med to-faktor autorisering for å sjekke om de har mottatt informasjon om sine elever. Ansatte opplever at systemet er både tidkrevende og lite brukervennlig, noe de mener bidrar til et skyggearkiv. Kommunen er kjent med dette, men vet ikke helt hvordan løse det. Det blir også vist til at det vet ett tilfellet gikk flere måneder før ansatt fikk nødvendig tilgang til fagprogrammet. Intervjuene avdekker også variasjoner i hvordan fagsystemet i skolen brukes, der noen utnytter flere funksjoner i systemene, mens andre ikke vet at disse eksisterer. Dette

[39] Public Oppvekst (PO) brukes spesifikt av skolene til lagring av elevmapper.
[40] Ansatte har ikke tilgang i dette systemet

eksempelvis ved opprettelse av individuelle opplæringsplaner (IOP), hvor noen skoler oppretter planen direkte i sikker sone/PO, andre ferdigstiller dokumentet på PC før opplastning. Ved noen skoler tar ledelsen seg av arkiveringen, mens dette ved andre skole er noe som også kontaktlærerne har tilgang til.

Ved to skoler blir vi vist at taushetsbelagte dokumenter, som IOP og aktivitetsplaner, var lagret på Google-disk (skytjeneste). I intervju fortelles det at det praktiseres en mellomlagring i utarbeidelsesprosessen, før planene blir lastet opp som endelige i PO. Videre får vi påpekt at ansatte er bevisste på å anonymisere dokumentene i størst mulig grad, ved for eksempel bruk av initialer, før det blir lagt i skyen, eller skrevet ut på papir. Sikker sone kontroll avdekket at seks av de 12 skolene hadde sensitiv dokumentasjon utenfor sikret sone, arkivert på Google disk (skytjeneste). Ved én skole ble det funnet sensitiv dokumentasjon på minnepenn som var tilgjengelig for alle ansatte på skolen.

Kommunen har også «*superbrukere*», som er ansatte som har fått en ekstra innføring i fagsystem som benyttes i sin virksomhet. For skolene er dette mest nevnt i sammenheng med arkivsystemet Public Oppvekst og det nye fagsystemet Vigilo[41]. Ansatte vi har intervjuet oppgir at et slikt tiltak er positivt og fungerer i stor grad bra. Men det er fortelles også at superbrukerne selv ikke opplever å ha bedre kompetanse enn øvrige ansatte eller ledere.

3.5 VURDERING

Kommunen har et gjennomgående styringssystem for informasjonssikkerhet, og vurderes i stor grad å legge til rette for at informasjonssikkerheten kan ivaretas. Gjennomgangen viser også at praksis knyttet til utsendelse av sikkerhetsinstruksen ved ansettelse sikrer ansattes signering av sikkerhetsinstruksen. Undersøkelsen avdekker allikevel at ansattes manglende kjennskap til retningslinjer og rutiner svekker kommunens ivaretakelse av krav knyttet til informasjonssikkerhet.

Arbeidet knyttet til protokollføring er omfattende og krever forløpende oppfølging, samt god kjennskap til rutiner og krav. Spørreundersøkelsen avdekker at flere systemansvarlige ikke vet om behandling av personvernopplysninger er protokollført. Videre oppfattes det i intervju med skoleansatte en usikkerhet knyttet til hvem som har ansvar for å protokollføre behandlingsaktivitet av personopplysninger. Dette mener vi utgjør en sårbarhet knyttet til ivaretakelse av krav om behandlingsoversikt.

[41] Vigilo er et komplett oppvekst- og administrasjonssystem (OAS), som skal dekke behovene oppvekstsektoren har for å kunne administrere barnehager, skoler og SFO (Hva er Vigilo). Fagprogrammet ble innført i Stavanger kommune i januar 2023.

At det nå arbeides med å få på plass en protokoll og oversikt som er lettere å følge opp er bra, men også det vil kreve at ansatte som skal være involvert i systemregistrering og protokollføringen er kjent med sitt ansvar. Her tyder funn på at flere systemansavelige ikke er kjent med oppgaver som ligger til rollen. Vi mener derfor at det er viktig å sikre at systemansvarlige er kjent med ansvaret knyttet protokollføring og systemregistrering, og at dette blir kommunisert til ansatte i virksomhetene.

Det er positivt at ansatte i skolen er bevisste på anonymisering i de tilfeller behandling av dokumenter skjer utenfor system/fagprogram. Vi finner likevel en risiko i dette, da praksisen kan gi et skyggesystem som det er utfordrende å få oversikt på. Mellomlagring i skyen er avvik på sikkerhetsreglementet, og bør derfor lukkes. Krav om interkontroll i den enkelt virksomhet/skole er noe som bør vurderes. En slik internkontroll kan bidra til økt bevissthet og bedre kjennskap til rutiner og krav om personvern og informasjonssikkerhet, som i neste omgang kan resultere i økt etterlevelse.

Spørreundersøkelsen viser variasjon i hvordan ansatte forholder seg til kommunens sikkerhetsmål, retningslinjer og prosedyrer. Dette understøttes langt på vei i intervjuene, hvor lærerne fremstår usikre og dermed forsiktige i sin behandling av sensitiv informasjon. Slik vi erfarer bygger derimot denne forsiktigheten/praksisen mer på oppfattelsen av taushetsplikt og «vær varsom»-plakaten, enn kjennskap til rutiner og retningslinjer/styrende dokumenter gjeldende behandling av personopplysninger.

Det er tydelig at etterlevelse av rutiner og retningslinjer i skolen utfordres når henvendelser til lærere kommer per epost og sms. Vi oppfatter at ansatte er klar over hvordan arkivere og besvare slike henvendelser, og at besvarelsene langt på vei følger rutiner. Vi finner det derimot utfordrende å etterprøve all den tid dette er henvendelser som kommer direkte til enkeltansatte, og da gjerne også på per sms. Det kan derfor være hensiktsmessig med jevnlig gjennomgang av rutiner og praksis knyttet til dette.

3.6 ANBEFALING

Revisjonen anbefaler kommunen å:

- Sikre at systemansvarlige er kjent med hva rollen innebærer av ansvar knyttet til protokollføring av behandlingsaktivitet, slik at dette blir gjort ihht. krav.
- Vurdere om det skal stilles krav til virksomhetene/skolene om jevnlig gjennomgang av rutiner og praksis knyttet til behandling av henvendelser per epost og sms

4 AVVIK – LÆRING - FORBEDRING

I hvilken grad bruker kommunen avvikssystemet til læring og forbedring?

4.1 REVISJONSKRITERIER

Avvik er hendelser som bryter med regelverk eller interne bestemmelser. Det kan være hendelser som har skjedd, mer permanente situasjoner, men også nesten-hendelser. Det er ulike regelverk som avvik kan knyttes til, noe som også kan variere fra tjenesteområde til tjenesteområde. Avviksrapportering har liten verdi dersom den ikke representerer noe annet enn en strøm av avviksmeldinger, eller årlige oppsummeringsrapporter til kommunedirektøren eller kommunestyret. Merverdien i form av styrket internkontroll oppstår først når avvikstilfellene enkeltvis og i sum benyttes til læring og utvikling, altså til et systematisk kvalitets- og forbedringsarbeid.

Kommunen skal etter kommuneloven § 25-1 ha internkontroll for å sikre at lover og forskrifter følges.[42] Internkontrollen skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold. I § 25-1 c fastslås at kommunedirektør skal «*avdekke og følge opp avvik og risiko for avvik*». Dersom avviket gjelder personopplysninger, skal den behandlingsansvarlige etter personvernforordningen artikkel 33 blant annet *«dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det….»* Videre hetere det i artikkel 24 at *«Den behandlingsansvarlige skal sørge for tilstrekkelige tekniske og organisatoriske sikringstiltak, herunder egnede retningslinjer, for behandlingen. Tiltakene er avhengig av hvilken behandling som gjøres, samt omfang, formål og kontekst, og risikoen som behandlingen medfører for personvern».*

Bruk av avvikssystemet til læring og forbedring er beskrevet i

- Forskrift om ledelse- og kvalitetsforbedring i helse- og omsorgtjenesten:
  - *§ 6 Plikten til å planlegge, punkt g)* innebærer blant annet å ha oversikt over avvik, herunder uønskede hendelser, evalueringer, klager, brukererfaringer, statistikk, informasjon og annet som sier noe om virksomheten overholder helse- og omsorgslovgivningen.
  - *§ 7 Plikten til å gjennomføre, punkt c),* stiller krav om å utvikle og iverksette nødvendige prosedyrer, instrukser, rutiner eller andre tiltak for å avdekke, rette opp og forebygge overtredelse av helse- og omsorgslovgivningen.
  - *§ 8 Plikten til å evaluere, punkt e)* viser til gjennomgang av avvik, herunder uønskede hendelser, slik at lignende forhold kan forebygges. Dette skal så følges opp med tiltak.

[42] Lov om kommuner og fylkeskommuner (kommuneloven)

- *§ 9 Plikten til å korrigere, punkt* c*)*, omhandler forbedring av nødvendige prosedyrer, instrukser, rutiner eller andre tiltak for å avdekke, rette opp og forebygge overtredelse av helse- og omsorgslovgivningen.

- Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (Internkontrollforskriften)
  Formålet med forskriften er fremme forbedringsarbeidet innen arbeidsmiljø, sikkerhet og forebygging av uønskede hendelser. Som del av internkontrollen skal virksomheten ifølge § 5:
  - *«6. kartlegge farer og problemer og på denne bakgrunn vurdere risiko, samt utarbeide tilhørende planer og tiltak for å redusere risikoforholdene»*
  - *«7. iverksette rutiner for å avdekke, rette opp og forebygge overtredelser av krav fastsatt i eller i medhold av helse-, miljø- og sikkerhets- lovgivningen».*

KS anbefaler kommunene å etablere rutiner for å evaluere årsaker til å informasjonssikkerhetsavvik, for å forebygge nye avvik, eller motvirke negative følger.[43]

I brosjyren «*Informasjonssikkerhet i Stavanger*» 2021 påpekes at alle ansatte må «*kjenne til Stavanger kommunes retningslinjer for informasjonssikkerhet, herunder rutiner for varsling av informasjonssikkerhetshendelser i «Si ifra!»*».

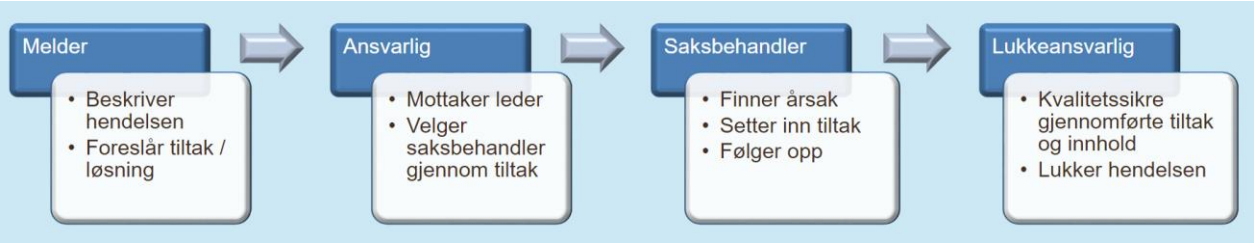
I kommunens veileder for informasjonssikkerhetsarbeid heter det blant annet at *«Informasjonssikkerhetsbrudd og rapporterte avvik skal følges opp regelmessig for å sikre erfaringsoverføring og læring»*. Kommunen har også en egne rutiner for behandling av avvik som sier at leder skal legger frem avviksrapporter i HMS-gruppen, videre at *«avvikshåndtering er en sentral prosedyre i virksomhetens systematiske HMS-arbeid og skal derfor gjennomgås årlig av virksomheten*». Herunder gjennomgang av antall avvik og fordelingen av disse, er avvikene fulgt opp og ført til eventuelle endringer på arbeidsplassen, samt vurdering av hvordan rapporteringsrutinene fungerer og om alle er kjent med prosedyrene.

Avvik skal rapporteres i kommunens kvalitetssystem TQM, gjennom modulen *Si ifra!*. Til dette kan både PC, mobil eller nettbrett benyttes. Rutiner for avviksrapportering skal gjennomgås av alle ansatte gjennom obligatorisk elektronisk kurs.

[43] Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet (ks.no)

Figuren under viser de ulike rollene og oppgavene i kommunens avvikshåndtering:

Figur 12: Roller i avvikshåndteringen



Kilde: Kurs 1 – Basiskurs Si ifra!

Leder blir automatisk informert om nye hendelser gjennom epost. Dersom hendelsen omhandler informasjonssikkerhet/personvern, mottar også personvernombudet epost.[44]

Ut fra dette er følgende revisjonskriterier utledet:

- Ansatte melder avvik
- Kommunen fører oversikt over avvik
- Kommunen har jevnlig gjennomgang av avvik og sikrer erfaringsoverføring og læring i etterkant

4.2 HVEM MELDER BRUDD PÅ INFORMASJONSSIKKERHET OG PERSONVERN – OG HVA BLIR MELDT?

I intervju får vi opplyst at avvik sjeldent meldes av lærerne selv – snarere er det skoleledelsen, rådgivere i stab og/eller personvernombudet som melder avvik på vegne av de ansatte, eller bistår i prosessen. Det vises til flere mulige årsaker til dette. Enkelte påpeker at det kan oppleves ubehagelig å melde inn avvik som andre er årsak til, de er redd for at det kan skape konflikt og ødelegge relasjonen til kollega, eller være en belastning for den ansatte som har utløst avviket. Andre årsaker som nevnes er at avviket ikke er av en slik karakter at det er behov for melding til Datatilsynet, eller at nærmeste leder allerede er orientert. Samtidig vises det til at ansatte har liten

[44] Kilde: Kurs 2 – Saksbehandling i *Si ifra!*, Stavanger kommune

kjennskap til hva som er brudd på informasjonssikkerhet og personvern. Flere av de intervjuede opplyser at informasjonssikkerhet er et tema som i liten grad omhandler deres hverdag. I tillegg viser funn fra spørreundersøkelsen at over halvparten av ansatte ønsker mer kunnskap om digital sikkerhet i sitt arbeid.

Flere av de intervjuede oppgir at informasjonssikkerhet ikke er et prioritert tema, og at avvikssystemet dermed ikke brukes som tiltenkt. Ansatte fra kommunens administrasjon forteller at avvik, som brudd på informasjonssikkerhet og personvern, ofte blir meldt inn etter at personvernombud eller stab i Oppvekst og utdanning er kontaktet og varslet. Tilsvarende blir også uttalt i intervju med Innovasjon og støttetjenester.

I kommunen er det de siste årene ført avvik ifm. brudd på informasjonssikkerhet og personvern innenfor alle tjenesteområder. Dette er illustrert i tabellen under:

Tabell 2: Rapporterte avvik ifm. brudd på informasjonssikkerhet og personvern 2020-2022

Område	2020	2021	2022	Totalsum
By- og samfunnsplanlegging	2	4	5	**11**
Bymiljø og utbygging	1	2	9	**12**
Helse og velferd	62	92	101	**255**
Innbygger og samfunnskontakt	5	6	6	**17**
Innovasjon og støttetjenester	24	13	15	**52**
Kommuneadvokaten	0	1	0	**1**
Oppvekst og utdanning	19	28	35	**82**
Økonomi og organisasjon	4	4	2	**10**
Totalt	**117**	**150**	**173**	**440**

Kilde: Stavanger kommune

Det er en betydelig økning i meldte avvik fra 2020 til 2022, særlig innen Oppvekst og utdanning og Helse og velferd. Vi får opplyst at økningen kan ses i sammenheng med innføringen av TQM *Si ifra!* i 2019 og økt søkelys på informasjonssikkerhet i kommunen siden 2021. Oppvekst og utdanning har i tillegg hatt en egen informasjonssikkerhet- og personvernrådgiver siden 2021. Vi blir videre gjort oppmerksom på at dette også er tjenesteområder med flest ansatte og med stort volum av tjenestemottakere.

Tabellen under gir en oversikt over årsakene til innrapporterte avvik de tre siste årene, for kommunen totalt sett:

Tabell 3: Årsak til rapportering av avvik knyttet til brudd på informasjonssikkerhet og personvern

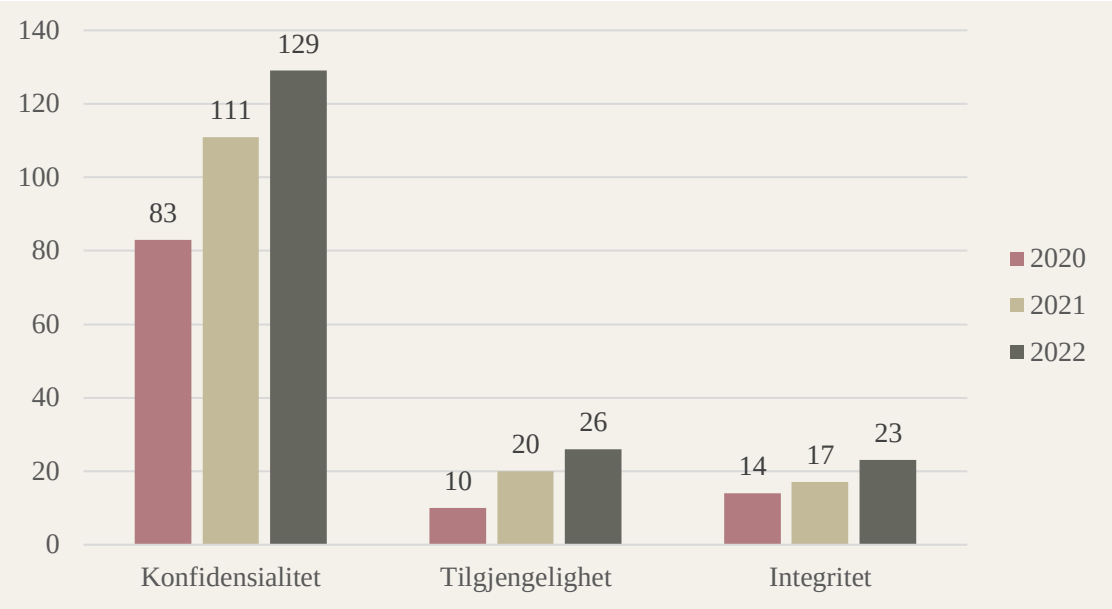
Årsak avvik	2020	2021	2022	Totalt
Brudd på lovverk / retningslinjer / rutiner	50	60	79	**189**
Brudd på taushetsplikt	36	42	53	**131**
Annet	16	16	20	**52**
Mangel på opplæring / kompetanse	14	11	18	**43**
Forsendelsesfeil	7	19	11	**37**
Uautorisert tilgang	10	6	17	**33**
Mistet / gjenglemt / forlagt	10	7	14	**31**
Midlertidig nedsatt sikkerhet	5	12	13	**30**
Svikt i datasystem	8	6	14	**28**
Utlån av brukernavn / passord	10	6	7	**23**
Manglende risikovurdering	7	6	8	**21**
Kaste / kvitte seg med opplysninger uten sletting / makulering	6	1	2	**9**
Nettpublisering av personopplysninger	4	3	2	**9**
Spredning i sosiale medier	1	2	4	**7**
Tilgangsstyring feilet / mangelfull / manglende	0	1	5	**6**
Feil gradering av informasjon	1	2	2	**5**
Hacking eller datainnbrudd	2	3	0	**5**
Nedetid	0	2	3	**5**
Skadelig programvare / virus	2	3	0	**5**
Mangel på DPIA	1	0	1	**2**
Fysisk innbrudd	0	0	1	**1**
Totalt	**190**	**208**	**274**	**672**

Kilde: Stavanger kommune

Tabellen viser at de fleste rapporterte avvikene knyttet brudd på informasjonssikkerhet og personvern, dreier seg om brudd på lovverk, retningslinjer, rutiner og taushetsplikt. Avvik som går igjen er sensitiv informasjon om pasienter eller brukere som er tilgjengelig for andre enn

ansatte, at dører ikke er lukket eller andre menneskelige feil. Noen avvik omhandler manglende lydisolering av kontor/lokaler, som medfører at uvedkommende kan lytte til taushetsbelagte samtaler. Brudd på rutiner, gjenglemte papirer eller sending til feil mottaker er avvik som kan svekke integritet og konfidensialitet. Som vi ser er av neste figur er de fleste avvik meldt som brudd på konfidensialitet.

Figur 13: Rapporterte avvik kategorisert etter konfidensialitet[45], tilgjengelighet[46] og integritet[47]



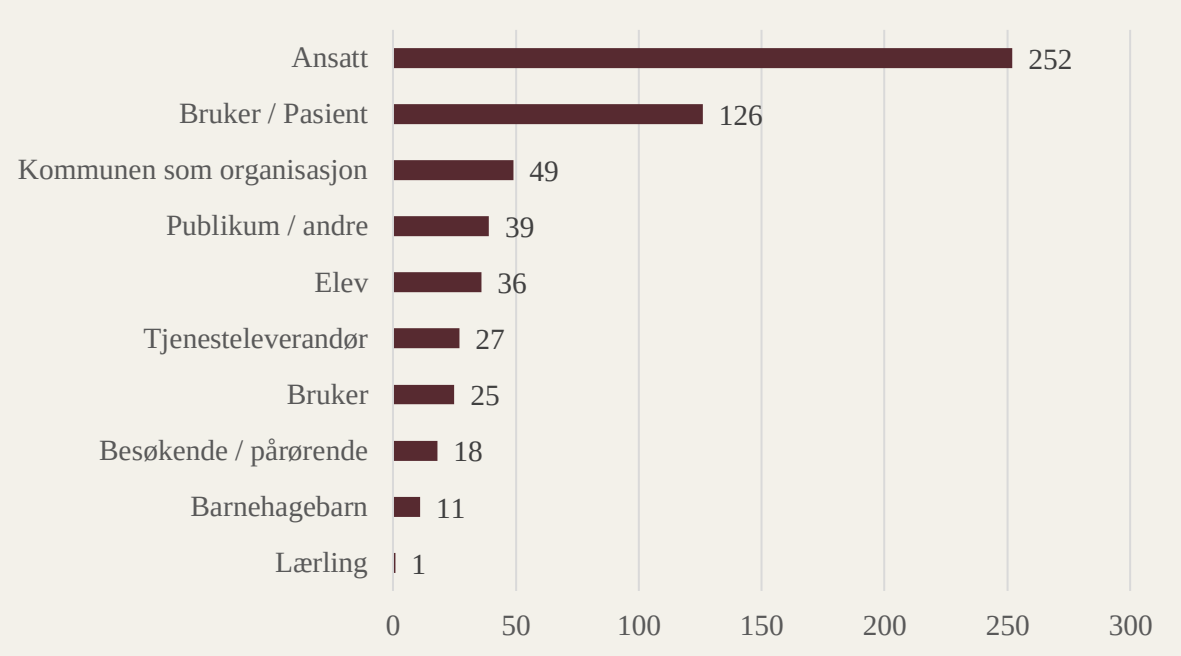
Kilde: Stavanger kommune

Her ser vi at brudd på konfidensialitet er hyppigste meldte avvik, samtidig som det registreres en økning i antall rapporterte brudd innenfor alle kategorier de tre siste årene.

[45] Brudd på konfidensialitet er en utilsiktet eller ulovlig utlevering av, eller tilgang til, personopplysninger.
[46] Brudd på tilgjengelighet er et utilsiktet eller ulovlig tap av tilgang til, eller sletting av, personopplysninger.
[47] Brudd på integritet er en utilsiktet eller ulovlig endring av personopplysninger.

Figuren under viser fordelingen av hvem som rammes av avvik, rapportert i perioden 2020 til 2022:

Figur 14: Oversikt over hvem hendelsen/avviket gjelder, sum 2020-2022

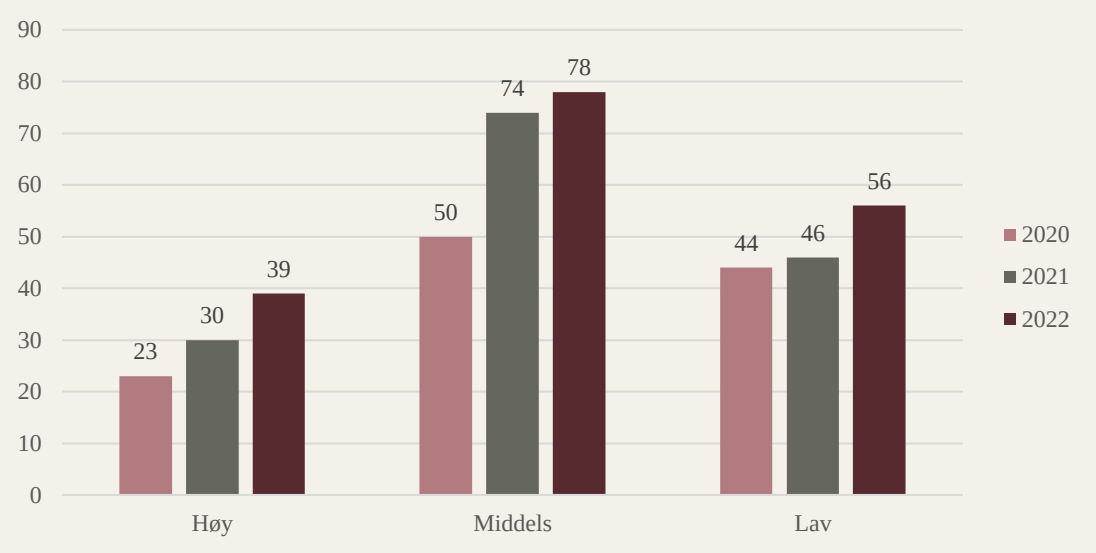


Kilde: Stavanger kommune

Figuren viser at hendelsene som rapporteres primært handler om ansatt og bruker/pasient. Vi finner at økning i rapportering i disse to kategoriene er større enn for de øvrige kategoriene.

Den som melder avvik skal kategorisere alvorlighetsgraden av avviket som høy, middels eller lav.[48] Figur under viser at økningen i innmeldingen i avvik har størst utslag i kategori høy og lav.

Figur 15: Alvorlighetsgrad for avvik rapportert i Si ifra!

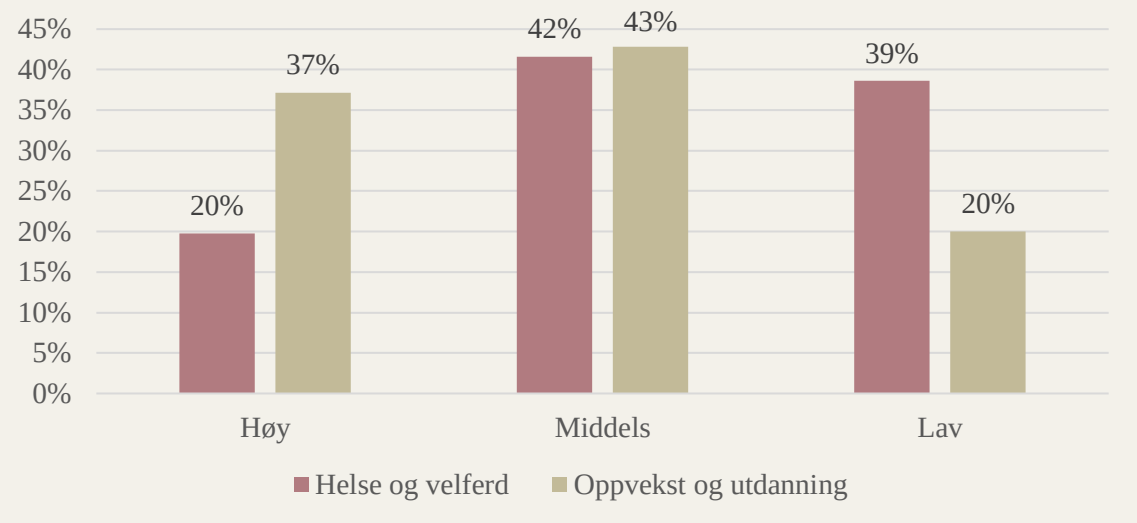


Kilde: Stavanger kommune

Totalt sett rapporteres flest avvik fra Helse og velferd, men av figuren under ser vi at det er Oppvekst og utdanning som har størst andel avvik med høy alvorlighetsgrad.

[48] Det foreligger ingen tydelige definisjoner på hva de ulike alvorlighetsgradene innebærer.

Figur 16: Sammenligning alvorlighetsgrad på rapporterte avvik



Kilde: Stavanger kommune

Under følger noen eksempler på innmeldte avvik og hvordan de er kategorisert.

Tabell 4 Eksempler på avvikskategorisering middels og høy

Alvorlighets-grad	Helse og velferd	Oppvekst og utdanning
Middels	- Pasientinformasjon funnet/mistet utenfor kontor - Feil dokumentasjon på pasienter	- Journal på avveie - Ulike hendelser tilknyttet papirer/dokumentet med sensitiv informasjon og/eller personopplysninger plassert uforsiktig/tilgjengelig for uvedkommende
Høy	- Feil henvisning av pasient - Utdelt brukernavn og/eller passord - Mistet arbeidsliste	- Elev filmer lærer i timen - Utdelt brukernavn og/eller passord - Sending av konfidensiell informasjon på epost

Vi blir fortalt at avvik med høy alvorlighetsgrad rapportert fra Helse og velferd, ofte er hendelser med brudd på konfidensialitet som kan få konsekvenser for flere. Fra Oppvekst og utdanning framgår avvikene mer variert, men også her er brudd på konfidensialitet, knyttet til lovverk, retningslinjer og/eller rutiner, det som blir meldt hyppigst.

I tillegg til alvorlighetsgrad, skal melder av avviket også vurdere konsekvensen av avviket. For begge tjenesteområdene er konsekvensen *personopplysninger på avve*ie oppgitt hyppigst. Det

registreres ellers en økende rapportering på konsekvens *redusert tillit og redusert sikkerhet for ansatt og bruker* i 2022.

4.3 HÅNDTERING AV AVVIK KNYTTET TIL BRUDD PÅ INFORMASJONSSIKKERHET OG PERSONVERN

Ledere, verneombud, saksbehandlere og andre nøkkelpersoner får opplæring i hvordan saksbehandle avvik meldt i *Si ifra!*,[49] samt opplæring i hvordan overholde lovkrav om personvern.[50] Etter rutiner skal et innmeldt/registrert avvik lukkes innen 30 dager. Det er ingen krav om at avvik skal resultere i tiltak, men den som rapporterer avviket skal vurdere behov for eventuelt strakstiltak .[51] Dersom avvik meldes med forbedringsforslag, skal saksbehandler av avviket ta forslag med i vurdering av tiltak/forebyggende tiltak før lukking av avviket. Tiltak kan innebærer opplæring, gjennomgang av rutiner e.a., eventuelt tiltak direkte mot enkelt ansatt.

Det opplyses at personvernombudet automatisk blir koblet inn i avvik som omhandler brudd på personvern. Dette innebærer at ombudet, med sin faglige kompetanse knyttet til personvern, bistår i saksbehandling og eventuelt varsling til Datatilsynet. Ved brudd på personopplysningssikkerheten skal personen som står overfor en *sannsynlig risiko* opplyses om bruddet.[52] Dette blir vi fortalt er en etablert praksis ved skolene som er involvert i denne undersøkelsen. Her vises til eksempler der det har oppstått risiko for at personopplysninger spres unødvendig på epost, og at det da er tatt kontakt med foresatte og informert om dette.

Ved avvik har behandlingsansvarlige (kommunen) ansvar for å sende melding til tilsynsmyndighet (Datatilsynet) dersom brudd kan medføre risiko for fysiske personers rettigheter og friheter.[53] I intervju blir vi fortalt at personvernombud alltid tar en vurdering på om avvik skal meldes Datatilsynet, men det vises til ulik praksis på hvem som melder avviket videre til Datatilsynet.

Kommunen, ved personvernombud, hadde fra januar til slutten av november 2022, meldt inn 11 avvik til Datatilsynet (se tabell under). Syv av disse var avvik i Helse og velferd, to i Oppvekst og utdanning, innovasjon og støttetjeneste hadde ett, og ett felles Oppvekst og utdanning/Innovasjon og støttetjeneste. I *Si ifra!* framgår at meldingsrutiner til Datatilsynet er fulgt i syv av de 11

[49] Kilde: Saksbehandling Si ifra!
[50] Dette innebærer blant annet at avvikene som meldes ikke skal inneholde navn eller annen sensitiv informasjon som kan identifisere personer.
[51] Ref. kommunens rutine for behandling av avvik, Retningslinje for rapportering av brudd på personvern eller informasjonssikkerhet avdekket av brukerstøtte og Retningslinje for rapportering av avvik.
[52] Lov om behandling av personopplysninger (personopplysningsloven) - Avsnitt 2 Personopplysningssikkerhet - Lovdata
[53] Personopplysningsloven kapittel IV, artikkel 33.

meldte avvikene. Sammenliknet med foregående år er det en nedgang i avvik meldt til Datatilsynet[54]. Se tabell under.

Tabell 5 Avvik meldt til datatilsynet, 2019-2022

Årstall	Antall avvik meldt til Datatilsynet
2019	16
2020	14
2021	16
2022	11

Kilde: Stavanger kommune

Personvernombudet mener at nedgangen handler om manglende kunnskap om melderutiner, og manglende kjennskap til det overordnede styringssystemet for informasjonssikkerhet.

Personvernombudet er som nevnt del av saksbehandlingen i avvik relatert til personvern. Vi får oppgitt at grunnen til dette er fordi ansatte ikke har samme kompetanse på feltet som personvernombudet. Vi blir fortalt at ombudet foretar en vurdering av avvikene som meldes i *Siifra!*, og deretter vurderer om det er nødvendig å melde avvikene til Datatilsynet eller ei.

4.4 LÆRING OG UTVIKLING

Av alle rapporterte avvik i 2022 ble 61% lukket innen frist (30 dager). Dette er en forbedring fra 2020 og 2021 som viser henholdsvis 48,7% og 45,9%. Av alle avvik som ble lukket i 2022, hadde 57 prosent registrert tiltak. Til sammenlikning hadde kun 43,2 prosent av avvik tiltak ved lukking året før (2021). Vi får opplyst at avvikssystemet ikke henter ut statistikk for strakstiltak[55], noe som kan bety at registrert prosentandel med tiltak kan være lavere enn realiteten.

Rutiner og retningslinjer legger opp til at avvik skal gjennomgås kontinuerlig. Vi blir fortalt at avvik i stor grad blir saksbehandlet og lukket, men at det på virksomhetsnivå ikke gjøres noe mer utover dette. Unntaksvis blir større hendelser/avvik gjennomgått i informasjonssikkerhetsrådet, som er del av sentraladministrasjonen. Vi blir opplyst om at gjennomgang og videre læring i avdelingene, avhenger av personene som har vært involvert i saksbehandling, samt tilgang på ressurser og tid. Det hevdes at læring av avvik krever tid til å følge opp, og i intervju ved skolene sier ansatte at de ikke har tilstrekkelig tid til å gjøre dette arbeidet. De forteller at de sjelden rapporterer avvik på informasjonssikkerhet/personvern, og at det er vanskelig å prioritere slike avvik fremfor avvik som vold og trusler, som i større grad påvirker deres arbeidshverdag. Det blir

[54] Tallene er mottatt fra Personvernombud i Stavanger kommune.
[55] Eksempel på strakstiltak kan være umiddelbar makulering av et dokument som er på avveie.

vist til godt læringsutbytte av å ha gruppene (informasjonssikkerhetsrådet og ressursgruppe personvern) for tjenesteområdet[56], noe som menes å bidra til kompetansedeling på tvers av organisasjonen. Det hevdes å mangle en overordnet analyse av avvik over tid.

Det blir opplyst at kommunen, ved meldt avvik til Datatilsynet, får veiledning fra tilsynet før avviket lukkes. Datatilsynet behandler årsak til avviket, analyserer konsekvenser og vurderer forslag til tiltak. Denne oppfølgingen mener kommunen fører til økt læring, da veiledningen gjerne går ut over enkeltsaker. Et eksempel som blir trukket frem i dette er tilfellet hvor kommunen blir anbefalt å «hashe» alle passord, - ikke lagre dem i klartekst[57]. Dette vil gi ekstra sikkerhet mot hacking og uautorisert tilgang.

Som en del av internkontroll har informasjonssikkerhetsrådet[58] innmeldte avvik i kategori informasjonssikkerhet og personvern som en del av sin faste rapportering. Rådet har møte fire ganger i året. Statistikken inngår også som en del av ledelsens gjennomgang, som gjennomføres årlig med kommunedirektørens ledergruppe. Vi får gjennom intervju oppgitt at gjennomgangene legger grunnlag for en årlig overordna analyse, som er styrende for opplæringsinnsats og rutineutbedring. Informasjonssikkerhetsrådet har i tillegg mulighet for å diskutere avvik innad i rådet, samt mulighet for å presentere løsninger på avvik, dersom det vurderes som relevant for gruppens medlemmer.

Vi får opplyst at avvik saksbehandles enkeltvis av nærmeste leder, noe som også fremgår av kommunens rutiner. Videre blir det av skoleansatte vist til at det ikke foreligger system for læring av avvik, men at det kan resultere i utbedring av rutiner. De vi har intervjuet er ikke kjent med hvordan avvik innen informasjonssikkerhet og personvern håndteres eller brukes til forbedring. Det viser derimot til erfaring med at innmeldte avvik har resultert i konkrete endringer i praksis.

Vi får opplyst at det i *Ressursgruppe personvern* blir diskutert mulige tiltak og løsninger dersom avvikshendelsen er kompleks, noe som de mener gir rom for læring på tvers av tjenesteområder. Også i gruppen for systemansvarlige innen Oppvekst og utdanning er det mulig å diskutere relevante avvik, og eventuelle løsninger.

4.5 VURDERING

Melding av avvik har som formål å føre til læring og forbedring. En lærende organisasjon stimulerer de ansatte til å melde fra om avvik og avvikene tas på alvor. Det innebærer dokumentasjon av tiltak som iverksettes, gjennomføring av evalueringer og nødvendige korrigeringer. På den måten kan avvik lukkes, samtidig som nye avvik kan forebygges gjennom

[56] Oppvekst og utdanning
[57] Passordet blir lagret i kryptert form. Når man hasher et passord er det ikke direkte leselig, slik som lagring i klartekst.
[58] Direktørene, IT-sjef, rådgiver informasjonssikkerhet fra IT og personvernombud.

utbedret internkontroll. Slik kan kommunen lære av sine feil. Ledelsens holdninger og kultur smitter over på medarbeiderne. Medarbeidere som erfarer at det å melde avvik bidrar til at organisasjonen lærer av episoder og feil, vil være mer tilbøyelige til å melde avvik enn om erfaringen er at avvik brukes til å henge ut enkeltpersoner eller -tjenester. Det samme gjelder rutiner for tilbakemeldinger til den som melder.

Kommunen har rutiner og retningslinjer, samt andre dokumenter som inneholder informasjon som danner grunnlag for å oppdage og melde avvik som ansatte blir gjort kjent med. Undersøkelsen gir indikasjoner på at det rapporteres færre avvik knyttet til informasjonssikkerhet og personvern enn det som faktisk forekommer. Vi vil derfor anbefale kommunen å vurdere om det kan være hensiktsmessig å iverksette tiltak/ytterlig opplæring for å øke bevisstheten rundt rapportering av slike avvik. En effekt av dette kan være redusert risikoen for avvik relatert til informasjonssikkerhet og personvern. I et slikt arbeid vil det være viktig å ta hensyn til de faktorene som kan hindre ansatte i å melde avvik, og tilby støtte og veiledning til de som trenger det.

Personvernombudet ser ut til å spille en viktig rolle i å vurdere avviksmeldinger som omhandler personvern. Kommunen sikrer på den måte å overholde personvernlovgivningen gjeldende innmeldte/registrerte avvik. Veiledning fra Datatilsynet ved meldte avvikt til tilsynet er positivt da også dette kan bidra til læring og forbedring av rutiner.

Informasjonssikkerhetsrådet og Ressursgruppe personvern oppfattes som positive arena for drøftinger av avvik og mulige løsninger på tvers av organisasjonen og viktig for kompetansedeling og læring. Det er derimot noe uklart hvordan deres anbefalinger og forslag blir tatt i bruk på virksomhetsnivå. Dette kan med fordel tydeliggjøres.

Økt fokus og dedikerte ansatte ser ut å ha bidratt positivt i avviksrapporteringen i Oppvekst og utdanning. Det vil imidlertid være viktig å følge dette opp med analyse av de rapporterte avvikene også på virksomhetsnivå, for å sikre at eventuelle problemer blir identifisert og løst. Dette innebærer blant annet å lukke avvik og at forbedringsforslag blir tatt med i vurderingen av tiltak. Å synliggjøre tiltak som resultat av avviksmelding, gir også et signal til ansatte om at meldte avvik tas på alvor og gir læring.

Rapportering av avvik er en sentral del av kommunens internkontroll. Kommunens rutiner legger opp til kontinuerlig gjennomgang av innmeldte avvik, og gjennomganger på mer overordnet nivå. Imidlertid ser det ut til at det er en utfordring i skolene når det gjelder å følge opp og lære av avvik i virksomhetene. Systematisk oppfølging av avvik, kan bidra til å sikre tiltak som i neste omgang kan hindrer gjentakelser og derav øke kvalitet og sikkerhet i tjenesteleveranse. Kommunen anbefales derfor å sørge for at oppfølging og læring av avvik, blir prioritert på alle nivåer i organisasjonen, fra ledernivå til den enkelte medarbeider.

4.6 ANBEFALING

Revisjonen anbefaler kommunen å:

- legge til rette for en åpen å støttende meldingskultur
- vurdere om det skal iverksettes bevisstgjørende tiltak/ytterlig opplæring knyttet til rapportering av avvik som omhandler informasjonssikkerhet og personvern
- sikre systematisk oppfølging av avvik også på virksomhetsnivå

VEDLEGG

Definisjoner

Personvernbegrepet refererer til vernet av privatlivets fred og den enkeltes personlige integritet, og rett til å ha innflytelse på bruk og spredning av egne personopplysninger.[59] Brudd på informasjonssikkerhet kan skyldes dataangrep og hacking som gjøres med hensikt, men også ved at ansatte gjør brukerfeil eller opptrer uaktsomt. Ansatte kan, for eksempel, utilsiktet bidra til datainnbrudd ved å klikke på lenke i e-post eller gi annen informasjon som gir hackere tilgang til IT-systemer.

Personopplysninger er enhver opplysning om en privatperson som er identifisert eller som kan identifiseres, for eksempel navn, adresse, telefonnummer, e-post, fødselsnummer, adferdsmønstre og bilde dersom personer kan gjenkjennes.

Særlige kategorier av personopplysninger: Personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, genetiske opplysninger og biometriske opplysninger, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering[60].

Særlig vern for barn: Barn er i mindre grad bevisste på aktuelle risikoer, konsekvenser og rettighetene de har, og deres personopplysninger skal ha et særlig vern.[61] Ifølge Utdanningsdirektoratet skal barns personopplysninger ved tvil behandles som særlig kategori. I tillegg finnes det andre opplysninger som ikke er definert som særlig kategori i personvernregelverket, men som skal behandles med ekstra forsiktighet. Eksempelvis adresse til elever eller foresatte som bor på hemmelig adresse, eller dersom adressen er tilknyttet helseinstitusjon vil dette regnes som behandling av helseopplysninger som er særlig kategori. Det samme gjelder for vanskelig familie- eller hjemmeforhold.

DPIA (Data Protection Impact Assessment) er en vurdering av personvernkonsekvenser som skal sikre at personvernet til de som er registrert i løsningen ivaretas.

Databehandler behandler personopplysninger på vegne av andre. Databehandleren behandler personopplysningene etter instruks fra en annen virksomhet, og kan ikke bestemme formål eller andre avgjørende elementer ved behandlingen. Dette avklares i en databehandleravtale, mellom behandlingsansvarlig (kommunen) og databehandleren (tjenesteleverandør)[62].

---

[59] Datatilsynet
[60] Lov om behandling av personopplysninger – artikkel 9
[61] Hva er personopplysninger? (udir.no)
[62] Behandlingsansvarlig og databehandler | Datatilsynet

Muntlig kilder fra kommunene

Totalt er det intervjuet 25 personer. Disse er:

- Seksjonssjef Informasjonssikkerhet, Innovasjon og støttetjenester
- Personvernombud
- Leder Forvaltning, Oppvekst og utdanning
- Prosjektleder Vigilo
- Seksjonssjef IT, Innovasjon og støttetjenester
- Informasjonssikkerhets- og personvernrådgiver
- Representanter for Austbø skole:
  - 3 representanter fra skolens administrasjon
  - 1 lærer
- Representanter for Eiganes skole:
  - 3 representanter fra skolens administrasjon
  - 2 lærere, 1 avdelingsleder

Skriftlige Kilder fra kommunen

- Rutiner, retningslinjer og veiledere for informasjonssikkerhetsarbeid
- Rutine for avviksbehandling
- Rollebeskrivelser for informasjonssikkerhetsansvar
- Sjekkliste for behandling av personopplysninger
- Intranett
- Tertialrapportering per 31.08.2021 – Rapportering (stavanger.kommune.no)