FORVALTNINGSREVISJONSRAPPORT
FREDRIKSTAD KOMMUNE
ROLVSØY, 27. MAI 2020

Personvern

INNHOLDSFORTEGNELSE

SAMMENDRAG

Den nye personvernforordningen innebærer nye og strengere regler på flere områder, og nye rettigheter for innbyggerne. Blant annet nye regler om avvikshåndtering som pålegger kommunene en økt plikt til rapportering av avvik til Datatilsynet og varsling av berørte.

Østre Viken kommunerevisjon fikk i oppdrag å gjennomføre forvaltningsrevisjon på området kommunens implementering og ivaretakelse av det nye personvernregelverket. Vi har undersøkt om kommunen har implementert personvernregelverket. I den sammenheng har vi sett på hvordan kommunen har vurdert hvilke personopplysninger de har behov for, hvorfor de har behov for disse, hvor lenge de har behov for opplysningene, hvordan opplysningene er lagret og hvem som skal ha tilgang til opplysningene. Vi har også sett på om kommunen har et personvernombud som får virke i henhold til regelverket.

Kommunen skal ivareta sitt ansvar på personvernområdet. Det betyr at kommunen må sikre at ansatte som håndterer personopplysninger etterlever regelverket. Vi har i den sammenheng sett på om kommunen har gitt de ansatte tilstrekkelig opplæring i regelverket, om kommunen har gjennomført risikovurderinger knyttet til behandlingen av personopplysninger og om de har intern kontroll på området.

Revisjonen tar utgangspunkt i personvernregelverkets syv grunnkrav, som er (1) lovlig, rettferdig og gjennomsiktig, (2) formålsbegrenset, (3) dataminimering, (4) riktighet, (5) lagringsbegrensing, (6) integritet og konfidensialitet, og (7) Ansvarlighet.

Metodene som er benyttet i gjennomføringen av denne revisjonen er intervjuer med et utvalg av kommunens ansatte på administrativt nivå, ansatte i en utvalgt barnehage og ansatte på en utvalgt skole. Det er innhentet dokumentasjon fra både administrativt nivå i kommunen, fra den utvalgte barnehagen og fra den utvalgte skolen. Vi har også hatt en gjennomgang av kommunens nettsider og den informasjonen som er tilgjengelig der på det reviderte området. Revisjonen har hatt et stedlig gjennomsyn av kommunens systemer for registreringer knyttet til personvernopplysninger i protokoll og avvikssystem, og det er gjennomført en spørreundersøkelse med kommunens ledergruppe, alle rektorer og styrere, og ansatte i syv barnehager og ansatte i 10 skoler. 70 % av kommunens ledergruppe og 78 % av rektorene og styrerne i kommunen svarte på spørreundersøkelsen, samt 158 lærere og barnehagepedagoger.

Resultatet av våre undersøkelser viser at kommunen informerer kommunens innbyggere om personvernet i en personvernerklæring og i tilknytning til de digitale skjemaene på sine nettsider. Informasjonene er imidlertid noe avgrenset og noe er ikke oppdatert i henhold til gjeldende regelverk. Kommunen ivaretar personers rettigheter til innsyn, retting og sletting av opplysninger, samt overføring av opplysninger til en annen behandlingsansvarlig. Kommunen har utarbeidet mange rutiner og prosedyrer på området personvern. Svært mange av rutinene og prosedyrene omhandler informasjonssikkerhet knyttet til personopplysninger behandlet i ulike IT-systemer, og i liten grad de andre områdene i personvernregelverket. I denne undersøkelsen kommer det frem at det er store forventinger til personvernombudet, utover det som er beskrevet i kommunens rutiner, og det er ikke tydelig for ansatte i organisasjonen hvem som skal utføre de ulike oppgavene i arbeidet med personvernregelverket. Det gjenstår fremdeles en del arbeid rundt vurderingen, registreringen og risikovurderingen av de ulike behandlingene av personopplysninger i kommunen. Det kommer også frem at ansatte har behov og ønske om mer opplæring på personvernregelverket, som er et omfattende regelverk.

Basert på våre vurderinger har vi anbefalt at kommunen bør:

- sørge for å gi de registrerte informasjon om behandlingen av personopplysninger, herunder kategoriene personopplysninger, hvor opplysningene hentes fra, hva som er formålet med behandlingen og hvor lenge de lagres
- vurdere å gi informasjon om behandlingen av personopplysninger og personers rettigheter som i større grad er tilpasset og forståelig også for barn og unge
- utarbeide en oversikt og føre protokoll over de ulike behandlingene av personopplysninger i kommunen, hvordan og hvor opplysningene lagres, når de skal slettes, og hvordan personopplysningene brukes og hva som er formålet
- gjennomføre risikovurderinger av personvernkonsekvens DPIA, der det er nødvendig
- oppdatere personvernerklæringene i de digitale skjemaløsningene til gjeldende regelverk, sørge for at sensitive personopplysninger ikke kan føres i åpne skjemaløsninger og informere om personvernet der det skal eller kan føres sensitive personopplysninger.
- tydeliggjøre hvem som skal ivareta de ulike oppgaven i arbeidet med personvern og vurdere personvernets tilgjengelige ressurser i forhold til pålagte oppgaver og forventning
- oppdatere prosedyrer og rutiner knyttet til sikkerhetsorganiseringen i kommunen, slik at disse er i tråd med dagens sikkerhetsorganisering.
- vurdere å synliggjøre personvernregelverkets krav i større grad i rutiner og prosedyrer som berører personvern
- se til at det er et fungerende system for rapportering fra personvernombudet til kommunens øverste leder, enten gjennom kommunens sikkerhetsutvalg eller på annen måte
- iverksette et system for å innhente informasjon fra virksomhetene for å vurdere om personvernregelverket etterleves og iverksette tiltak der det er nødvendig (internkontroll)
- gi mer tilgjengelig og målrettet opplæring til ansatte i organisasjonen på personvernregelverket

1 INNLEDNING

1.1 Bakgrunn

Østre Viken kommunerevisjon IKS utfører forvaltningsrevisjon på oppdrag fra kontrollutvalget. Forvaltningsrevisjon er en lovpålagt oppgave for kommunene, og er kontrollutvalgets ansvarsområde, jf. kommuneloven § 77. Forvaltningsrevisjon er systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger fra kommunestyrets eller fylkestingets vedtak.

I bystyret 15. mars 2018 - sak 47/18, ble forvaltningsrevisjonsplan for 2018-2019 vedtatt. Planen bygger på risiko- og vesentlighetsvurderinger av kommunen. Av vurderingene kommer det frem følgende:

«Flere av kommunens virksomheter forvalter en stor mengde personopplysninger, både opplysninger om kommunens innbyggere, men også opplysninger om ansatte. Kommunen plikter å behandle slike opplysninger i tråd med personopplysningsloven. Personopplysningsloven krever at opplysningene skal beskyttes tilfredsstillende mot uberettiget innsyn og endringer – konfidensialitet og integritet. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene når de har behov for det. Loven stiller krav til etablering og oppfølging av tiltak som er nødvendig for å oppfylle kravene til behandling av personopplysninger – i et internkontrollsystem.

I april 2016 vedtok EU en ny forordning om behandling av personopplysninger. Forordningen erstatter og opphever EUs gjeldende personverndirektiv 95/46. Forordningen er EØS-relevant, og det legges opp til at den skal innlemmes i EØS-avtalen og gjennomføres i norsk rett. Regjeringen har lagt opp til at det gis en ny personopplysningslov som gjennomfører forordningen, og at den någjeldende personopplysningsloven og -forskrift oppheves. Loven skal etter planen tre i kraft 25. mai 2018 (samme dag som forordningen gjøres gjeldende i EU). Forordningen innebærer nye og strengere regler på flere områder, og nye rettigheter for innbyggerne. Blant annet kommer det nye regler om avvikshåndtering som pålegger kommunene en økt rapportering av avvik til Datatilsynet og varsling av berørte. Regelverket endrer også reglene knyttet til gebyr og åpner for at det kan ilegges bøter på opptil 20 millioner Euro alt. 4 % av omsetning.

Brudd på personvern er egnet til å skape mistillit, både hos ansatte og kommunens innbyggere, noe som igjen kan påvirke kommunens omdømme. For å redusere potensielle sikkerhetsrisikoer er det, etter revisjonens oppfatning, avgjørende at ansatte får hensiktsmessig opplæring om krav til internkontroll og informasjonssikkerhet, oppgavefordeling og rutiner, samt riktig bruk av IKT-systemene. I en fase med nye regler er dette ekstra viktig for å sikre at kommunen etterlever de nye reglene.

Revisjonen har ikke opplysninger som tilsier at det foreligger brudd på regelverket i Fredrikstad kommune, men erfaringsmessig mener vi at risikoen for brudd er stor. Datatilsynet har i perioden 2013 til 2016 gjennomført nærmere 45 kontroller hos norske kommuner og fylkeskommuner. Datatilsynet fant at kommunene i stor grad sliter med å ha tilstrekkelig oversikt over sine behandlinger av personopplysninger og med å dokumentere reelle risikovurderinger til disse. Datatilsynet fant også at en god del kommuner mangler oversikt over plikter knyttet til informasjon og innsyn etter personopplysningsloven. Noe overaskende ble det funnet mindre forskjeller på store og små kommuner enn man skulle forvente og datatilsynet fant heller ingen tydelige geografiske forskjeller. Flere av kommunene hadde så graverende avvik at de ble ilagt overtredelsesgebyr.

Det faktum at det er nye regler på området innebærer, etter revisjonens oppfatning, dessuten en økt grad av sannsynlighet for brudd på regelverket. Ettersom gebyrene som kan ilegges for brudd på

regelverket i henhold til ny forordning har økt drastisk vil dette også innebære en økt økonomisk konsekvens.»

Prosjektet er utformet på bakgrunn av beskrivelsen i risiko- og vesentlighetsvurderingene. Vi har gjennomført oppstartsmøte med kommuneadministrasjonen slik at det også er tatt hensyn til administrasjonens innspill i prosjektet

Prosjektplan for gjennomføring av prosjektet ble vedtatt av kontrollutvalget i møte 27.11.2019, sak PS 19/69.

1.2 Gjennomføring av prosjektet

Østre Viken kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med «Standard for forvaltningsrevisjon» (RSK 001)/god revisjonsskikk. Dette innebærer blant annet at rapporten skal skille klart mellom hva som er innsamlet data og hva som er revisjonens vurderinger, og at det skal være en tydelig sammenheng mellom problemstillinger, innsamlede data, vurderinger, konklusjoner og eventuelle anbefalinger.

Oppstartsmøtet ble gjennomført 15. november 2019. Arbeidsutkast med faktadelen i rapporten ble sendt til Fredrikstad kommune 18.03.2020 for vurdering. På grunn av Coronasituasjonen så ikke kommunen seg i stand til å komme med vurderinger av fakta i denne omgang og ba i brev datert 03.04.2020 om en ny mulighet senere i prosessen. Arbeidsutkast med fakta, vurderinger, konklusjoner og anbefalinger ble sendt kommunen og et høringsmøte på Teams ble gjennomført 24.04.2020. Kommunaldirektør for utdanning og oppvekst hadde ikke anledning til å delta og kommunen ba om forlenget frist for faktavurdering av virksomhetene i revisjonen. Ny frist for faktavurderinger ble satt til 11.05.2020. Endelig rapport ble sendt på offisiell høring til kommunen 18.5.2020. Vi mottok kommunedirektørens høringsuttalelse xx. xx 2020. Kommunedirektørens høringsuttalelse er å finne i kapittel 4 i denne rapporten.

1.3 Problemstilling og avgrensing

I prosjektplanen er det vedtatt at prosjektet skal besvare følgende problemstilling:

- Har kommunen implementert personvernregelverket – GDPR[1]?

Å sikre at de ansatte etterlever regelverket er en forutsetning for implementering, og revisjonen vil ta utgangspunkt i grunnkravene i personvernregelverket:
1. Lovlig, rettferdig og gjennomsiktig
2. Formålsbegrenset
3. Dataminimering
4. Riktighet
5. Lagringsbegrensing
6. Integritet og konfidensialitet
7. Ansvarlighet

Revisjonen er gjennomført både på administrativt nivå og ut mot utvalgte enheter i kommunen. I oppstartsmøte med kommuneadministrasjonen 15.11.2019, kom det frem at det er ønskelig fra administrasjonens side at revisjonen gjennomføres både med en utvalgt skole og med en utvalgt

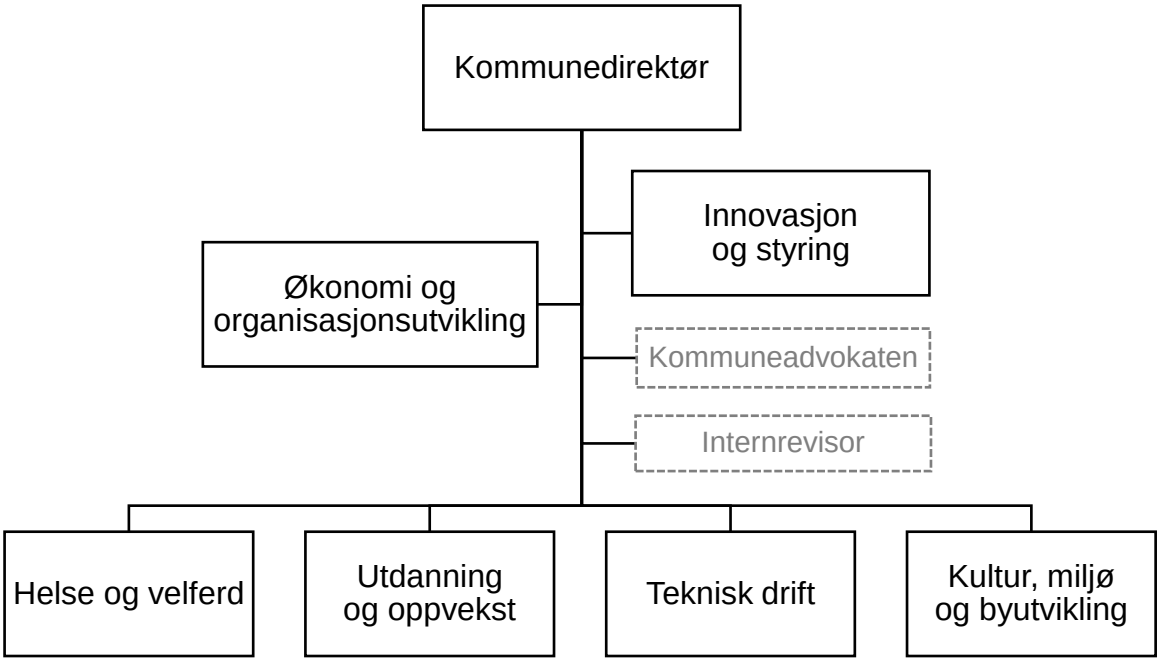
[1] Personvernforordningen - General Data Protection Regulation (GDPR)

barnehage. Dette for å gjøre en vurdering av om personvernregelverket er implementert helt ut mot brukerne i kommunen.

På bakgrunn av de rammene som er lagt til grunn, vil prosjektet handle om kommunen har implementert den nye personvernlovgivningen som fremkommer i personopplysningsloven (popplyl) og personvernforordningen (pvf eller GDPR). Revisjonen vil da vurdere om kommunen har implementert personvernforordningens syv grunnkrav, om de har et personvernombud etter regelverket, databehandleravtaler, om de har gjennomført en risikovurdering på området og om de har satt ansatte i stand til å ivareta regelverket. Revisjonen har ikke vurdert hvorvidt det er samlet inn opplysninger som strider mot personvernlovgivningen, utover det som fremkommer i intervjuene og spørreundersøkelsene. Vi har heller ikke vurdert de enkelte databehandleravtalenes innhold, utover at vi ser om kommunen har rutine for å utarbeide slike avtaler, hvordan de går frem og om de har oversikt.

Fredrikstad kommune er organisert med kommunedirektør, to stabsfunksjoner og fire fagseksjoner. Hver seksjon er organisert med tilhørende etater og virksomheter.

Figur 1: Organisasjonskart Fredrikstad kommune



Definisjoner og begrepsforklaringer er å finne i vedlegg 3.

1.4 Revisjonskriterier

Revisjonskriterier er en samlebetegnelse for krav og forventninger som blir brukt til å vurdere ulike sider av kommunens virksomhet og tjenester. Kriteriene blir blant annet utledet av regelverket, politiske vedtak og føringer, eller kommunens egne retningslinjer på det området som prosjektet tar for seg.

I denne rapporten er følgende kilder benyttet til å utleder revisjonskriteriene

Lov og forskrift

- Lov om behandling av personopplysninger (personopplysningsloven), LOV-2018-06-15-38
- EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR]'
- Forskrift om kameraovervåking i virksomhet, FOR-2018-07-02-1107
- Prop. 56 LS (2017-2018)

Veiledninger og føringer

- https://www.datatilsynet.no/ - veiledninger på personvernregelverket
- *Personvern, taushetsplikt og meldeplikt – Regelverk for skolen*, Pedlex, ISBN: 978-82-8372-140-9
- *Personvern i skole og barnehage*, samlerapport juni 2014 – Datatilsynet
- *Veiledning om kontroll og overvåking i arbeidslivet – Arbeidstilsynet – Datatilsynet – Petroliumstilsynet og Partene i arbeidslivet*

Utledning av revisjonskriteriene følger i vedlegg 1. Revisjonskriterier fremkommer punktvis under hvert tema. Revisjonskriterier ble også oversendt kommunen i oppstartsbrevet 29.11.2019, med muligheter for innspill fra kommunen.

1.5 Metode

Fakta er en gjengivelse av informasjonen vi har fått tilgang til gjennom datainnsamlingen. I dette prosjektet er informasjonen hentet inn gjennom bruk av følgende metoder:

- Dokumentanalyse
- Intervjuer
- Spørreundersøkelse
- Systemgjennomsyn – avviksregistrering og protokoll

Der vi konkluderer, vil alltid vurderingene bygge på skriftlig dokumentasjon eller informasjon som kommer fra flere kilder.

1.5.1 Dokumentanalyse

Vi har gjennomgått sentrale dokumenter på området. Det er innhentet dokumentasjon fra både administrativt nivå i kommunen og fra den utvalgte skolen og den utvalgte barnehagen. Vi har også hatt en gjennomgang av kommunens nettsider og den informasjonen som er tilgjengelig der på det reviderte området. Vi tok utgangspunkt i relevante dokumenter som ble sendt inn i forbindelse med det forrige forvaltningsrevisjonsprosjektet Cyberangrep og informasjonssikkerhet i Fredrikstad kommune. I kommunikasjon med kommunen fremkom det imidlertid at flere av dokumentene var blitt oppdatert. De oppdaterte dokumentene er lagt til grunn i dette prosjektet. Fullstendig oversikt over dokumentene følger i vedlegg 2.

1.5.2 Intervjuer

Det er gjennomført totalt 11 intervjuer med 15 personer i prosjektet

- Personvernombud
- Leder for byarkivet
- Avdelingsleder servicetorget
- Teamleder HR
- Digitaliseringssjef
- Løsningsansvarlig utdanning og oppvekst
- Styrer i barnehage

- Gruppeintervju med 3 barnehagelærere
- Rektor på en skole
- Merkantilt ansatt på en skole
- Gruppeintervju med 3 kontaktlærer på en skole

Alle intervjuer er verifisert. Det betyr at den som er intervjuet, får lese gjennom referatet fra intervjuet for å bekrefte at referatet er i overenstemmelse med det som ble sagt under intervjuet og rette opp eventuelle misforståelser.

1.5.3 Spørreundersøkelse

Det er gjennomført spørreundersøkelse i Questback[2]. Det er gjennomført to spørreundersøkelser i denne revisjonen. En spørreundersøkelse til kommunens ledergruppe på administrativt nivå, og en spørreundersøkelse til alle rektorene, styrerne i kommunen og lærere ved 10 utvalgte skoler og barnehagelærere ved 7 utvalgte barnehager.

Spørreundersøkelsen til kommunens ledergruppe ble sendt til 37 ledere. 26 personer besvarte undersøkelsen, noe som tilsier en svarprosent 70 %.

Spørreundersøkelsen til rektorene og styrerne ble sendt til 51 personer. 40 personer besvarte undersøkelsen, noe som tilsier en svarprosent på 78 %. Den samme undersøkelsen ble sendt til et utvalg lærere ved 10 skoler og barnehagelærere ved 7 barnehager. Undersøkelsen ble sendt via rektor/styrer i den enkelte virksomhet. 158 lærere og barnehagelærere og 2 merkantile har besvart undersøkelsen.

Det er vår vurdering at antall svar i undersøkelsen gir et godt grunnlag for analysen, som presenteres i rapporten. Spørreundersøkelsene er å finne i vedlegg 3 og 4.

1.5.4 Systemgjennomsyn

Revisjonen har hatt et stedlig gjennomsyn av protokoll for behandling av personopplysninger og system for registrering av brudd/avvik på personvernregelverket. I denne gjennomgangen var personvernombudet tilstede. Kommunen bruker ulike moduler i Risk Manager til disse registreringene.

1.5.5 Validitet og reliabilitet

I henhold til god revisjonsskikk skal praksis eller tilstand innen det reviderte området beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner. I dette prosjektet har vi benyttet data fra ulike kilder, og brukt ulike innsamlingsmetoder for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet.

Utfordringer og begrensninger i rapportens faktagrunnlag er beskrevet ovenfor sammen med beskrivelsen av de ulike metodene som er benyttet. Vi tar også hensyn til metodens begrensninger i vurderingene.

Vi har kvalitetssikret faktagrunnlaget underveis, både gjennom verifisering av intervjuer, bistand fra kommunen ved gjennomsyn av kommunens systemer og ettersending av dokumentasjon. I tillegg er rapportens faktadel i sin helhet gjennomgått av kommunen i høringsmøtet 24.04.2020, samt supplert med innspill pr. e-post i etterkant, slik at eventuelle faktafeil eller misforståelser er rettet opp. På denne bakgrunn mener vi at rapporten fremstiller kommunen på en riktig måte, og at vi har et godt grunnlag for våre konklusjoner og anbefalinger.

[2] Questback er et digitalt system for blant annet spørreundersøkelser og analyser.

Undersøkelsen er gjennomført av forvaltningsrevisor Karianne Åsheim og Unn Elisabeth West i perioden november 2019 til april 2020.

2 IMPLEMENTERING AV PERSONVERNREGLEMENTET

2.1 Lovlig, rettferdig og gjennomsiktig

2.1.1 Behandling av personopplysninger

Personopplysningsloven krever at opplysningene skal beskyttes tilfredsstillende mot uberettiget innsyn og endringer – konfidensialitet og integritet. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene når de har behov for det.

Revisjonskriterier

- Kommunen behandler personopplysninger på en lovlig, rettferdig og åpen måte med hensyn til den registrerte.
- Kommunen skal gi den registrerte informasjon om behandlingen av personopplysninger, skriftlig herunder elektronisk
- Kommunen fører en protokoll over behandlingsaktiviteter som utføres under deres ansvar.
- Protokollene skal være skriftlige, herunder elektroniske.
- Kommunen har innhentet samtykke til de nødvendige kategoriene personopplysninger.
- Kommunen bruker kameraovervåking i henhold til retningslinjene.
- Kommunen har sørget for å ikke benytte uekte kameraovervåkingsutstyr eller ved skilting, oppslag eller lignende gi inntrykk av at kameraovervåking finner sted.

Fakta

Administrative nivå

I prosedyren *Organisering av personvern- og informasjons-sikkerhetsarbeidet*, sist oppdatert 09.12.2019 er det en beskrivelse av hvilke funksjoner i kommunen som skal utføre de ulike oppgavene i arbeidet med personvern og informasjonssikkerhet. Her fremkommer det at det er etablert et sikkerhetsutvalg, som jobber på tvers i hele kommunen og utgjør et team for å ivareta IT-sikkerheten i hele kommunen. I intervjuene kommer det frem at alle sider av personvernet, både det som er knyttet opp mot IT sikkerheten og andre deler av arbeidet med personvernet skal ivaretas av sikkerhetsutvalget.

I intervjuene viser ansatte til kommunens personvernerklæring når det gjelder det å informere om behandlingen av personopplysninger. På nettsidene til kommunen står det nederst til høyre på første siden et punkt om personvern. Der ligger det først informasjon om bruken av informasjonskapsler (cookies). Nederst på denne siden er det en link med teksten «*Du kan lese mer om informasjonssikkerhet her».* Under denne linken står det *Informasjonssikkerhet*, her finnes kommunens personvernerklæring. Alternativt må brukerne gå inn på linken «om kommunen» og velge underpunktet informasjonssikkerhet. I erklæringen gir kommunen blant annet informasjon om hvordan kommunen sikrer brukerens personopplysninger i ulike system og om personers rettigheter.

Det kommer frem av intervjuene at ansatte ikke synes at personvernerklæringen er så enkel å finne som den burde være, på kommunens hjemmeside. Når det gjelder andre måter å informere om personvernregelverket på, så fremkommer det av intervjuene at helseområdet i større grad enn

resten av kommunen også informerer direkte til brukerne om personvernet. Det kommer frem av intervjuene at det ble gjort en stor jobb med å utarbeide en personvernerklæringen da det nye regelverket trådte i kraft. Personvernerklæringen ble «språkvasket» for å bli mer forståelig. Det kommer imidlertid frem av intervjuene at personvernregelverket ikke er lett å forstå for alle grupper brukere og at personvernerklæringen er mer for bevisste voksne.

I oversendt presentasjon *Ny personvernlov GDPR til LA ,* datert 28.05.2018 står det på s. 3 at alle skal forstå personvernerklæringen, også barn.

I kommunens personvernerklæring står det «*Våre elektroniske skjema leveres av eksterne leverandører. For å kunne benytte deg av disse skjemaene er du nødt til å samtykke i en personvernerklæring.»* På kommunens nettsider, under *Skjema A-Å* har kommunen en rekke skjemaer som er ment for kommunens brukere. I intervjuene fremkommer det at de fleste digitale søknader går via id-porten. Skjemaer som inneholder blant annet personnummer skal gå via id-porten. Ved innlogging på id-porten, må det hukes av for å ha lest personvernreglene før brukerne kommer til selve skjemaene. Informasjonen som fremkommer om behandlingen av personopplysninger er ikke oppdatert i henhold til gjeldende regelverk. Siste oppdatering var i 2015.

Ved en gjennomgang av andre skjemaer på kommunens nettsider, kommer det også frem flere skjemaer som ikke er elektroniske. Det er ikke angitt informasjon om personvernet og behandlingen av personopplysninger i disse skjemaene.

Kommunikasjonsavdelingen legger ut skjemaene på nettsidene, men i henhold til opplysninger fra intervjuene er det den enkelte fagavdelingen som skal sikre innholdet og formatet på de ulike søknads- og henvisningsskjemaer. Det er også den enkelte fagavdeling som skal se til at det fremkommer opplysninger om personvernet knyttet til skjemaene. Noen skjemaer fremkommer i pdf-format, og kan lastes ned. Et eksempel er *Søknad vedrørende bolig*. I dette skjemaet ber kommunen om personopplysninger og det er åpne felt der søkeren kan fylle ut flere personopplysninger. På slutten av skjemaet fremkommer det at vedkommende som fyller ut skjemaet skal samtykke til bruk og lagring av opplysningen jf. personvernloven. Det fremkommer ikke informasjon om hvordan opplysningene behandles, lagres, sikres eller slettes. Det vises ikke til personvernforordningen eller hvordan skjemaet kan sendes til kommunen på en sikker måte. Et annet eksempel på dette er skjema for *Henvisning til fysio- og ergoterapitjenesten*. For skjema *Bekymringsmelding* skal melder krysse av for å ha lest og samtykket til behandling av personopplysninger. Informasjonen som fremkommer om behandlingen av personopplysninger er heller ikke her oppdatert i henhold til gjeldende regelverk. Siste oppdatering var i 2015.

Det kommer frem av intervjuene at det ikke finnes rutiner for hvem som skal sørge for å informere om behandlingen av personopplysninger knyttet til selvbetjeningsskjemaene.

I intervjuene informerer servicetorget om at de mottar mange henvendelser som inneholder personopplysninger, særlig pr. telefon. Antall ansatte på servicetorget har blitt redusert de siste årene pga. økt digitalisering. Servicetorget får nå flere henvendelser via andre medier, det er dermed færre telefoner og personlig oppmøte enn tidligere. Personopplysninger nedtegnes kun i CRM[3] Dette er et meldingssystem til andre virksomheter internt i kommunen.

<u>Kameraovervåking</u>
Det kommer frem av intervjuene at personvernombudet har utarbeidet prosedyrene for kameraovervåking. Personvernombudet informerer om at det har vært en gjennomgang med de

[3] Custom Relationship Managment.

som følger opp bruken av kameraene i kommunen, blant annet en opplæring om utlevering og sletting etc. Det kommer frem av intervjuene at alt på kameraene blir slettet automatisk etter 7 dager, hvis ikke sletting blir stoppet av en gyldig årsak. Det *er Teknisk drift v/ Vakt og sikring* som skal ivareta dette området. Det er *Bygg og eiendom* som skal avgjøre når/hvor det skal være kameraovervåkning. Det kommer frem av intervjuene og ved observasjon at det er montert kameraer utenfor servicetorget, disse er det skiltet for.

Det kommer frem av intervjuene at når personvernombudet har fått meldinger om at det er satt opp nye kamera, så har ombudet etterspurt registrering av behandlingene. Det kommer frem av intervjuene og systemgjennomgangen at behandlingene av kameraovervåking først ble registrert uken før intervjuene med revisjonen.

Det kommer frem av intervjuene at ansatte ikke kjenner til at det er satt opp skilting for kamera steder det ikke er montert kamera. Det kommer også frem at kommunen ikke har montert web-kameraer.

Ansatte

I dokumentet *Saksbehandling i personalsaker som kan få arbeidsrettslige følger – arbeidstakers forhold*, datert 21.10.2019 fremkommer det informasjon om hvordan personopplysninger samles inn og brukes. Det fremkommer også opplysninger om at den ansatte skal informeres om saksbehandlingen og rutinen. Det står at den ansatte skal få lese eventuelle referater som utarbeides underveis og om den ansattes rettigheter dersom det fattes vedtak i saken.

Personopplysninger om ansatte i kommunen henter IT-avdelingen fra HR. Bruker-id som benyttes, hentes fra HR-ident. Alle brukere av IT- systemene finnes også i HR-registeret.

Det kommer frem av intervjuene at IT-avdelingen ikke overvåker hva ansatte søker på, e-postbruk ol. De kan i praksis gjøre det, da enkelte systemer loggfører aktivitet. Tilgangen til disse løsningene benyttes bare ved høyst spesielle tilfeller, som hvis politiet ber om bevismateriale. AD[4] kan brukes til å sjekke når ansatte kommer på jobben, eller når ansatte går fra jobb. IT-avdelingen har fått henvendelser fra ledere som for eksempel ønsker å vite når en ansatt har gått fra jobb. IT opplyser om at de ikke leverer ut data internt på disse områdene. Dataene brukes bare til «nøkkelkontroll» og ikke til å kontrollere hvem som er tilstede på kontoret, som eksempel. IT er imidlertid usikker på om ansatte har fått informasjon om at AD informasjon lagres en viss tid, og at det ikke brukes til andre formål.

I intervjuene blir det bekreftet at ansatte ikke har blitt informert om hvorvidt registreringer med adgangskort blir lagret eller hvordan det brukes/ikke brukes. Når det gjelder kameraene inne på servicetorget, sier avdelingsleder på servicetorget at hun mener at de ansatte ikke blir filmet av disse kameraene når de arbeider på servicetorget.

Kommunen har GPS i bilene til ansatte i hjemmesykepleien. Det kommer frem av intervjuene at dette ble drøftet for noen år siden og de ansatte dette berører, er orientert om hvordan disse opplysningene brukes, lagres og slettes.

Protokoll

I RUNDSKRIV nr. 3 2018 om GDPR datert 04.06.2018 under punktet *Oppgaver i seksjoner/etater/virksomheter* står det *«Fredrikstad kommune skal ha oversikt over alle behandlinger av personopplysninger elektronisk. Alle seksjoner/etater/virksomheter som eier et datasystem der personopplysninger behandles, må registrere i et skjema hvordan disse behandlingene foregår. Det er*

[4] Teknisk definisjon av bruker ved adgangskontroll og inn-logging

viktig at alle systemer, også skytjenester som behandler personopplysninger, finnes i kommunens felles oversikt.» Det fremkommer ikke her at alle behandlinger av personopplysninger skal med i denne oversikten uavhengig av om behandlingen er i et digitalt system.

I en annen presentasjon *Rådmannsinnlegg på LUP*[5] *5. september 2018*, står det «*Kommunen skal ha oversikt over alle behandlinger.»* Det fremkommer av intervjuene at oversikten over behandlingene som gjøres i kommunen skal føres i Risk Manager, og at behandlingene skal registreres fortløpende. De som skal registrere behandlinger må gis tilgang til systemet, da dette ikke er tilgjengelig for alle.

I dokumentet *Sikkerhetsleder- Personvernombud,* datert 17.12.2018 står det at personvernombudet er «*Ansvarlig for å tilrettelegge for registrering av behandlinger. Registereier er ansvarlig for å registrere behandlingen*.» og «*Gi råd og veiledning til behandlingsansvarlig om behandling av personopplysninger og reglene for dette*.» Det står videre at personvernombudet har ansvaret for kontroll med risikovurderinger.

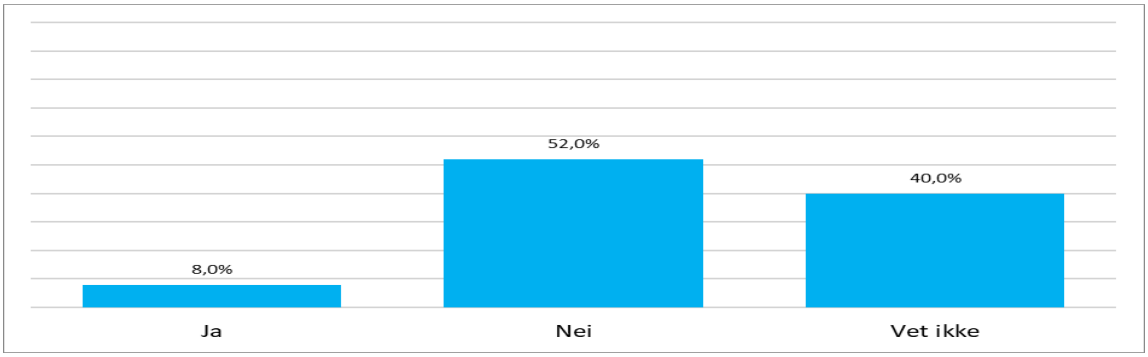
I en oversendt presentasjon *Ny personvernlov GDPR til LA* i 2018, datert 28.05.2018 står det *«Vi må gjennomgå alle våre behandlinger, dvs. all programvare og annet som inneholder personopplysninger. Det blir nye krav til behandlingene. Konsesjoner går ut. Vi må lage en ny oversikt som inneholder bl.a. formål og avgrensninger, bl.a. alle fagprogram, Ephorte, kamera etc.»* Under punktet *Fremdrift* står det *«LA-ene registrerer behandlinger i mai/juni 2018.»*

Når det gjelder føring av de ulike behandlingene av personopplysninger inn i protokollen (Risk Manager), sa flere av de vi har intervjuet at denne oppgaven ligger hos personvernombudet. I dokumentet *Sikkerhetsleder – personvernombud,* står det at personvernombudet er «*Ansvarlig for å tilrettelegge for registrering av behandlinger. Eier (kan være løsningsansvarlige) er ansvarlig for å registrere behandlingen.»*

I revisjonens gjennomgang av kommunens kvalitetssystem 19.12.2019 sammen med personvernombudet fremkommer det at det ikke er ført registreringer over de fleste av behandlingene av personopplysninger som kommunen gjennomfører. De få føringene som fremkommer i systemet har ulik detaljeringsgrad. Det kommer frem i intervjuene at få er kjent med om de behandlingene av personopplysninger som gjennomføres på deres område, er ført i modulen i Risk Manager.

I spørreundersøkelsen blir kommunes ledergruppe spurt om det er ført protokoll over de behandlingsaktivitetene som gjennomføres av personopplysninger på den enkeltes fagområde.

Figur 2: Er det ført protokoll over behandlingsaktiviteter?



N=25

[5] Lederutviklingsprogram i Fredrikstad kommune

Av de som sier at de behandler personopplysninger i deres virksomhet/enhet svarer 13 av 25 ledere at det ikke er ført protokoll over behandlingene av personopplysninger, 10 ledere sier at de ikke vet om det er gjort og 2 sier at behandlingene er ført i protokoll.

Virksomheter - grunnskole og barnehage

Det kommer frem av intervjuene med administrasjonen at det er de enkelte virksomhetene, som blant annet hver enkelt skole og barnehage, som skal orientere brukere/foreldre om personvern og ivaretakelsen av personopplysninger.

I intervjuene med ansatte på skolen kommer det frem at det i forbindelse med innføring av GDPR var mange spørsmål om hvordan skolene skulle informere de foresatte om personvernregelverket. De vi intervjuet på administrativt nivå kjente ikke til om det var utarbeidet informasjon om personvern rettet spesielt mot barn og unge i Fredrikstad kommune. Skolen har ikke utarbeidet slik informasjon.

I spørreundersøkelsen blir virksomhetsledere på 9 skoler med ungdomstrinn spurt om kommunen eller skolen har utarbeidet en egen personvernerklæring tilpasset barn og unge. En av skolene i undersøkelsen sier at det er utarbeidet en egen personvernerklæring tilpasset barn og unge. De andre 8 skolene sier at det ikke er utarbeidet en slik personvernerklæring, eller at de ikke vet.

Det kommer frem i intervjuene at alle skoleelever skal skrive under på et ordensreglement hvor det fremkommer at kommunen kan kontrollere systemene de er inne på, dersom de gjør noe de ikke har lov til på skolens IT-utstyr, for eksempel surfer på hatsider, porno etc. Alle skolene i kommunen har det samme ordensreglementet. Når det gjelder de yngste elevene, er det foreldrene som skriver under og det er deres ansvar å orientere sine barn om dette. Det sies i intervjuene at lærerne også burde orientere elevene om det i klasserommet.

I redegjørelse fra administrativt nivå 9.12.2019 står det at når barn skrives inn i skolen må foreldre blant annet undertegne ulike samtykkeskjema for innhenting av personopplysninger. Denne praksisen bekreftes i intervjuene med ansatte i skolen. Elevene blir rutinemessig tatt bilde av i forbindelse med skolekatalogen. Dersom det er gitt samtykke på innskrivningsskjemaet ved innskrivingen til skolen, hentes det ikke inn spesielt samtykke for dette. Dersom det ikke er gitt samtykke ved innskriving til skolen, vil skolen drøfte med foresatte før eventuelle bilder blir tatt. Det samme gjelder dersom det tas gruppebilder eller film i forbindelse med ulike sosiale aktiviteter på skolen. Dersom det skal tas bilder eller film av enkeltelever eller elever i små grupper til for eksempel avis, TV eller lignende, henter skolen inn samtykke fra foresatte, uansett om hva de tidligere har krysset av for i samtykke om dette i innskrivningsskjemaet. Denne praksisen blir også bekreftet i intervjuene med de ansatte i skolen. Ansatte sier at dette samtykket gjentas hvert år gjennom hele skolegangen. Det kommer frem av intervjuene at skolen ikke informerer om personers rettigheter ved innhenting av personopplysninger.

I skjemaet *Samtykke hjem – barnehage*, datert 12.10.2018 fremkommer de personopplysningene som barnehagen ber om samtykke til å kunne innhente. Barnehagen henter inn samtykke til bading/svømming, om barnet kan sitte på i privat bil og taxi, buss eller annen offentlig kommunikasjon. Videre hentes det inn samtykke til om navn, adresse og telefon kan utleveres til andre foreldre, om barnet kan bli filmet eller fotografert i forbindelse med aktiviteter og om barnet kan være med i ulike media (TV, radio, aviser, internett). Samtykke innhentes ved oppstart i barnehagen.

I spørreundersøkelsen svarer 35 av 40 rektorer og styrere at de kjenner til hvilke personopplysninger de må ha samtykke til å innhente. 5 av 40 svarer imidlertid at de ikke kjenner til hvilke personopplysninger de må ha samtykke til å innhente.

Det kommer frem av intervjuene med ansatte i barnehagen at de ikke informerer spesielt om behandlingen av personopplysninger og rettigheter til foreldrene, og dette har heller ikke vært tema i virksomhetsledergruppa. De mener imidlertid at det burde vært diskutert der, for eksempel ved overgang til skole.

I mottatt dokument for *Samtykke hjem-barnehage – opplysninger ved oppstart i barnehage*, datert 12.10.2018 fremkommer det opplysninger om at side 2 i dokumentet er unntatt offentligheten. Det fremkommer ikke informasjon om side 3 i dokumentet, som er et åpent tekstfelt der foreldre kan fylle inn personopplysninger de mener er relevante. Dokumentet gir ikke informasjon om personvernregelverket. Det fremkommer heller ikke informasjon om dette i dokumentet for samtykke til *Overføring av opplysninger barnehage-skole*, datert 15.10.2018 og heller ikke i dokumentet for samtykke til *Overføring av dokumenter barnehage-barnehage*, datert 15.10 2018, men det er her gitt opplysninger om at samtykke kan trekkes tilbake.

Vurderinger

Administrative nivå

Personvernregelverket sier at informasjon om behandling av personopplysninger skal gis skriftlig eller på annen måte, herunder elektronisk. Virksomheten må selv finne en passende måte å gi informasjonen på, innenfor visse rammer. Det er vår vurdering at kommunen gir skriftlig informasjon om behandlingen av personopplysninger under punktet *Informasjonssikkerhet* i personvern-erklæringen på kommunens nettsider. Kommunen gir også informasjon om behandling av personopplysninger ved inngangen til de elektroniske skjemaene der brukere skal registrere personopplysninger. Etter innlogging kommer det opp informasjon om bruk av informasjonskapsler og en personvernerklæringen. Vi finner imidlertid at regelverket det vises til i disse personvern-erklæringene er utgått og ikke gir ikke informasjon i henhold til regelverket som trådte i kraft i 2018. Vi vurderer videre at kommunen ikke i tilstrekkelig grad informerer om behandlingen av personopplysninger i skjemaer, som det ikke kreves innlogging til.

Plikten til å behandle personopplysninger på en åpen måte, innebærer at kommunen må gi kort og forståelig informasjon om hvordan de behandler personopplysningene. Det stilles også krav til hvordan det kommuniseres med enkeltpersoner.

Datatilsynet sier i sin veiledning at det ikke skal være nødvendig for brukerne å måtte lete etter informasjon om behandling av personopplysninger. Det skal være lett for den enkelte å finne frem i informasjonen. Det er vår vurdering at personvernerklæring kunne vært lettere tilgjengelig for brukerne av kommunens tjenester, enn slik den er plassert i dag. Kommunens brukere må gå flere trinn via informasjon om kommunen, for å komme frem til opplysningene om behandlingen av personopplysningene eller via opplysninger om cookies og inn på informasjonssikkerhet.

Det er vår vurdering at informasjonen om behandling av personopplysninger er skrevet på en måte som gjør at den er forståelig for mange av kommunens brukere. Datatilsynet sier imidlertid i sin veileder at for å sikre informasjon og åpenhet *«…må virksomheten kommunisere på en kortfattet, åpen, forståelig og lett tilgjengelig måte. Språket skal være klart og enkelt, særlig når informasjonen er spesifikt rettet mot barn.»* Det er vår vurdering at opplysningene i den generelle personvernerklæringene ikke gir informasjon på en sånn måte at barn og unge forstår hva som kan samles inn av personopplysninger, hva opplysningene skal brukes til, hvordan personopplysningene behandles, lagres eller slettes.

At behandlingen av personopplysninger skal være rettferdig, betyr at behandlingen skal gjøres i respekt for de registrertes interesser og rimelige forventninger. De som er registrert må forstå

behandlingen og behandlingen må ikke foregå på en skjult eller manipulerende måte. I erklæringen gir kommunen blant annet informasjon om hvordan kommunen sikrer brukerens personopplysninger og om personers rettigheter. Det fremkommer imidlertid lite informasjon om hvilke kategorier opplysninger som innhentes, hvor opplysningene hentes fra, hva som er formålet med behandlingen og hvor lenge opplysningene lagres slik kravet er i personvernforordningen artikkel 13 og 14. For at behandlingen skal være lovlig må det finnes et rettslig grunnlag for behandlingen av personopplysningene. Dette området er vurdert under kapittel 2.2 *Formålsbegrenset*.

I offentlig sektor behandles mange sensitive personopplysninger som er nødvendig for å kunne utøve tjenestene (formålet). I personvernforordningens fortale punkt 42 står det at samtykke ikke er å anse som frivillig dersom det ikke er reell valgfrihet, heller ikke dersom det å nekte samtykke er til skade for den registrerte. Kommunen må derfor i det enkelte tilfelle vurdere om det er aktuelt å benytte samtykke som behandlingsgrunnlag ved utøvelse av offentlig myndighet.

På bakgrunn av det som fremkommer i prosedyren *Organisering av personvern- og informasjons-sikkerhetsarbeidet* og intervjuene, er det sikkerhetsutvalgets oppgave å ivareta IT-sikkerheten. Det ser derfor ut til at ikke alle deler av arbeidet med personvern i kommunen ivaretas av dette utvalget. Gjennom intervjuene får vi imidlertid en annen forståelse av dette utvalgets oppgaveområde. I intervjuene kommer det frem at alle sider av personvernet, både det som er knyttet opp mot IT sikkerheten og andre deler av arbeidet med personvernet skal ivaretas av sikkerhetsutvalget. Det er vår vurdering at dette ikke er tydeliggjort i kommunens rutiner og organisering. På bakgrunn av denne uklarheten er det vår vurdering at kommunen i større grad bør tydeliggjøre at sikkerhetsutvalgets oppgaver omfatter arbeidet med personvernet i sin helhet.
Det gjelder for eksempel personvern knyttet til behandlinger av personopplysninger, der opplysningene for eksempel kun lagres og ikke er behandlet i et spesielt system. Virksomheten behandler opplysninger om personer selv om opplysningene ikke aktivt brukes. Det er å regne som en behandling enten behandlingen skjer elektronisk, automatisk eller manuelt.

Ansatte
Det er vår vurdering at kommunen behandler personopplysninger om de ansatte på en lovlig måte, men at de i liten grad informerer ansatte om hvilke personopplysninger som registres om dem, utover de opplysningen ansatte gir fra seg selv. Dette begrunnes i informasjon fra intervjuene og kommunens dokumenterte rutiner, der det fremkommer hvordan personopplysninger samles inn og brukes. Det fremkommer at den ansatte skal informeres om saksbehandlingen og rutinen, men ikke at den ansatte også skal informeres om rettighetene etter personvernregelverket.

Kameraovervåking
På bakgrunn av den informasjon som fremkom i intervjuene og kommunens dokumenterte rutiner for kameraovervåking, er vår vurdering at kameraovervåking benyttes i henhold til retningslinjene. Gjennom intervjuene er det sannsynliggjort at kommunen ikke benytter uekte kameraovervåkingsutstyr eller ved skilting, oppslag eller lignende gir inntrykk av at kameraovervåking finner sted.

Protokoll
Det er vår vurdering at kommunen har lagt til rette for å kunne etablere et system for å føre en skriftlig oversikt/protokoll over behandlingsaktivitetene i Risk Manager. Gjennomgangen av kommunens system og intervjuene viser imidlertid at dette arbeidet så vidt er påbegynt. De relativt få behandlingene som er ført i protokollen har også en svært ulik detaljeringsgrad. Datatilsynet sier i sin veiledning at behandlingene må være konkrete. For eksempel er «barnehage» ikke en behandling, mens søknader om barnehageplass eller notater-observasjoner av barn i barnehagen kan være eksempler på behandlinger på barnehageområdet. Gjennom intervjuene blir det også avdekket at det ikke er en enhetlig forståelse for hvem som skal sørge for å føre de ulike behandlingene i

protokollen. Vi legger til at alle behandlinger som omfatter personopplysninger skal registreres i protokollen jf. personvernforordningen artikkel 30. Dette gjelder uavhengig om det benyttes digitale systemer til behandlingene.

Det er vår vurdering at kommunen ikke i tilstrekkelig grad har ført sine behandlinger av personopplysninger i en oversikt/protokoll og at kommunen per i dag ikke har en fullstendig oversikt over behandlingsaktivitetene som gjennomføres i kommunen.

Virksomheter – skole og barnehage

Det foreligger ikke et krav om hvordan informasjon om behandling av personopplysninger skal gis, men det er et krav at den skal gis skriftlig – herunder elektronisk. Dersom noen ber om det kan den i tillegg gis muntlig. Informasjonen må gis før personopplysningene innhentes. Det er vår vurdering at barnehagene og skolene i møte med foreldrene bør opplyse om personvernregelverket og personers rettigheter for behandling av personopplysninger som gjelder for barna i barnehagen, elevene i skolen og familien deres. Denne informasjonen skal gis skriftlig, herunder elektronisk. Informasjonen skal gis før personopplysningene hentes inn. Informasjonen må omhandle hvorfor personopplysningene samles inn, hva opplysningene skal brukes til, hvordan personopplysningene behandles, lagres og eventuelt slettes i barnehagen, skolen og kommunen. Informasjonen kan i tillegg gis muntlig, dersom noen ber om det.

Både barnehagene og skolene behandler personopplysninger som ikke er nødvendige for driften. Dette krever samtykke. Kommuneadministrasjonen sier i sin redegjørelse at det kun innhentes samtykke ved innskriving i skolen og ellers kun i tilfeller der bilder eller film skal publiseres i aviser eller på TV. De vi intervjuet på skolen sier imidlertid at skolen også innhenter samtykke til å innhente ulike personopplysninger fra foreldrene hvert år. Det er vår vurdering at det er sannsynliggjort at skolens praksis er i tråd med Datatilsynets anbefalinger om at virksomheten bør ha en årlig rutine som sikrer at et gyldig samtykke er gitt.

Når det gjelder barnehage, fremkommer det av dokumentasjon og intervjuer at det innhentes samtykke til behandling av personopplysninger, som ikke er nødvendig for barnehagedriften kun ved oppstart i barnehagen. Det er vår vurdering at barnehagen også bør følge Datatilsynets anbefalinger om å ha en årlig rutine som sikrer at et gyldig samtykke er gitt.

2.1.2 Personers rettigheter

Revisjonskriterier

- Kommunen ivaretar retten til innsyn i personopplysningene (hvor de kommer fra, hvordan de behandles og en kopi av registrerte opplysninger).
- Kommunen informerer om rettighetene.
- Kommunen sørger for at personer får utført rettighetene gratis.
- Kommunen sikrer at den registrerte mottar personopplysninger om seg selv som vedkommende har gitt til kommunen, i et strukturert, alminnelig anvendt og maskinlesbart format.
- Kommunen begrunner avslag om innsyn skriftlig.
- Kommunen skal sørge for å overføre nevnte opplysninger til en annen behandlingsansvarlig når den registrerte ber om det og det er teknisk mulig (dataportabilitet).

Fakta

I kommunens personvernerklæring fremkommer det informasjon om retten til innsyn i egne personopplysninger. Det står også en beskrivelse av fremgangsmåten og retten til å få opplysninger rettet og eventuelt slettet. Det fremkommer at disse tjenestene er gratis.

Når noen ber om innsyn på servicetorget, ber servicetorget om informasjon om hva det konkret ønskes innsyn i. Dersom det er innsyn i egne personopplysninger videreformidles det til byarkivet. Servicetorget får daglig muntlige henvendelser om innsyn. De jobber med å få på plass en rutine for å kunne dokumentere hvem som har bedt om innsyn i saker.

I dokumentet *Innsynsbegjæring*, datert 25.06.2019 pkt. 7 er rutinene for ivaretakelse av innsynsretten i personopplysninger beskrevet. Det er byarkivet som skal motta og koordinere innsynsbegjæringer i personopplysninger. Det fremkommer også av dette dokumentet at avslag skal gis skriftlig og at det er saksbehandler i byarkivet som produserer svarbrevet med personopplysningene. Rutinen viser innledningsvis til blant annet lovhjemmel for innsynsbegjæringer. Det fremkommer at det er offentlighetsloven som er grunnlaget for innsyn. Nederst i rutinen vises det imidlertid til personopplysningsloven også.

Det kommer frem av intervjuene at innsyn i personopplysninger må være skriftlig, og at den som ber om innsyn må legitimere seg. Det gis imidlertid ikke informasjon til brukere om at innsynskrav i personopplysninger skal være skriftlig på kommunens nettsider. Det står at personer kan henvende seg til en hvilken som helst av kommunens virksomheter og be om å få vite hva slags opplysninger de har om personen, hva de skal brukes til, og hvor de er innhentet fra.

Ved krav om innsyn i personopplysninger sender arkivet en henvendelse til den som er eier av behandlingen av personopplysningene, enten superbrukere eller virksomhetsledere, hvor de ber om den informasjonen som er registrert om den enkelte personen. Det sendes i Elements[6]. Arkivet samordner opplysningene og sender det til brukeren i sikker digital post[7].

Arkivet opplyser at de ikke har mottatt så mange henvendelser om innsyn i personopplysninger hittil. De trodde det skulle bli mer enn det som har kommet. Arkivet stipulerer antall henvendelser til ca. 10 stk. totalt. I intervjuene blir det sagt at GDPR-innsyn er svært ressurskrevende. Arkivet sladder taushetsbelagt informasjon som ikke gjelder vedkommende som har begjært innsyn. Alle virksomheter i kommunen kan henvende seg til arkivet dersom de trenger hjelp i forbindelse med innsynsbegjæringer, både GDPR-innsyn og andre innsyn etter offentlighetsloven eller forvaltningsloven. Arkivet samarbeider med saksbehandlere og ledere ved krav om innsyn. Saksbehandler/leder må godkjenne dokumentet før det blir sendt ut. Alle krav om innsyn blir journalført, slik at de har en liste over alle innsynskrav.

Kommunen skal sørge for å overføre personopplysninger til en annen behandlingsansvarlig når den registrerte ber om det og det er teknisk mulig (dataportabilitet). Arkivet sier at de har koordineringsrollen dersom noen ønsker å oversende dokumentasjonen for eksempel til en annen kommune. Dataportabilitet skjer kun via sikker digital post, dersom det er arkivet som sørger for overføringen. Arkivet opplyser om at de ikke overfører data på noen annen måte.

I kommunens dokument *Mål personvern og informasjonssikkerhet*, datert 09.12.2019 står det at kommunens overordnede målsetting ved dataoverføring mellom ulike kommunale enheter, er å sikre nødvendig tilgjengelighet og rask saksbehandling. Målsettingen med dataoverføring til virksomheter utenfor kommunen er å ivareta effektiv samhandling med andre samfunnssektorer eller forvaltningsnivå.

[6] Kommunens arkivsystem
[7] Kommunen bruker SvarUt

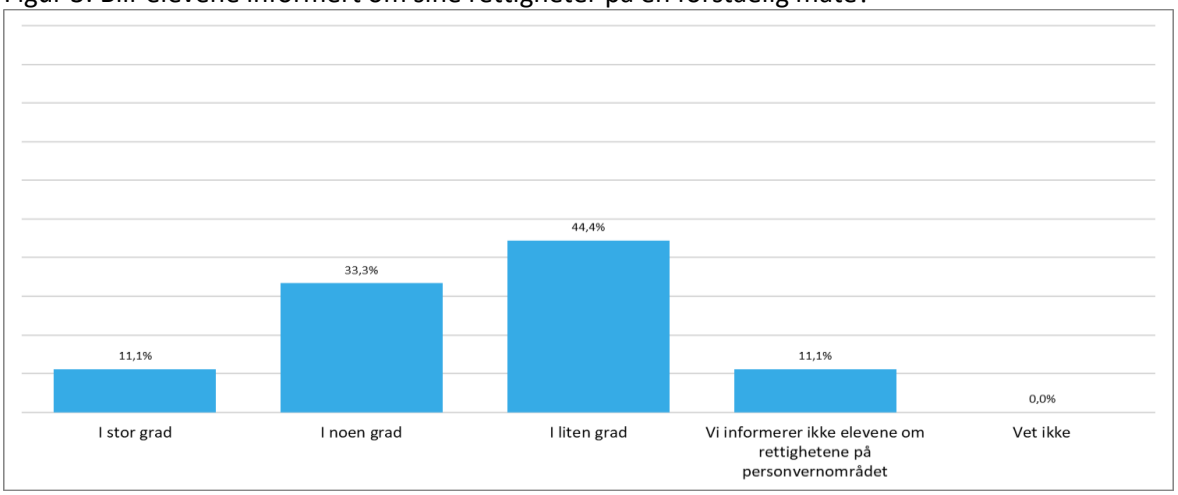
I intervjuene sier digitaliseringssjefen at dataportabilitet utøves i svært liten grad. Helsenett kan portere til legevakt e.l. Kommunen har ikke systemer som kan overføre data digitalt mellom kommuner eller til andre på dette området. Det er kun på helse dette er mulig.

I dokumentet *Saksbehandling i personalsaker som kan få arbeidsrettslige følger – arbeidstakers forhold,* datert 21.10.2019 blir det ikke informert om hva som er den ansattes rettigheter når det gjelder innsyn, retting, sletting eller lagring av personopplysninger. Det samme gjelder for *Retningslinjer for konflikthåndtering*, datert 02.09.2019. Retningslinjene viser til taushetsplikten når det gjelder behandling av særlig sensitive opplysninger, men det fremkommer ikke hva som er ansattes rettigheter når det gjelder behandlingen av disse opplysningene.

Kommunen har også en innsynsprosedyrene knyttet til e-post. Prosedyren er kun beregnet for innsyn i ansattes e-post og gjelder hvis en leder skal ha tilgang. Det er kun ved mistanke om ulovligheter og saklige tjenstlige behov at det kan gis innsyn i ansattes e-post.

I spørreundersøkelsen ble rektorer ved skoler med ungdomstrinn spurt om de informerer elevene om rettighetene på personvernområdet på en sånn måte at det er forståelig.

Figur 3: Blir elevene informert om sine rettigheter på en forståelig måte?



N=9

Av de 9 skolene med ungdomstrinn som var med i undersøkelsen svarer 5 av skolen at de i liten eller ingen grad informerer elevene om rettighetene på personvernområdet. 3 skolene svarer at de i noen grad informerer om rettighetene på personvernområdet og en skole sier at de i stor grad informerer om elevenes rettigheter.

Det fremkommer av intervjuene med ansatte i barnehagen at de i liten grad informerer om personers rettigheter til innsyn i egne/barnas personopplysninger.

Vurderinger

Det er vår vurdering at kommunen i stor grad informerer om personers rettigheter til å få vite hvilke personopplysninger som er registrert om den enkelte i kommunen. Opplysninger om dette fremkommer i personvernerklæringen. Kommunen har utarbeidet en rutine om personers rettigheter og det er vår vurdering at kommunen har implementert rutinen og ivaretar retten til innsyn i personopplysninger. På bakgrunn av intervjuene er det sannsynliggjort at den registrerte mottar informasjonen på et strukturert og lesbart format. Det er videre vår vurdering at når noen ber innsyn, får de utført denne rettigheten gratis. På bakgrunn av intervjuene er det sannsynliggjort at

kommunen begrunner eventuelle avslag skriftlig. Det er vår vurdering at det bør fremkomme tydeligere at rutinen for innsynsbegjæringer også omhandler innsyn i personopplysninger hjemlet i personopplysningsloven.

Det kommer frem av intervjuene at innsyn i personopplysninger må være skriftlig, og at den som ber om innsyn må legitimere seg. Det gis imidlertid ikke informasjon til brukere om dette på kommunens nettsider. Det er vår vurdering at kommunen med fordel kan tydeliggjøre fremgangsmåten på sine nettsider.

På bakgrunn av intervjuene det er vår vurdering at kommunen overfører opplysninger til en annen behandlingsansvarlig når den registrerte ber om det, og det er teknisk mulig.

2.2 Formålsbegrenset

Revisjonskriterier

- Kommunen sikrer at personopplysningene kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål og at opplysningene ikke viderebehandles utover formålet.
- Kommunen vurderer hvilke formål personopplysningene samles inn til.
- Kommunen vurderer om det valgte formålet er forenlig med det personopplysningene opprinnelig ble samlet inn til.
- Kommunen har kunnskap om personopplysninger benyttes til andre formål enn det de er samlet inn til.

Fakta

I spørreundersøkelsen med kommunens ledergruppe svarer 16 av 25 ledere at de har gjort en vurdering av om de har rettslig grunnlag til å behandle personopplysninger. 20 av 25 ledere svarer at det kun samles inn opplysninger som er relevante for formålet i virksomhetene/enhetene i deres seksjon. 5 av lederne sier at de ikke vet om det kun samles inn opplysninger som er relevante for formålet i deres virksomheter/enheter.

Det kommer frem av intervjuene at personvernombudet har gjennomført noen samlinger der løsningsansvarlige har blitt oppfordret til å vurdere formålet. Personvernombudet sier i intervjuet at det ikke er undersøkt hvorvidt de ansatte har forstått hva et formål er. Personvernombudet opplever at rollen som personvernombud har blitt litt borte fordi det har vært mer fokus på det systemtekniske enn personvernet. Det er i liten grad ført behandlinger i Risk Manager, hvor formålet med behandlingene også skal beskrives. I revisjonens gjennomgang av kommunens registreringer i Risk Manager 19.12.2019 blir dette bekreftet.

Det gjøres loggføringer i IT-systemene. Formålet med loggføringen er datasikkerhet. Det fremkommer av intervjuene at loggføringen slettes i henhold til regelverket, og dataene ikke brukes til annet enn formålet.

Det kommer frem av intervjuene at formålet med kameraovervåking er vurdert. I kommunens prosedyre *Kameraovervåking*, datert 17.12.2018 står det at formålet med kameraovervåking er å hindre hærverk, innbrudd og annen uautorisert tilgang til kommunens lokaler og utstyr. Videre står det at det kun gjelder på områder hvor det foreligger særlig risiko for denne typen kriminalitet. Det kommer frem av intervjuene at formålet med kameraovervåking på skoler eller barnehager er å forhindre og avdekke hærverk, og er kun satt opp der dette har vært et problem. Skolen og barnehagen som er intervjuet har ikke kameraovervåking.

Virksomheter – skole og barnehage

I oppstartsbrev til kommunen 29.11.2019, ba vi om dokumentasjon fra kommunen og de utvalgte virksomhetene. Vi ba da blant annet om informasjon om/rutiner for innhenting og registrering av personopplysninger om barna i barnehagen og elever i skolen, inkludert type opplysning (kategorier). I dokumentasjonen som er mottatt fra kommunen foreligger det en oversikt over hvilke personopplysninger som samles inn om elevene, fra en skole.

I oversendt dokumentasjon fra kommunen 9.12.2019 fremkommer det en oversikt over de formålene der skolen behandler personopplysninger.

- Innskrivning av elever – grunnlagsinformasjon og informasjon med krav om samtykke
- Flyttemelding/bytte av skole – grunnlagsinformasjon og informasjon med krav om samtykke
- Innskrivning til SFO – grunnlagsinformasjon og informasjon med krav om samtykke

Det fremkommer av intervjuene at skolen har gjort vurderinger av hva de henter inn av personopplysninger. De henter inn navn, personnummer, foreldres navn, bosted, sykdommer det er viktig å vite om, allergier og kontaktinformasjon til fastlege. De henter ikke aktivt inn opplysninger om for eksempel religion, men dette kan komme frem i samtaler med foreldrene, dersom det er nødvendig å ta hensyn til f.eks. mat.

I intervjuene med ansatte i barnehagen fremkommer det at det ikke er så mange personopplysninger barnehagen henter inn hvis det ikke er nødvendig. Når nye barn begynner i barnehagen får foreldrene et skjema hvor det skal fylles inn opplysninger ved oppstart i barnehage. Der fyller foreldrene ut barnets navn, barnets fødselsdato, tlf.nr, navn på foreldre eller andre kontaktpersoner, hvilken helsestasjon og fastlege barnet har. I skjemaet skal foreldrene også samtykke/ikke samtykke til fotografering, både i og utenfor barnehagen, kjøring i bil og bruk av svømmehall mm. Det er også et åpent felt der foreldre selv kan velge hva de vil informerer om. Som eksempel nevnes kronisk sykdom og allergier.

Barnehagen deler ikke lenger ut felles navnelister med tlf. og e-post til alle foreldrene. På et foreldremøte ble foreldrene enige om å heller opprette en felles Facebook-gruppe slik at de kan kommunisere der.

Det fremkommer i intervjuene at virksomhetslederne i barnehagene har diskutert bruk av helseskjema, bl.a. vaksiner. De er ikke ferdige med denne diskusjonen. Skjema ble ikke delt ut i barnehagen vi snakket med i år, da dette ennå ikke er vurdert på kommunalt nivå.

Ansatte i barnehagen sier at dersom barnehagen har behov for å snakke med f.eks. helsestasjon så gjør de det i samarbeid med foreldrene. Foreldrene krysser av for morsmål i skjema, men ikke religion. De spør muntlig foreldrene om det for eksempel er behov for bestemte typer mat. Dette noterer de ned og oppbevarer i barnas mappe/perm på avdelingen.

Dersom de ansatte gjør observasjoner av et barn, for eksempel ved bekymring, noteres dette ned og legges i et skap på avdelingen. Barnets navn «kodes», slik det ikke kan gjenkjennes av andre enn de ansatte. Er det bekymringer som er viktige å spare på så arkiveres det i Ephorte/Elements. Ansatte i barnehagen tar ikke front-bilder av barna, dette er for å beskytte dem.

Etter førstegangssamtalen med foreldrene utarbeider barnehagen et notat. I notatet fremkommer opplysninger om barnet og familiesituasjon. Foreldre godkjenner/gir samtykke til det barnehagen noterer. I intervjuene sier ansatte i barnehagen at de ikke samler inn informasjon som kun er «kjekt å

vite». De har nå redigert skjema for førstegangssamtalen. Her henter barnehagen inn viktig informasjon dersom barnet f.eks. har flyktet, da dette er en viktig kunnskap for barnehagen.

I spørreundersøkelsen sier 33 av 40 rektorer og styrere at de har vurdert hvilke personopplysninger de har behov for, mens 7 av 40 ikke har gjort en vurdering av dette. 32 av 40 skoler/barnehager at de har vurdert formålet med å hente inn ulike personopplysninger. 8 av 40 skoler/barnehager sier at de ikke har vurdert eller ikke vet om de har vurdert formålet med å innhente ulike personopplysninger om elever og foreldre.

37 av 40 skoler/barnehager sier at de kun henter inn personopplysninger som er direkte relevante for formålet, mens 3 skoler/barnehager sier at de også innhenter personopplysninger som er «kjekt å vite». En skole svarer at den logger elevenes internettbruk uten å informere foreldrene og elevene om det.

Vurderinger

Datatilsynet viser til at alle formål skal være forklart på en måte som gjør at alle berørte har samme forståelse av hva personopplysningene skal brukes til. At formålet skal være legitimt innebærer at det, i tillegg til å ha et rettslig grunnlag, også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer. Formålet må holde seg innenfor det som er lovlig. Datatilsynet sier i sin veileder at personopplysninger er mer enn navn, adresse, telefon osv. Beskrivelser av personer og registrering av adferdsmønster ol. er også regnet som personopplysninger. Personopplysninger kan ikke gjenbrukes til formål som er uforenelig med det opprinnelige formålet. Det er vår vurdering at de fleste av kommunens ledere og kommunens skoler og barnehager har tenkt gjennom formålet med innsamling av personopplysninger, og ser til at personopplysninger kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål. Kommunen har også vurdert formålet med kameraovervåkingen, der det er besluttet å montere kamera.

Et fåtall skoler sier at de også samler inn personopplysninger som ikke er direkte relevant for formålet. Samtidig viser undersøkelsen at 20 % av skolene og barnehagene ikke har vurdert eller ikke vet om de har vurdert formålet med å innhente ulike personopplysninger om elever og foreldre.

I dokumentasjonen som er mottatt fra kommunen foreligger det en oversikt over hvilke personopplysninger som samles inn om elevene, fra en skole. Det er vår vurdering at skoler innhenter flere typer personopplysninger, til flere formål enn det som fremkommer i oversikten fra skolen. Skoler henter for eksempel inn personopplysninger som for eksempel beskrivelse av elevene (og noen ganger foreldrene) fra utviklingssamtaler – hvor det kan være flere formål. Det hentes inn personopplysninger i forberedelsesfasen til eventuelle vedtak om spesialundervisning – hvor formålet er tilpasset opplæring[8], det hentes inn personopplysninger i skolemiljøsaker – hvor formålet er et trygt og godt skolemiljø[9] og så videre.

Det er også vår vurdering at barnehager på lik linje med skoler samler inn flere personopplysninger enn det som fremkommer i oversendt dokumentasjon. Barnehagene samler inn personopplysninger gjennom observasjoner av barna og samtaler med foreldrene – formålet kan være hjelp til barnets utvikling og læring[10] med mer.

[8] Opplæringsloven § 1-3
[9] Opplæringsloven kapittel 9 A
[10] Barnehageloven § 19 a

På bakgrunn av det overnevnte og intervjuene er det vår vurdering at kommunen ikke i tilstrekkelig grad har etablert en god nok kunnskap i organisasjonen om hva som er personopplysninger og knyttet dette opp mot et konkret formål.

Kommunen har ikke i tilstrekkelig grad gjennomført en systematisk vurdering av de ulike formålene som det samles inn personopplysninger til i kommunen. Det har vært drøftet, men det er vår vurdering at det ikke er en felles forståelse for hva formålene er i kommunen. Det er derfor også vanskelig for kommunen å vurdere om personopplysninger brukes til andre formål enn det opprinnelige formålet.

2.3 Dataminimering

Revisjonskriterier

- Kommunen gjør en vurdering av om de innsamlede opplysningene i hvert tilfelle er adekvate, relevante og begrenset til formålet.
- Kommunen har en oversikt over de ulike kategoriene personopplysninger som er registrert til ulike formål.
- Kommunen har vurdert om personopplysningene er nødvendig for å utøve lovpålagte oppgaver – utøve offentlig myndighet.
- Kommunen har vurdert når det er behov for behandling av særlige kategorier personopplysninger.

Fakta

Det kommer frem av intervjuene at dataminimering ikke har vært drøftet. Det kommer frem av kommunens personvernerklæring at kommunen sletter eller sperrer opplysninger som ikke lenger er nødvendige for formålet med registreringen, men at det ikke slettes dersom opplysningene skal oppbevares i henhold til annen lovgivning, for eksempel regnskapsloven og arkivloven.

I intervjuene kommer det frem at når ansatte har sluttet, blir personen anonymisert i systemene ved at vedkommende er registret med en id, i stedet for navn. Bruker-id slettes ikke, fordi den er unik for den enkelte og dersom det begynner andre ansatte med tilsvarende initialer, må de få en annen bruker-id.

Vurderinger

Datatilsynet sier i sin veiledning at prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet med behandlingen. Kravet til dataminimering henger også sammen med kravet til lagringsbegrensing, men også arkiveringsplikten og formålet med å oppbevare opplysningene. Arkiveringspliktig dokumentasjon skal uansett oppbevares etter gjeldende retningslinjer, det skal også opplysninger til historiske, vitenskapelige og statistiske formål. Det er imidlertid viktig å presisere at for personopplysninger som ikke kommer under kriteriene nevnt foran, må det gjøres en vurdering i det enkelte tilfelle.

Gjennom intervjuene er det sannsynliggjort at kommunen gjør vurderinger av om personopplysningene er nødvendig for å utøve offentlig myndighet og om det er behov for behandling av særlige kategorier personopplysninger. Det er vår vurdering at kommunen gjør en vurdering av om de innsamlede opplysningene i hvert tilfelle er adekvate, relevante og begrenset til formålet, der formålene er definert. Som nevnt tidligere er det imidlertid vår vurdering at kommunen ikke i tilstrekkelig grad har definert alle formålene, som det samles inn opplysninger til, slik at

kommunen heller ikke har oversikt over de ulike kategoriene personopplysninger som blir registret til ulike formål.

2.4 Riktighet

Revisjonskriterier

- Kommunen sikrer at personopplysningene er korrekte og om nødvendig oppdaterte.
- Kommunen ser til at personer får korrigert opplysningene dersom de ikke er korrekte – uten ugrunnet opphold.
- Kommunen ser til at personer som ber om at opplysninger om seg blir sperret eller slettet, uten ugrunnet opphold, får utført dette. Dette gjelder dersom opplysningene
    - ikke lenger er nødvendig for formålet
    - bygger på samtykke og personen trekker samtykke, forutsatt at opplysningene ikke er grunnlag for en behandling
    - har blitt behandlet ulovlig (innsigelse)

Fakta

Kommunen har en rutine for retting og sletting av personopplysninger, datert 17.12.2018. Rutinen angir at kommunen skal sørge for å ikke behandle personopplysninger som er uriktige. Det fremkommer videre at dersom enkeltmennesker henvender seg til virksomheten og ber om at opplysninger rettes eller slettes, skal virksomheten gjøre vurderinger av om opplysningene kan slettes og rettes. Dersom den opplysningen gjelder ønsker å slette opplysningene helt, eller at de sperres, kan en beslutning om retting/tilføying klages inn for Datatilsynet. Det fremkommer at det er virksomhetens leder som skal påse at dette blir gjort.

I kommunens personvernerklæring står det at de registrerte skal kunne kreve at feilaktige eller mangelfulle opplysninger om seg blir rettet. Videre står det at kommunen anbefaler at alle bruker innsynsretten aktivt, og gir beskjed til virksomheten det gjelder om det er registrert feil opplysninger. Kommunen jobber for at opplysningene skal være korrekte og oppdaterte til enhver tid. I personvernerklæringen står det også at kommunen sletter eller sperrer opplysninger som ikke lenger er nødvendige for formålet med registreringen. Opplysningene som skal oppbevares i henhold til annen lovgivning, for eksempel regnskapsloven og arkivloven, slettes ikke.

I intervjuene kommer det frem at Byarkivet får noen henvendelser vedr. retting/sletting av personopplysninger. De opplyser om at de vanligvis ikke kan slette opplysninger, men de kan rette opp feil i opplysningene. Det fremkommer et eksempel fra en varslingssak der opplysninger ble slettet. Før varslingssekretariatet hadde tatt tak i saken ønsket ikke varsleren å varsle likevel. Varslingen ble da kassert etter varslerens ønske.

Vurderinger

På bakgrunn av intervjuene er det vår vurdering at kommunen jobber for at personopplysningene som er samlet inn skal være korrekte og oppdaterte til enhver tid. Der det fremkommer at personopplysninger ikke er korrekte, ser kommunen til at personer får korrigert opplysningene.

På bakgrunn av intervjuene og informasjon til brukerne på kommunens nettsider under *Informasjonssikkerhet*, avsnittet om rett til innsyn, er det vår vurdering at kommunen ser til at personer som ber om at opplysninger om seg blir sperret eller slettet, får utført dette, dersom det ikke er et krav til oppbevaring i henhold til annen lovgivning.

2.5 Lagringsbegrensing

Revisjonskriterier

- Kommunen sikrer at personopplysningene lagres slik at det ikke er mulig å identifisere de registrerte lengere enn det som er nødvendig for formålet som personopplysningene behandles for.
- Kommunen sletter personopplysninger uten ugrunnet opphold dersom personopplysningene ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for.

Fakta

I kommunens rutine for retting og sletting av personopplysninger, datert 17.12.2018, fremkommer det at opplysninger som ikke lenger er nødvendig for å oppfylle formålet, skal slettes, med mindre de skal oppbevares i henhold til annen lovgiving, for eksempel arkivloven og helseregisterloven.

Det kommer frem av intervjuene at byarkivet jobber med et nytt «bevarings- og kassasjonsreglement». Første utkast skal være klart i mars/april og ferdigstilles til sommeren. Byarkivet opplyser at de ventet lenge på at det skulle komme en ny bevarings- og kassasjonsplan fra sentrale myndigheter. Da den kom for et par år siden, var den ikke så presis som de hadde ønsket. Det er noe som er tydelig at alltid skal arkiveres, men det er flere områder som omhandler hva som kan kasseres/arkiveres og som kommunen selv må ta stilling til. Det er det de jobber med nå.

Custom Relationship Managment (CRM) er et meldingssystem som blant annet servicetorget benytter til å nedtegne personopplysninger som skal videreformidles til andre virksomheter internt i kommunen. Informasjonen her blir lagret i 1 ½ år og er tilgjengelig for både servicetorget og fagavdelingene i denne perioden. Det blir rapportert på antall henvendelser i CRM, sortert etter KOSTRA-nr.

Det fremkommer i intervjuene at besøkende registreres på servicetorget. Disse opplysningene blir slettet hver kveld.

I intervjuene blir det sagt at det ikke er etablert en prosedyre for sletting av opplysninger som sendes med SMS/telefonen. I oversendt dokumentasjon foreligger det ikke rutiner for bruk av sms, når det gjelder lagring og sletting.

Det kommer frem av intervjuene at IT-avdelingen har to rutiner å følge når ansatte slutter. Når ansatte slutter slettes alt av dokumenter og e-poster, som de har lagret på sitt område. I etterkant finnes ansatte anonymisert som en id i systemet. Bruker-id slettes ikke, fordi den er unik for den enkelte og dersom det begynner andre ansatte med tilsvarende initialer, må de få en annen bruker-id.

Når det gjelder lagringsbegrensing av personopplysninger om ansatte i kommunen, kommer det frem av intervjuene at personalsaker som blir til disiplinærsaker lagres. For eksempel dersom en ansatt stjeler fra en bruker. Opplysningene lagres så lenge den ansatte er tilsatt. Det er byarkivet som vurderer hva som kan slettes eller ikke slettes i personalmapper. I undersøkelsesfasen, før en

personalsak eventuelt blir en disiplinærsak, lagres også informasjonen. Avsluttes saken uten at det blir en disiplinærsak, slettes personopplysningene. HR har nylig endret rutinene som omhandler vanskelige personalsaker, da den gamle ikke var helt oppdatert. Taushetsplikt er med i denne rutinen.

Det kommer frem av intervjuene at kommunen har hatt mange diskusjoner om lagring og oppbevaring av personopplysninger. Et eksempel er personopplysninger knyttet til saker jf. opplæringsloven kap 9 A-5[11]. Det er en utfordring for HR og ledere å vurdere hvor langt en skolemiljøsak etter opplæringsloven § 9 A-5 kan gå uten at læreres rettigheter også blir ivaretatt.

Det kommer frem av intervjuene med ansatte i skolen at når elever bytter skole eller har fullført løpet på skolen, skal personopplysninger som ikke lenger er nødvendig, slettes. Det er imidlertid en del personopplysninger som er arkivpliktig. Noen lærere oppbevarer opplysninger om elever i papir på sitt kontor. Noe av dette kan også være sensitivt. Det kommer frem i intervjuene at slik dokumentasjon etterspørres av og til i ettertid, blant annet knyttet til rettsaker. Skolen har fått beskjed om at dette ikke skal lagres i Ephorte/Elements, men sier at ett sted må det oppbevares. Dokumentene er blant annet notarer fra samtaler hvor foreldrene har undertegnet.

Det fremkommer av intervjuene at for eksempel anmerkninger for elever i skolene, som ikke fører til nedsatt karakter skal kasseres/slettes.

Det kommer frem av intervjuet med ansatte i barnehagen at når et barn slutter i barnehagen eller begynner på skole, blir informasjon som ikke ligger i elektronisk mappe makulert. Skademelding må f.eks. spares på, men denne ligger i elektronisk mappe. Notater fra for eksempel samtaler med foreldre og barnevern blir lagret i Ephorte/Elements. Bilder og skjemaene til foreldresamtaler slettes når barnet slutter.

I intervjuene utrykker barnehagens ansatte at de kunne tenkt seg at noen kom og hjalp dem med å rydde i det de har av gamle dokumenter ol. De er usikre på om det kan ligge opplysninger der som ikke burde ligge der i papir. De vil også gjerne få et svar på hvor lenge ting skal lagres og hva er det ok at lagres på papir i et skap.

Vurderinger

Datatilsynet sier i sin veiledning at hvor lenge det er lov å lagre opplysninger er avhengig av hva som er formålet med at opplysningene ble registrert, og om de er arkivpliktige. Arkivpliktige opplysninger blir lagret på ubestemt tid i kommunen arkiv. Personopplysninger som ikke er arkivpliktige skal slettes når formålet med at de ble lagret er oppfylt. Det er vår vurdering at kommunen på mange områder gjør vurderinger av hvilke personopplysninger som skal lagres. Det fremkommer imidlertid at enkelte personopplysninger lagres lenger enn det som er det opprinnelige behovet for formålet, for eksempel for noen elever i skolene og barn i barnehagene. Det er da viktig at kommunen gjør en ny vurdering av formålet med behandlingen, da formålet har endret seg fra det opprinnelige.

Kommunen arbeidet med nytt bevarings- og kassasjonsreglement. Som våre funn viser er det behov for å vurdere hva som skal lagres og hva som skal kasseres av personopplysninger også ute i virksomhetene. Det kan være hensiktsmessig om det er en sammenheng mellom bevarings- og kassasjonsplanen og det som blir beskrevet i protokollen angående når personopplysninger skal slettes. Etter revisjonens vurdering kan det også være hensiktsmessig å vurdere andre reglementer og rutiner i sammenheng med personvernregelverket, eksempelvis innenfor HR- området.

[11] Skjerpet aktivitetsplikt dersom en som arbeider på skolen, krenker en elev.

Kommunen bør også gjøre en vurdering av om personopplysninger allikevel skal lagres, men da knyttet til et annet formål enn det som det opprinnelig ble samlet inn for. Dette kan eksempelvis være aktuelt i elevsaker eller personalsaker hvor det kan oppstå en rettssak/søksmål i ettertid. I slike tilfeller kan kommunen ha en berettiget interesse i å oppbevare dokumentasjonen frem til alle søksmålsfrister er utløpt, men da er imidlertid formålet med behandlingen et annet enn det opprinnelige formålet. Formålet med oppbevaring av personopplysningene må da endres.

2.6 Integritet og konfidensialitet

Revisjonskriterier

- Kommunen sikrer at personopplysningene behandles på en måte som gir tilstrekkelig sikkerhet for personopplysningene.
- Kommunen gjør en vurdering av hvilke ansatte som skal ha autorisert tilgang til hvilke personopplysninger. Personopplysningene skal være kryptert for ansatte som ikke har autorisert tilgang.
- Kommunen gjennomfører egnede tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering.
- Kommunen iverksetter egnede tekniske og organisatoriske tiltak både når det blir bestemt hvilke midler som skal brukes til behandling av personopplysninger og ved selve behandlingen av personopplysningene.
- Kommunen iverksetter egnede retningslinjer for vern av personopplysninger.

Fakta

Administrativt nivå

I kommunens rutine *Låserutiner og adgangskontroll*, datert 17.12.2018 beskrives det hvordan tilgangen til personopplysninger skal avgrenses og sikres. Den omhandler både hvordan områder der det behandles personopplysninger skal fysisk sikres og hvordan tilgang skal avgrenses i systemene. Kommunen har også en rutine *Adgang til utstyr*, datert 17.12.2018. Denne rutinen omhandler sikring av tilgang til utstyr som benyttes ved behandling av sensitive personopplysninger.

Det kommer frem av intervjuene at ansatte på IT-avdelingen har mange tilganger til ulike systemer, men også at de er gradert etter hva den enkelte ansatte har som oppgaveområde. Det er en hierarkisk tilgang innenfor avdelingen. Det er kun 3 ansatte med administratortilgang (domene).

Det kommer frem i intervjuene og ved observasjoner at publikums-pc er plasser litt åpent på servicetorget. Den er plassert slik at andre kan se skjermen. Det kommer frem i intervjuene at kommunen mangler et rom hvor man kan sitte alene dersom noen har behov for det. Når det gjelder ansattes PC, kommer det frem av intervjuene at det ikke er mulig for utenforstående å kunne se inn på PC'ene i skranken på servicetorget og det blir heller ikke behandlet sensitiv informasjon på PC i skranken. Servicetorget har en egen printer i lukket rom.

Noen av kommunens brukere oppgir sensitiv informasjon muntlig til servicetorget. Det kommer frem av intervjuene at det kan være vanskelig å stoppe personer som møter opp på servicetorget, fra å snakke om sensitiv informasjon høyt slik at andre som er tilstede ikke skal høre det.

Det kommer frem av intervjuene at når servicetorget mottar sensitive personopplysninger på e-post eller i de ulike meldingssystemene, printer de ut informasjonen og sender det til aktuell fagavdeling i lukket konvolutt. Deretter sletter de personopplysningen i meldingssystemet.

Det kommer frem av intervjuene at flere virksomheter bruker sms, chat, e-poster o.l. i kommunikasjonen med brukerne, for eksempel skoler og barnehager. Skolen har arkiverer sms/loggføringer. Skolene i kommunen er i ferd med å gå over til et nytt system for denne typen sendinger, men er ikke helt i mål ennå. Per i dag brukes både det nye systemet og det vanlige e-post systemet parallelt. I oversendt dokumentasjon foreligger det ikke rutiner for hva som kan sendes av personopplysninger på sms eller hvordan disse personopplysningene skal behandles.

Kommunen har rutiner for sending av e-poster, som angir at det blant annet ikke skal være personopplysninger i e-poster. I dokumentet Retningslinjer for personvern og informasjonssikkerhet, datert 04.04.2019 står det «*Personopplysninger skal ikke sendes over e-post…….. Alle som mottar e-post som inneholder konfidensiell/personsensitiv informasjon, er ansvarlig for å gjøre avsender oppmerksom på at kommunen ikke kan svare på e-post av denne type. Som medarbeider er du pliktig til å henvise til å ta kontakt på tradisjonelt vis (telefon, brev, personlig oppmøte).»* Det fremkommer i rutinene for e-post at dokumenter som er unntatt offentligheten bør en unngå å sende som e-post, men dersom de likevel må sendes eksterne på e-post, så må de krypteres.

I dokumentet *E-post,* datert 09.12.2019 står det «*Alle som mottar e-post som inneholder konfidensiell / personsensitiv informasjon, er ansvarlig for å gjøre avsender oppmerksom på at kommunen ikke kan svare på e-post av denne type. En plikter da å henvise til å ta kontakt på tradisjonelt vis (telefon, brev, personlig oppmøte).»* Dokumentet nevner ikke at de sensitive personopplysningene må slettes før det sendes svar ut, eller at den mottatte e-post skal slettes.

I dokumentet *Facebook og andre sosiale medier*, datert 13.08.2019 står det *«Meldinger på Facebook og andre sosiale medier skal behandles som alle annen inn- og utgående post hos virksomheten, og skal journalføres hvis de er gjenstand for saksbehandling og har verdi som dokumentasjon. Det er innholdet som bestemmer om kommunikasjonen skal journalføres og arkiveres, ikke mediets utforming, format eller tekniske spesifikasjoner.»*

I intervjuene blir det sagt at det har blitt mye omtaler av Vigilo og svakhetene i dette systemet i media, men at dette også ville kunne skjedd i andre tilsvarende systemene som benyttes i skolene i andre kommuner. I oktober 2019 oppdaget kommunen en feil med meldingstjenesten Vigilo, der en meldingsutveksling om et barns fravær ble delt med flere enn barnets foresatte. Samtidig med at kommunen oppdaget dette avviket knyttet til personopplysninger og Vigilo, var det en hendelse i Bergen knyttet til det samme systemet. Etter hendelsen i Bergen har Folkeregisteret sendt ut et brev om at de ikke lenger tar ansvaret for «overføring» av data når det gjelder hvilke foreldre som har omsorg for barn, og rett til opplysninger om barnet eller informasjon om foreldre som ikke skal ha informasjon om barnet. Ansvaret er nå lagt til kommunene. Det er en stor og uoversiktlig oppgave for kommunene. På barnevernområdet har de også utfordringer med et tungt og gammeldags system (Familia). Om ikke lenge kommer det imidlertid et nytt system på barnevernområdet (Digi-barnevern). Virksomheten må nå selv sørge for å innhente opplysninger for å sikre at foreldre eller andre som ikke skal ha informasjon om barnet, ikke får det.

Når det gjelder sikker behandling av personopplysninger knyttet til ulike skjemaer på kommunens nettsider, er mange av disse elektroniske og sikret med to-trinns verifisering. Det finnes imidlertid flere skjemaer der som er i pdf-format, noen av disse har åpne felt. Det kommer frem i intervjuene at de som bruker skjemaene mange ganger legger inn personsensitive opplysninger i disse feltene.

Kommunen har en rutine *Taushetsplikt*, datert 09.12.2019. Under punktet *Referanser* står det *«Alle som behandler personopplysninger er også underlagt krav til taushetsplikt etter personopplysningsforskriften § 2-9 Taushetsplikt: "Medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten*

skal også omfatte annen informasjon med betydning for informasjonssikkerheten."» Denne forskriften ble opphevet da ny personvernlovgivning og GDPR trådte i kraft.

Kommunen har lagt til rette for muligheten til å arbeide utenfor kommunens lokaler. Når det gjelder bruk av bærbar PC og arbeid utenfor kontoret så sies det i intervjuene at kommunen har en egen klient som gjør at hver enkelt ansatt får passord tilsendt på mobiltelefon. PC'ene går i hvilemodus relativt fort.

Det kommer frem av intervjuene at varslingssaker internt i kommunen blir lagret i Ephorte/Elements avgrenset med en egen kode i arkivsystemet. Det er kun et lite antall personer som har tilgang til disse sakene fordi så få som mulig skal ha den informasjonen. Det er tilsvarende kode i AKAN[12]-saker. Det er etablert et eget team som følger opp vanskelige personalsaker og det er dette teamet som blant annet bistår i AKAN-saker.

Det kommer frem av intervjuene at HR-avdelingen ikke gir innsyn i personalmapper, til for eksempel ledere. Det er byarkivet som håndterer innsyn og tilgangsbegrensning i personalmapper.

I intervjuene fremkommer det at av og til blir det sendt sensitive personopplysninger per e-post til HR. HR tar kontakt med de saksbehandlerne/lederne eller andre som eventuelt sender sensitive opplysninger via e-post. De informerer da om at sensitive opplysninger ikke skal sendes på e-post. Det har blitt en større bevissthet rundt dette i kommunen. Kommunen har ikke en rutine på at man ikke skal svare direkte på e-poster med sensitive opplysninger, men de har snakket mye om det.

<u>Virksomheter – skole og barnehage</u>
Det kommer frem i redegjørelse fra administrativt nivå 9.12.2019 at alt av personopplysninger skal lagres forsvarlig i Vigilo og Elements/Ephorte. Alle møtereferater (med ledelsen), sakkyndige vurderinger, rapporter til BUPP o.l. lagres i Elements/Ephorte. Dersom lærer skriver dette selv blir det lagt på minnepinne og gitt til rektor. Rektor lagrer i Elements. Deretter blir filen slettet fra minnepinnen. Kontaktbøker/møtebøker fra kontaktsamtaler lagres på lærerens hjemmeområde digitalt, og kun med elevens initialer. Logg skrives på papir og oppbevares i skuffer på kontoret til den enkelte lærer. Eldre kontaktbøker/møtebøker som kun er skrevet på papir oppbevares også på kontoret til den enkelte lærer.

Det fremkommer av intervjuene med ansatte på skolen at det å arkivere dokumenter med personopplysninger er en utfordring. Lærerne har kun lesetilgang i Ephorte/Elements. Skolen ønsker å lagre det som er sensitivt i arkivsystemet. Hvis en lærer har utarbeidet en IOP, så har ikke vedkommende skrivetilgang til arkivsystemet. For å få IOPen inn i arkivsystemet, lagres den midlertidig på en minnepinne, som umiddelbart gis til merkantil ansatt, som lagrer IOPen i arkivsystemet fra minnepinnen.

Det kommer frem av intervjuene at det i første rekke er hver enkelt skole som skal sørge for at det er riktige opplysninger i Vigilo. De har laget en rutine for barn på hemmelig adresse. Dersom de får henvendelse om å stenge tilgangen for en forelder, kan de stenge tilgangen midlertidig i 4 uker, men så må den enkelte forelder dokumentere at det faktisk stemmer at adressen er hemmelig. De har hatt møte med Kripos og barnevern om dette. En sentral person i administrasjonen ordner dette (løsningsansvarlig for Vigilo) da dette er for sensitivt til å overlate til den enkelte skole.

[12] AKAN - Arbeidslivets kompetansesenter for rus- og avhengighetsproblematikk, tidligere Arbeidslivets komité mot alkoholisme og narkomani. Arbeideidet med å forebygge og håndtere rus- og avhengighetsproblematikk.

I spørreundersøkelsen kommer det frem at 40 % av skolene og barnehagene også har egne papirarkiv som inneholder opplysninger om barn/elever.

Det kommer frem av intervjuene at ansatte i skolen opplever at det er utfordringer med personvern på skoleområdet. De har diskutert hva som er «need too know» og «nice too know». De opplever at ansatte har både respekt og forståelse for personvernet, men at arbeidsflyten i arbeidsdagen er en utfordring sett opp mot dette. Det er også en utfordring å til enhver tid å vurdere hvem som trenger hvilke opplysninger i skolen, for eksempel hva en assistent må vite sett i forhold til en lærer eller hva en kontaktlærer må vite i forhold til en faglærer.

Det oppleves som utfordrende få lagret for eksempel notater fra foreldresamtaler på en trygg måte. Skolen kan ikke selv scanne inn i Ephorte/Elements, det må byarkivet gjøre. Skolen opplyser om at de har fått en forståelse av at det kan lagres mindre i Elements enn det lærerne har behov for. I møte med kommuneledelsen har de ikke kommet frem til noen konkrete praktiske løsninger per dags dato. De ansatte på skolen mener at skolene trenger hjelp til å få tilgang på et system der de kan lagre disse dokumentene på en trygg og tilgjengelig måte.

Skolen har oversendt en oversikt over hvilke digitale plattformer som benyttes pr. desember 2019.

Skoleadministrasjon	
Vigilo (nytt 2019)	Skoleadministrativt system for informasjon om elever, foresatte, elevgrupper, timeplaner, dokumentasjon av fravær for elever m.m. Skoleadministrativt system for informasjon om personalet, arbeidstidsavtaler, timeplaner, dokumentasjon av fravær for personalet m.m.
Extens (utgår 2019)	Skoleadministrativt system for informasjon om elever, foresatte, elevgrupper m.m.
Visma	Skoleadministrativt system for håndtering av personal og økonomi. Informasjon om personalet, lønnsmeldinger, personalmeldinger, fravær m.m.
Teams	For lagring og deling av informasjon og dokumenter.
ShareIT	For lagring og deling av informasjon og dokumenter.
PAS/UBAS	Administrativt system i regi av utdanningsdirektoratet for registrering, lagring og oppfølging av informasjon om elever (nasjonale prøver, elevundersøkelsen m.m.)
Engage	Digitalt system for lagring og oppbevaring av informasjon om elevenes skolefaglige utvikling (kartleggingsprøver, nasjonale prøver, språktester m.m.)
Insight	Digitalt system for lagring og oppbevaring av informasjon om skolemiljø (for eksempel elevundersøkelsen) m.m. Et digitalt system for systematisk kvalitetsarbeid.
Spekter	Et ikke-anonymt verktøy for lærere, som brukes til å avdekke mobbing og kartlegge læringsmiljøet i en skoleklasse.
Arkiv	
Elements (nytt 219)	Digitalt system for saksbehandling og arkiv
Ephorte (utgår 2019)	Digitalt system for saksbehandling og arkiv

Digitale plattformer for elevene	
Office 365	Digital læringsplattform for elevenes skolefaglig arbeid. Arbeid med og lagring av ulike dokumenter som Word, Excel, OneNote m.m.
Skooler	Digital læringsplattform for lagring og deling av elevenes skolefaglig arbeid. Deling i denne sammenhengen mellom lærer, elev og foresatte. Dokumentasjon av elevenes fravær.

Det kommer frem i intervjuene med administrativt nivå og skolen at skolene ikke lenger gjennomfører ikke-anonyme kartlegginger i Spekter. Skolen har blitt informert om at Spekter ikke kan brukes på grunn av personvernet til elevene.

På Datatilsynets nettsider fremkommer det at tilsynet har behandlet en klage på bruk av verktøyet Spekter i en kommune. Datatilsynet har konkludert med at behandlingen av personopplysninger i Spekter er i strid med personvernforordningen. Datatilsynet mener det mangler rettslig grunnlag og at bruk av systemet blant annet bryter grunnleggende prinsipper for vern av personopplysninger og informasjonssikkerhet.

Det kommer frem av intervjuene at lærerne må finne andre steder å lagre dokumenter med personopplysninger. De lagrer derfor notater fra foreldresamtaler i skyen. Lærerne sier i intervjuene at de stoler på at det kommunen oppgir som trygge lagringssteder er trygt å bruke. Det er også viktig for lærerne at de har lett tilgang til de opplysningene de trenger i arbeidet med elevene.

Det kommer frem av intervjuene at lærerne har møtebøker for kontaktsamtaler/utviklingssamtaler og at dette er et viktig arbeidsdokument for dem. Lærerne bruker initialer for å identifisere elevene og noen lærere bruker navn på eleven, fordi de har for mange elever til at initialer er praktisk å bruke. Dokumentene skal lagres på hjemmeområdet med passordbeskyttelse. Utfordringen kan være at skolen sannsynligvis ikke får tilgang til dokumentene dersom en lærer slutter.

Noen lærere kan oppbevare opplysninger i papir på sitt kontor. Noe av dette kan være sensitivt. Slik dokumentasjon etterspørres av og til i ettertid, blant annet knyttet til rettsaker. De har fått beskjed om at dette ikke skal lagres i Ephorte/Elements, men ett sted må det oppbevares. Dokumentene er blant annet notarer fra samtaler hvor foreldrene har undertegnet.

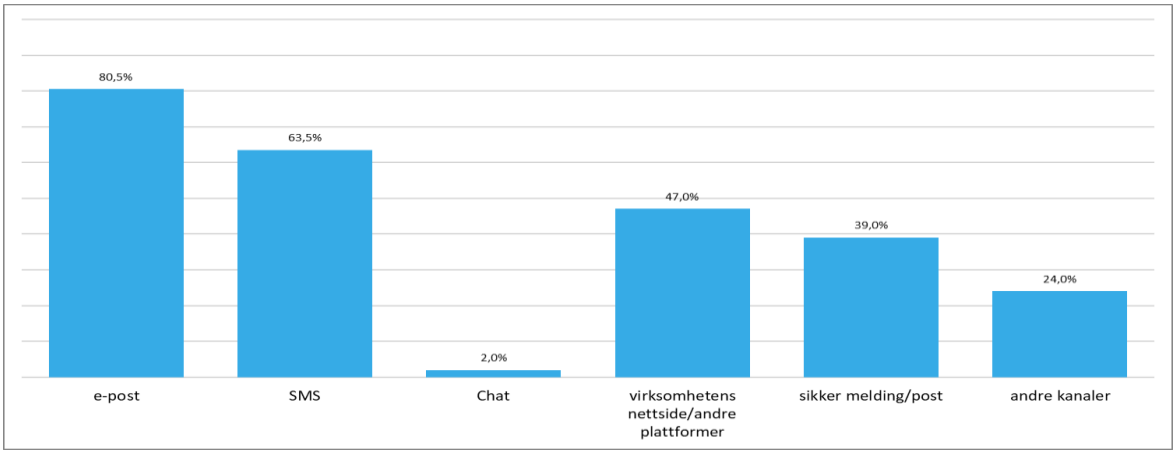
På skolen har lærerne også et elevopplysningsskjema. Det er et dokument med viktige opplysninger om eleven for eksempel kontaktinformasjon, fastlege mm. Lærerne har tidligere fått beskjed om at dette skulle ligge ved telefonen på lærernes kontor og det gjør det fortsatt. Det er viktig at slik informasjon er tilgjengelig dersom det skulle skje noe med en elev og kontaktlærer ikke er tilstede. Kontorene til lærerne er ikke låst, men inngangen til lærerkontorene er låst. Lærerne sier i intervjuene at de synes det er en utfordring å finne ut hvor de kan lagre dokumenter med personopplysninger. Dette er viktig informasjon å ta vare på. De må kunne hente ut denne informasjonen, da dette er opplysninger som de bruker til barnet beste. Lærerne sier at de trenger å få flyt i arbeidshverdagen – alt fra elevskjema til kontaktbøkene er informasjon de må ha tilgjengelig.

I redegjørelse fra administrativt nivå 9.12.2019 kommer det frem at «*Alle foreldre/foresatte i en klasse får kontaktinformasjon om de andre elevenesforeldre/foresatte (adresse og telefonnummer) ved skolestart. Dersom noen svarer negativt på dette i innskrivningsskjema blir vedkommende foreldre/foresatte fjernet fra listene (eventuelt deler av informasjonen blir delt etter samtykke fra de aktuelle foreldre/foresatte).*» Det kommer frem av intervjuene med ansatte på skolen at skolen ikke gir ut elevlister til foreldrene.

Det kommer frem av intervjuene at lærere kommuniserer med foreldre på ulike måter; e-post, sms og telefon er vanlig. Skolene har fått konkrete beskjeder/føringer fra kommunalt nivå på at man skal være restriktiv med bruk av e-post (jf. sensitive opplysninger), men utfordringen er at de i mindre grad opplever å få hjelp til alternative kommunikasjonskanaler. De har også nylig fått Vigilo og de ansatte sier at her trenger foreldrene litt opplæring, så ikke de sender så mye sensitivt i dette systemet. Fravær og kommunikasjon mellom skole og hjem registreres i Vigilo. De mener imidlertid at de trenger et halvt til ett år til for at de skal bli godt nok kjent med verktøyet.

I spørreundersøkelsen ble ansatte og ledere i skoler og barnehager spurt hvordan de kommuniserer med foreldre og elever.

Figur 4: Hvordan kommuniseres det med foreldre og elever?



N=200

80 % kommuniserer på e-post og 63,5 % bruker sms. 34 % av ansatte i skoler og barnehager sier at de ikke har prosedyre for lagring og sletting av personopplysninger fra disse kanalene, mens 38 % sier at de ikke vet om det er prosedyrer for det. 28 % sier at de har prosedyre for lagring og sletting av personopplysninger fra disse kanalene.

Det kommer frem av intervjuene at skolene bruker et verktøy for kartlegginger av faglige vurderinger. *Kartleggeren* brukes i norsk, engelsk og matte fra 5.-10. klasse. Her er opplysningene sikret gjennom innlogging via Feide[13]. Dokumenter og personinformasjon knyttet til spesialundervisning er lagret i arkivsystemet Ephorte/Elements.

I intervjuene sier ansatte at det også kan tilflyte personopplysninger på en måte som kan gjøre det utfordrende å håndtere for de ansatte. De opplever at noen foreldre kan snakke om sensitive personopplysninger på foreldremøte, i butikken etc. I disse tilfellene gir lærer beskjed om at dette kan de snakke om på et annet tidspunkt. De informerer om at de aktivt jobber med å avverge at foreldre gir sensitive personopplysninger foran egne eller andres barn eller foreldre.

I følgebrev fra Seksjon utdanning og oppvekst, 9.12.2019 fremkommer det at barnehagene i kommunen bruker Ephorte/Elements arkivsystem, Vigilo opptak datasystem og GAT oppmøtesystem.

I intervjuene med ansatte i barnehagen fremkommer det at det ikke sendes ut sensitive opplysninger i Vigilo. På spørsmål om hva som er utfordrende med personvern blir det sagt at de har hatt diskusjoner i virksomhetsledergruppa om hva de skal lagre av dokumenter i arkivet. De har henvendt seg til kommunens ledelse, men har ikke fått avklaringer. De er usikre på om for eksempel notater fra

[13] Feide er et system for sikker innlogging til en rekke digitale tjenester

foreldresamtaler kan lagres i Ephorte/Elements. Noen barnehager lagrer dette i arkivsystemet, mens andre barnehager ikke gjør det. De opplever at de ikke får et tydelig svar på hva de skal gjøre med disse dokumentene for å sikre trygg lagring.

Det kommer frem av intervjuene med ansatte i barnehagen at de ikke har snakket med foreldre om hva de kan sende til barnehagen via Vigilo. Foreldrene fikk noen informasjonsbrosjyrer ved oppstart av Vigilo. I Vigilio velger personalet sin avdeling og har fått beskjed om at det ikke er lov å se andres avdelinger.

Gjennom intervjuene kommer det frem at barnehagen utarbeider bursdagslister for barna. Barnehagen har valgt å beholde denne listen frem til noen foreldre eventuelt uttrykker at de ikke ønsker den. Barnehagen gir ikke ut e-postadresser eller tlf til andre foreldre.

I redegjørelsen fra kommunen, datert 9.12.2019 står det at «*Rutiner for arkivering og lagring av opplysninger om barna, inkludert dokumenter knyttet til observasjoner av barna, lagres alt dette i barnas mapper på ePhorte*.» I intervjuene med ansatte i barnehagen blir det bekreftet at alle barn i barnehagen har mapper. Barnehagen sender kopi av innmeldingsskjema til byarkivet som oppretter mapper på barna i Elements/Ephorte. Styrerassistenten har tilgang til nesten alle mapper i Elements/Ephorte. Noen pedagogiske ledere har hatt opplæring i Ephorte/Elements. Den enkelte pedagogiske leder får kun tilgang til de barna som er på sin avdeling. Spesialundervisningsvedtak, søknader og lignende legges i mappen til barnet i Ephorte/Elements. Pedagogiske ledere får stort sett informasjon om barnet fra styrer og styrerassistent.

Det kommer frem av intervjuene med ansatte i barnehagen at det lages notater fra førstegangssamtalene med foreldrene. Notatene blir lagt i barnets perm, som de har stående inne på avdelingen i et skap. Denne blir ikke registrert i Elements/Ephorte.

Noen av pedagogene har en egen bok hvor barnets navn er «kodet». Pedagogene opplyser at de må gjøre observasjoner av barna og dette nedtegnes i en bok som for eksempel kan ligge på avdelingen. Det er litt ulik praksis i hver avdeling på dette området. Dersom det ikke har blitt til en sak, så skal det ikke i Ephorte/Elements. Det henger en plan på avdelingen for et enkelt barn med spesielle behov, men her står det ikke noe navn eller fødselsnr. på barnet. Tidligere var informasjon om bleieskift tilgjengelig for alle på en tavle, men nå er denne informasjonen skjult for foreldre. Noen avdelinger har denne på badet. Det er kvalitetssikring for dem å ha en liste så de vet hvem de har skiftet på. Nå informerer de foreldre om dette muntlig.

Avvik/brudd på personvernregelverket

Det kommer frem av intervjuene at dersom det er en hendelse/avvik knyttet til personopplysninger, så gjør de internt i kommunen en felles innsats for å rette opp dette. IT-avdelingen er gjerne involvert, gjennom for eksempel testing og stenging av systemer o.l., men ansvaret ligger hos kommunaldirektørene når det gjelder iverksetting av tiltak for å rette avviket.

I intervjuene med ansatte kommer det frem at alle kjenner til avvikssystemet. Det er imidlertid få som har meldt avvik på personvernregelverket. De synes ikke det er så klart når de skal melde avvik på dette området.

Vurderinger

Administrativt nivå

Kommunen har utarbeidet rutiner, som sier at systemer som behandler personopplysninger skal fysisk sikres og tilgang skal være avgrenset. På bakgrunn av dette og informasjon om praksis fra

intervjuene, er det er vår vurdering at kommunen sørger for å avgrense tilgangen til ulike personopplysninger i sine systemer.

Servicetorget mottar mange henvendelser fra brukere. På bakgrunn av det som fremkommer i intervjuer, dokumentasjon og observasjoner er det vår vurdering at personopplysninger behandles på en trygg måte. Ansatte på servicetorget behandler personopplysninger på en måte som sikrer at opplysningene ikke er tilgjengelig for innsyn fra utenforstående. Kommunen bør imidlertid vurdere tiltak for å sikre at brukere på publikums-PC'en ikke risikerer at andre personer ser eventuelle personopplysninger som de registrerer.

Kommunen har rutiner for bruk av e-post og at personopplysninger ikke skal sendes med e-post. Det er vår vurdering at det av og til, fremdeles sendes personopplysninger på e-post. Når dette oppdages er det rutine for å melde avvik. Den som oppdager avviket melder også tilbake til den enkelte saksbehandler om dette. Det fremkommer av rutinen at alle som mottar e-post som inneholder konfidensiell/personsensitiv informasjon, skal sørge for å gjøre avsender oppmerksom på at kommunen ikke kan svare på e-post av denne type. Det er viktig at kommunen da også sørger for at dersom ansatte i kommunen informerer om dette ved å svare på den innkomne e-posten, må de sørge for å slette de innkomne personopplysningene slik at de ikke sendes ut fra kommunen også.

Det er vår vurdering at kommunen bør kartlegge på hvilke områder i virksomhetene det benyttes sms, chat eller liknende som kommunikasjonskanal med brukerne av kommunens tjenester. De ulike måtene å kommunisere på må ha et behandlingsgrunnlag etter GDPR. Hvilke data som kan sendes og mottas bør dokumenteres og danne grunnlag for beslutninger. I dette må også kommunen gjøre en vurdering av lagring og sletting av personopplysninger som eventuelt er behandlet i disse kanalene.

Flere av kommunens rutiner, som skal ivareta konfidensialitet er ikke knyttet opp mot personvernregelverket, eksempelvis rutinen *Taushetsplikt*, datert 09.12.2019 og rutine for journalføring og arkivering av kommunikasjon på Facebook og andre sosiale medier. Etter revisjonens oppfatning kan det være hensiktsmessig å vurdere om det bør være en kobling mellom kommunens ulike rutiner og personvernregelverket.

Det er vår vurdering at kommunen må sørge for at personvernet blir ivaretatt for søknad om ulike kommunale tjenester og støtte/tilskudd, som for eksempel er i pdf format. Intervjuene viser at brukere ofte legger inn personsensitive opplysninger i de skjemaene som har åpne felt. Det er vår vurdering at kommunen ikke bør legge til rette for at sensitive personopplysninger kan registreres og sendes på en usikret måte.

<u>Virksomheter barnehager og skoler</u>
Alle registreringene om et barn fra barnehage og gjennom et helt utdannelsesløp utgjør til sammen et sett med opplysninger som gir et omfattende og detaljert bilde av barnets utvikling, faglige og sosiale atferd. Datatilsynet sier i sin veiledning at barn og unge er en ekstra sårbar gruppe, da de ikke kan samtykke til all registreringen selv. Det er i den sammenhengen viktig at barnehage- og skoleeierne tar personvern på alvor, både i egen organisasjon, og overfor barna og deres foresatte.

På bakgrunn av intervjuene er vår vurdering at kommunen ikke i tilstrekkelig grad har tydeliggjort for skolene og barnehagene hvilke dokumenter med personopplysninger, som kan lagres i Ephorte/Elements og hvilke som ikke skal lages der. Dette gjelder for eksempel personopplysninger fra foreldresamtaler, underveisvurderinger, observasjoner osv. Det gjøres derfor ulikt mellom barnehager og skoler. Det er vår vurdering at ansatte i skoler og barnehager opplever det som en utfordring å forvalte personopplysningene på en forsvarlig måte.

Det fremkommer at lærere i skolene ikke har skrivetilgang til Ephorte/Elements og må bruke minnepinne for overføring av det som kan være sensitive personopplysninger om elevene fra egen PC til Ephorte/Elements. Det er vår vurdering at kommunen må gjøre en risikovurdering av bruken av minnepinner med sensitive personopplysninger for å redusere risikoen for at slike opplysninger kommer på avveie. Det er også vår vurdering at kommunen bør etablere en rutine for kontroll av sletting av personopplysninger fra slike mellomlagringsenheter.

I intervjuene opplyses det om at personopplysninger, som referater fra foreldresamtaler o.l. blir lagret i Vigilo, og at personopplysninger også oppbevares i papirformat hos den enkelte lærer. Det er vår vurdering at det er uheldig at personopplysningene lagres på flere ulike måter og steder. Det kan føre til at virksomhetsleder ikke har oversikt over hvor og hvordan ulike personopplysninger om elevene er lagret, og at slike opplysninger ikke er tilgjengelige dersom den ansatte slutter i stillingen. Datatilsynet sier på sine nettsider at hele 10 prosent av avvikssakene de får inn gjelder barns personopplysninger, og det spenner fra systemsvikt til menneskelige feil. Kommunen bør skaffe seg en oversikt over alle måtene slike personopplysninger er lagret på, og gjøre konkrete vurderinger av formålet og gjennomføre en risikovurdering av behandlingene. Det er vår vurdering at kommunen, i tillegg til å gjennomføre en behandling av de ulike typene personopplysninger og gjennomføre risikovurderinger (DPIA), bør etablere og implementere konkrete rutiner for behandling og lagring/arkivering av personopplysninger i skoler og barnehager. Det gjelder både for personopplysninger som i dag lagres i ulike systemer og personopplysninger som oppbevares i papir, slik at virksomhetene i kommunen kan lagre dokumenter med personopplysninger på en sikker og enhetlig måte.

2.7 Ansvarlighet

2.7.1 Personvernombud

Revisjonskriterier

- Kommunen har et personvernombud, som har rammer og oppgaver i henhold til regelverket.
- Kommunen har offentliggjort kontaktopplysningene til personvernombudet og meldt disse til Datatilsynet.
- Kommunen sørger for at personvernombudet blir involvert i saker om personvern på riktig måte og til rett tid.
- Kommunen stiller til rådighet de ressurser som er nødvendig for å utføre nevnte oppgaver.
- Kommunen gir personvernombudet tilgang til personopplysninger og behandlingsaktiviteter, og gjør det mulig for vedkommende å opprettholde sin dybdekunnskap.
- Kommunen sikrer at personvernombudet ikke mottar instrukser om utførelsen av nevnte oppgaver. Vedkommende skal ikke avsettes eller straffes av kommunen eller databehandleren for å utføre sine oppgaver.
- Personvernombudet rapporterer direkte til det høyeste ledelsesnivået i kommunen

Fakta

Stillingen som personvernombud ble opprettet i kommunen i 2008/2009. Personvernombudsjobben ble først lagt til i stillingen som IT-sikkerhetsleder. Stillingen som IT-sikkerhetsleder hadde i hovedsak oppgaven å utarbeide prosedyrer på IT-sikkerhet. Oppgavene som personvernombud ble gjennomført i en 50 % stilling.

Personvernombudet som deltok i denne revisjonen sluttet i stillingen ved utgangen av 2019. Per 1. januar 2020 hadde ikke kommunen et personvernombud. I e-post fra kommunen 30. januar er vi blitt informert om at kommunen har fått på plass et nytt personvernombud. Det nye personvernombudet skal også virke i 50 % stilling. Kontaktinformasjonen til det nye personvernombudet er oppdatert på kommunens nettsider per 14.02.2020. På Datatilsynets oversikt over registrerte personvernombud fremkommer det at kontaktopplysningene til det nye personvernombudet er meldt inn til Datatilsynet.

I prosedyren *Organisering av personvern- og informasjons-sikkerhetsarbeidet*, sist oppdatert 09.12.2019 fremkommer det noen steder at personvernombudet er IT-sikkerhetsleder og andre steder at personvernombudet er sikkerhetsleder. Her fremkommer det også at det er etablert et sikkerhetsutvalg, som jobber på tvers i hele kommunen for å ivareta IT-sikkerheten i hele kommunen. I dokumentet som beskriver personvernombudet oppgaver *Sikkerhetsleder-Personvernombud*, sist oppdatert 17.12.2018 fremkommer det at sikkerhetsleder også er personvernombud. Her fremkommer det at sikkerhetsleder er sekretær for IT-sikkerhetsutvalget.

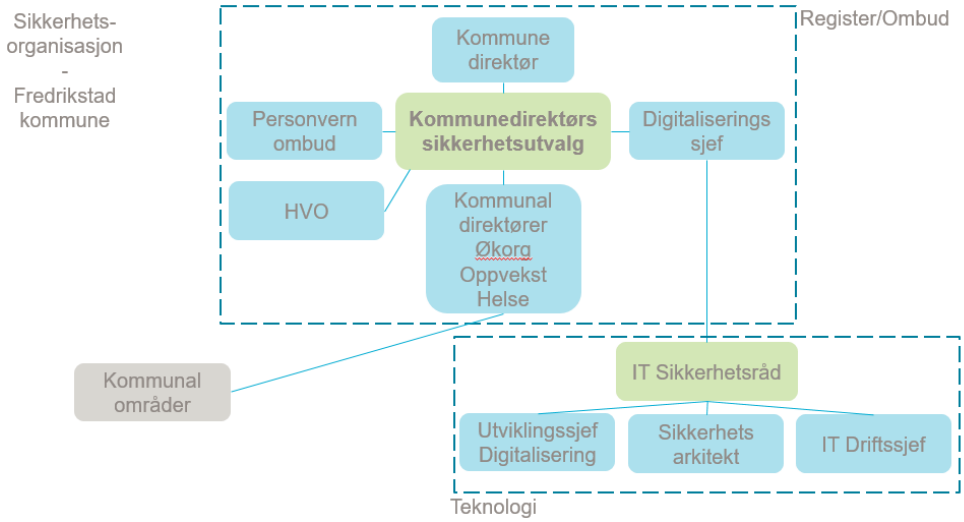
I dokumentet *Sikkerhetsleder-Personvernombud* står det at stillingen innehar følgende oppgaver:

Internt:
- Kontrollere og koordinere sikkerhetsarbeidet og dokumentasjonen av dette.
- Forberedelse av årlige ledelsesgjennomganger, skrive rapport / referat.
- Gjennomføring av årlige sikkerhetsrevisjoner, skrive rapport / referat
- Ansvarlig for å tilrettelegge for registrering av behandlinger. Eier (kan være løsningsansvarlige) er ansvarlig for å registrere behandlingen.
- Medansvarlig for at sikkerhetsdokumentasjonen er oppdatert sammen med leder/ løsningsansvarlig.
- Overordnet ansvarlig for sikkerhetsopplæringen til ansatte i kommunen
- Gi råd og veiledning til behandlingsansvarlig om behandling av personopplysninger og reglene for dette.
- Kontroll med risikovurderinger
- Kontroll med avviksbehandling.
- Varsle Datatilsynet når det er nødvendig

Eksternt:
- Bistå de registrerte (innbyggere/ansatte) med å ivareta deres rettigheter etter reglene om behandling av personopplysninger.
- Gi Datatilsynet opplysninger dersom tilsynet ber om det, herunder foreta undersøkelser i konkrete saker.

I høringsmøtet med kommuneadministrasjonen 24.04.2020 kommer det frem at det er gjort en omorganisering i sikkerhetsorganiseringen i kommunen. I e-post fra kommunen 24.04.2020 fremkommer det at Digitaliseringsavdelingen har et IT Sikkerhetsråd. IT sikkerhetsrådet har ukentlige møter og ledes av en Sikkerhetsarkitekt på full tid.

Figur 5: Kommunens sikkerhetsorganisasjon



Beskrivelsen av kommunens organisering av sikkerhetsarbeidet i rutinene og prosedyrene som fremkommer i kommunens kvalitetssystem, er en annen enn den som fremkommer i figuren og beskrivelsen over.

Det kommer frem av intervjuene og dokumentasjon at kommunens sikkerhetsutvalg har det overordnede oppgaven, å se til at personvernet ivaretas i kommunen. Det er kommunedirektøren som er leder av dette utvalget. Utvalget skal i utgangspunktet ha møter 2 ganger i året. Det blir sagt i intervjuene at det er en stund siden det ble gjennomført et møte i sikkerhetsutvalget.

Når GDPR regelverket ble innført i 2018 ble det etablert en egen GDPR-gruppe i kommunen. Gruppen skulle jobbe med innføringen av GDPR. *Rundskriv 3* i Risk Manager beskriver dette. Gruppen ble avviklet fordi den hadde gjennomført de oppgavene de hadde planlagt å gjøre. Resten av arbeidet skulle gjennomføres av personvernombudet og andre i organisasjonen jf. prosedyren *Organisering av personvern- og informasjons-sikkerhetsarbeidet*.

I vedtatt handlingsplan for Fredrikstad kommune 2019-2022, område for økonomi og organisasjonsutvikling er det under økonomi et punkt om personvernarbeidet i kommunen. *«Det har kommet ny personlovgivning (GDPR). I dag har kommunen en 50 prosent stilling som personvernombud. Seksjonen vil følge med på utviklingen og vurdere om denne stillingen må økes til 100 prosent.».* Utover dette fremkommer det ikke annen informasjon om kommunens arbeid med personvernregelverket i perioden.

I høringsmøtet med kommunen 24.04.2020 kommer det frem at kommunen har vurdert ressursen til personvernombudet og at det fremkommer i Handlingsplanen for 2020-2023 at kommunen har besluttet å videreføre personvernombudsrollen i 50 % stilling.

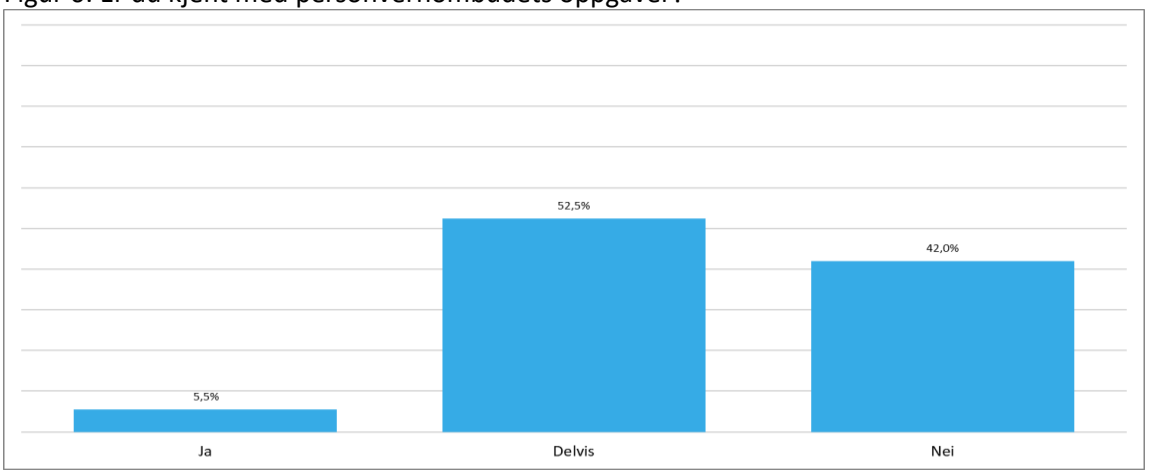
Det kommer frem av intervjuene at forvaltning av personvernregelverket i virksomhetene, i sin helhet er delegert ut til virksomhetene. Det er per i dag ikke gjennomført kontroll av om virksomhetene ivaretar dette. Personvernombudet sier i intervjuet at dersom oppgaven til personvernombudet er ment å være tettere på arbeidet med personvern i virksomheten, er en 50 % stilling som personvernombud for lite.

Det kommer frem av intervjuene at personvernombudet i liten grad har blitt involvert i arbeidet med å vurdere de ulike behandlingene. Personvernombudet har ofte blitt kontaktet etter at saken var behandlet/iverksatt og fikk dermed ikke mulighet til å påvirke behandlingene.

Det blir sagt i intervjuene at det er etterspurt mer bemanning på personvernområdet i kommunen. Det fremkommer at det er et ønske å få hjelp til å rydde i en del dokumenter og rutiner, samt at det er behov for en pådriver som kan se om ansatte og ledere følger opp de kravene som settes.

I spørreundersøkelsen ble ansatte og ledere i skoler og barnehager spurt om de kjenner personvernombudets oppgaver.

Figur 6: Er du kjent med personvernombudets oppgaver?



N=200

Av de 200 ansatte som svarte på dette spørsmålet sier 52,5 % at de delvis kjenner personvernombudets oppgaver, mens 42 % sier at de ikke kjenner til det. Av disse er 30 av 40 virksomhetsledere delvis kjent personombudets oppgaver, mens 8 virksomhetsledere sier at de ikke kjenner til hva som er personvernombudets oppgaver.

På de samme spørsmålet til kommunens ledergruppe svarer 11 av 25 leder at de kjenner til personvernombudets oppgaver, 10 kjenner delvis til det og 4 ledere svarer at de ikke kjenner til personvernombudets oppgaver. 3 leder sier også at de kjenner til at det er områder der personvern-ombudet burde vært involvert på deres fagområde, men ikke ble det.

Ingen av lærerne eller barnehagepedagogene som vi snakket med i intervjuene kjenner til hvem som er kommunens personvernombud (per desember 2019).

Vurderinger

Det er vår vurdering at kommunen har et personvernombud. Kommunens personvernombud som var del i denne revisjonen sluttet i sin stilling før denne rapporten ble utarbeidet. Det er er tilsatt en ny person i stillingen. Opplysningene om hvem som nå er kommunens personvernombud, med nye kontaktopplysninger er oppdatert på kommunens nettsider. Det nye personvernombudet er også tilsatt i 50 % stilling.

Kommunen har offentliggjort kontaktopplysningene til personvernombudet og meldt disse til Datatilsynet. Det er vår vurdering at personvernombudet hadde tilstrekkelig kompetanse på personvernregelverket. Vi har imidlertid ikke grunnlag for å vurdere det nye personvernombudets kompetanse på området.

Rutiner og intervjuer viser at mye av arbeidet med personvern er delegert ut til virksomhetene. Det er imidlertid vår vurdering at virksomhetene ikke er gjort i stand til å ivareta denne oppgaven. Vi legger til grunn funn som er vurdert tidligere i rapporten. Virksomhetene opplever at opplæringen på

personvernområdet er for generell og at de har behov for mer konkret hjelp for å kunne ivareta arbeidet på personvernområdet. Arbeidet med personvern er ressurskrevende og oppgavene til personvernombudet er omfattende i oppbyggingsfasen. I tillegg skal personvernombudet ha mulighet til å opprettholde sin dybdekunnskap på området. Det fremkommer at ansatte i virksomheten har behov for mer kunnskap og hjelp til arbeidet med personvernregelverket, enn det de opplever å ha fått hittil. På bakgrunn av opplysningene som fremkommer i intervjuene er det vår vurdering at kommunen heller ikke har sørget for at personvernombudet har blitt involvert i saker om personvern på riktig måte og til rett tid.

På bakgrunn av intervjuene og det arbeidet som er gjennomført hittil på personvernområdet vurderer vi at det er sannsynlig at kommunen per i dag, totalt sett ikke stiller til rådighet de ressurser som er nødvendig for å utføre oppgavene på personvernområdet. Arbeidet med å implementere og bygge opp systemet på personvernområdet i en så stor kommune som Fredrikstad, krever ekstra ressurser spesielt i en implementeringsfase. Slik det også fremkommer i kommunens Handlingsplan for 2019-2022. Kommunen har besluttet å videreføre et personvernombudet i 50 % stilling. Det er vår vurdering at dersom dette skal være tilstrekkelig, er det avgjørende at kommunen tydeliggjør oppgavefordelingen på andre roller i kommunen på personvernområdet, samt setter de ulike rollene i stand til å ivareta disse oppgavene og følger opp implementeringen av personvernregelverket i større grad enn hva som er tilfellet på revisjonens tidspunkt.

Det er videre vår vurdering at kommunen bruker begrepene IT-sikkerhet, informasjonssikkerhet, personvern og sikkerhet om hverandre på flere av de samme områdene. Dette kan gjøre at det blir uklart hva sikkerhetsarbeidet omfatter og hvem som skal utføre oppgavene på de ulike områdene. Begrepet informasjonssikkerhet dekker all informasjonsbehandling, også de delene som ikke handler om bruk av IT. IT sikkerhet omhandler også IT-sikkerheten utover det å ivareta personvernet. Det er derfor vår vurdering at kommunen bør rydde i begrepsbruken på disse områdene. Prosedyrer og rutiner i kvalitetssystemet er heller ikke oppdatert i henhold til dagens organisering av sikkerhetsarbeidet.

I pvf art. 38 punkt 3 står det at «Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet ikke mottar instrukser om utførelsen av nevnte oppgaver». Det er vår vurdering at kommunen sikrer at personvernombudet ikke mottar instrukser om utførelsen av oppgavene vedkommende har som personvernombud.

Senere under artikkelens punkt 3 står det at «Personvernombudet skal rapportere direkte til høyeste ledelsesnivå hos den behandlingsansvarlige eller databehandleren». I en kommune er det kommunedirektøren som er det høyeste ledernivå. I e-post 05.12.2019 viser personvernombudet til rutine for organisering av personvern og informasjonssikkerhet. Her fremkommer det at sikkerhetsutvalget er mottaker av rapporter og oppfølging på sikkerhetsområdet. Det er kommunedirektøren som er leder av sikkerhetsutvalget, slik sett er det vår vurdering at det er lagt opp til at rapporteringen går direkte til øverste leder.

Det kommer imidlertid frem av intervjuene at møtene i sikkerhetsutvalget ikke har blitt gjennomført etter planen. Det blir sagt i intervjuene at det er en stund siden det ble gjennomført møte i sikkerhetsutvalget. Da møtene i sikkerhetsutvalget ikke har blitt avhold slik planen er, er det vår vurdering av rapporterings- og oppfølgingssystemet på personvernområdet ikke fungerer slik intensjonen har vært.

2.7.2 Risikovurdering - personvernkonsekvens

Revisjonskriterier

- Kommunen har gjennomført en risikovurdering av personopplysningssikkerheten før alle behandlinger igangsettes.
- Kommunen har gjennomført en vurdering av personvernkonsekvensene (DPIA) i henhold til Datatilsynets liste.

Fakta

I kommunens dokument *Risikovurdering informasjonssikkerhet og personvern*, datert 02.06.2019, står det *«Risikovurderinger skal gjennomføres før behandling av helse- og personopplysninger igangsettes, og ved endringer som kan berøre informasjonssikkerheten».* Videre står det at *«Risikovurderinger skal gjennomføres av virksomhetsledere/daglig behandlingsansvarlige i Fredrikstad kommune med mulig bistand av IT-driftsansvarlig og sikkerhetsleder/personvernombud. Risikoen vurderes og dokumenteres i kvalitetssystemet i egen modul for dette.»*

Personvernombudet informerer om at alle som er eiere av de ulike behandlingene har fått informasjon om at de skal gjennomføre risikovurdering (DPIA) av behandlingene. Det kommer frem av systemgjennomgangen i RiskManager at dette ikke er ivaretatt.

I en oversendt presentasjon *Ny personvernlov GDPR til LA*, datert 28.05.2018 står det *«Nye risikovurderinger med personvernkonsekvenser for alle behandlinger, prosjekter o.l.. Risikomodulen i Kvalitetssystemet kan brukes som det er.»* Under punktet Fremdrift står det *«LA-ene registrerer behandlinger i mai/juni 2018» og «Risikovurderinger i løpet av 2018».*

I en annen presentasjon *Rådmannsinnlegg på LUP*[14] *5. september 2018*, står det *«Nye risikovurderinger må gjøres av alle ledere»*

I *RUNDSKRIV nr 3/2018 fra Seksjon for økonomi og organisasjonsutvikling,* 04.06.2018 til kommunalsjefer, etatssjefer og virksomhetsledere står det at «*Alle skal vurdere risiko- og personvernkonsekvenser. Dersom et tiltak utgjør en stor risiko for personvernet, må virksomheten også utrede hvilke personvernkonsekvenser det kan ha. Her vil alle virksomheter i Fredrikstad kommune få nye oppgaver…»* Under punktet *Oppgaver i seksjoner/etater/virksomheter* står det at det skal gjennomføres risikovurderinger av hvordan kommunen behandler personopplysninger og at det skal gjennomføres risikovurderinger av fag- og fellessystemer.

I en gjennomgang av kommunens kvalitetssystem 19.12.2019 fremkommer det at det ikke er gjennomført DPIA – vurderinger av personvernkonsekvenser i kommunen kvalitetssystem.

Det kommer frem av intervjuene at ansatte mente at oppgaven med vurderinger av konsekvensen av behandling av personopplysninger (DPIA) ligger hos personvernombudet.

Det kommer frem av intervjuene at kommunen har et prosjekt på gang som omhandler robotisering. Personvernombudet har i den forbindelse minnet om at kommunen må tenke på at det ikke må hentes inn mer personopplysninger enn nødvendig for formålet. Robotiseringen skal i første omgang kun brukes ved enkle vedtak som ikke trenger vurderinger.

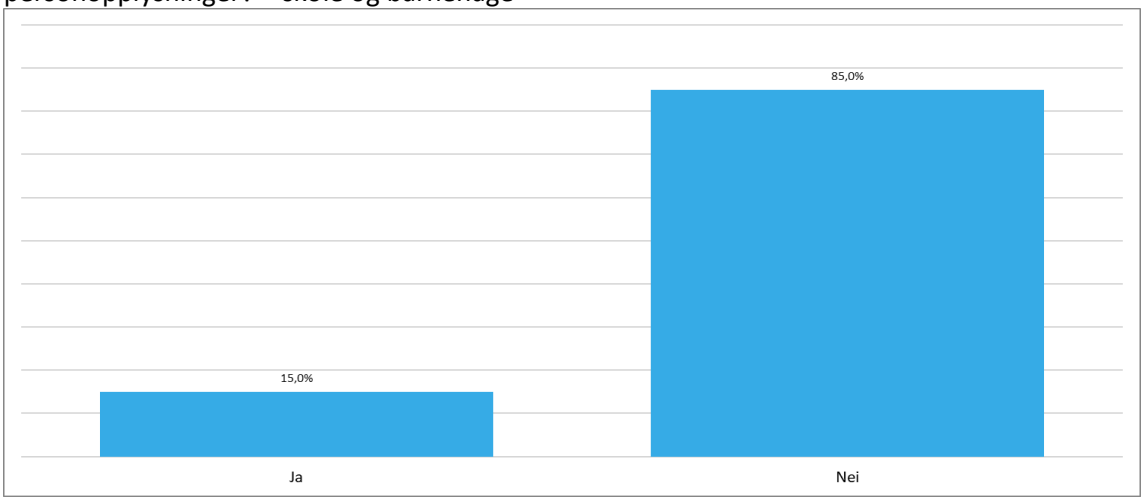
[14] Lederutviklingsprogram i Fredrikstad kommune

Kommunen har gått over fra Ephorte til Elements, og det er gjort en risikovurdering på dette. Det kommer frem av intervjuene at det ikke er gjennomført risikovurderinger av behandlinger av personopplysninger i Elements. Byarkivaren opplyser imidlertid at det skal gjennomføres. De opplyser om at de har risikovurdert «Svar-ut» og at de også vil gjøre risikovurderinger innenfor HMS. Byarkivaren sier at de kan bli bedre på risikovurderinger, og at de er kjent med at det skal gjøres risikovurderinger.

Det kommer frem av intervjuene at det er gjennomført risikovurderinger av Vigilo. Personvernombudet har ikke deltatt i denne vurderingen. Denne risikovurderingen har de i kvalitetssystemet – Risk Manager. Risikovurderingen er gjort av Vigilo som system og ikke av personopplysninger spesielt. Når det gjelder den tidligere nevnte hendelsen knyttet til Vigilo, har kommunen hatt møte med leverandøren om dette. På grunn av slike hendelser, vil ikke Folkeregisteret lenger sender fra seg opplysninger dersom foreldrene bor på ulike adresser. Det er kommunen som får ansvaret for å påse at opplysningene de fører inn i Vigilo er riktig.

I spørreundersøkelsen ble virksomhetsledere spurt om de kjenner til om det er gjennomført risikovurdering av konsekvensen ved behandling av personopplysninger i skoler/barnehager.

Figur 7: Kjenner du til om det er gjennomført risikovurdering av konsekvensen ved behandling av personopplysninger? – skole og barnehage

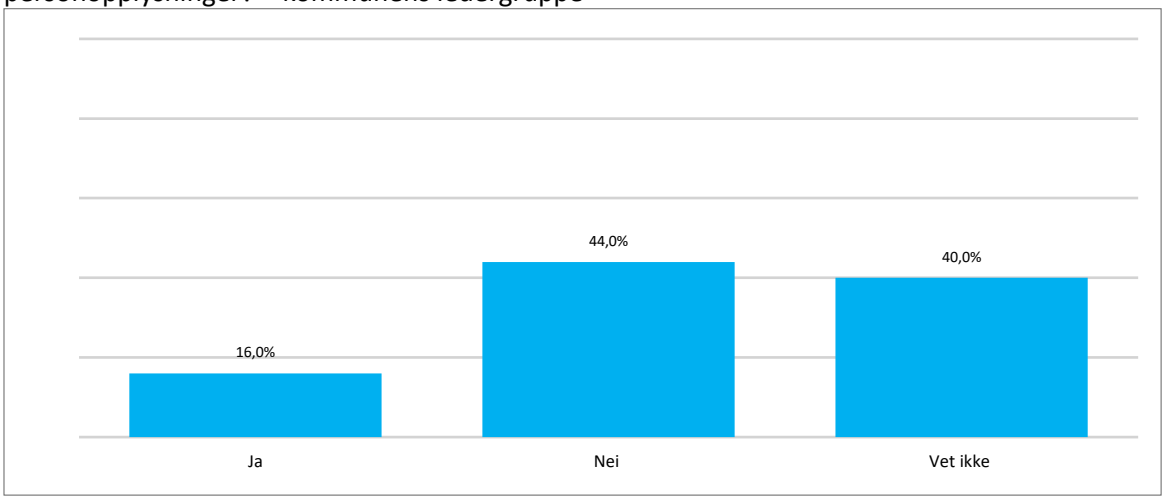


N=40

15 % sier at de kjenner til at det er gjennomført, mens 85 % av virksomhetslederne sier at de ikke kjenner til om det er gjennomført en risikovurdering for konsekvensen ved behandling av personopplysninger i skoler og barnehager.

Tilsvarende spørsmål ble stilt til kommunens ledergruppe.

Figur 8: Kjenner du til om det er gjennomført risikovurdering av konsekvensen ved behandling av personopplysninger? – kommunens ledergruppe



N=25

4 ledere sier at det er gjennomført en risikovurdering for konsekvensen ved behandling av personopplysningene på deres fagområde. 11 leder sier at det ikke er gjennomført og 10 sier de ikke vet om det er gjort.

Vurderinger

Det er vår vurdering at kommunen har gjennomført en risikovurdering av mange av systemene som kommunen benytter til å behandle personopplysninger. Det er etter hva vi har blitt informert om de respektive LA'ene som er delegert oppgaven med å risikovurderinger. Det fremkommer imidlertid opplysninger om at det fremdeles er systemer som ikke er risikovurdert, som Elements. Regelverket presiserer at en risikovurdering av personopplysningssikkerheten skal gjennomføres før alle behandlinger igangsettes.

I personvernforordningen artikkel 35 står det at behandlingsansvarlig skal gjennomføre en vurdering av personvernkonsekvensene (DPIA) der det er sannsynlig og høy risiko for den registrertes rettigheter. Datatilsynet sier i sin veiledning at en vurdering av personvernkonsekvenser er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak.

En vurdering av om en behandling av personopplysninger utgjør en høy risiko må baseres på en vurdering av fire kriterier: behandlingens art, omfang, formål og i hvilken sammenheng behandlingen utføres. Kommunen må først skaffe seg en oversikt over hvilke behandlingsaktiviteter de gjennomfører i hele virksomheten. Deretter må de gjøre en vurdering av hvilke behandlingsaktiviteter som innebærer en høy risiko - for konsekvens og sannsynlighet for avvik. På de behandlingsaktivitetene som kommunen vurderer at det er en høy risiko må kommunen gjennomføre en full vurdering av personvernkonsekvensen.

Eksempelvis skal det gjennomføres DPIA av alle behandlinger av personopplysninger for å evaluere læring, mestring og trivsel i skoler eller barnehager. Det er vår vurdering at kommunen ikke har gjennomført vurderinger av personvernkonsekvenser (DPIA) av alle behandlingene med høy risiko, og heller ikke alle behandlingsaktivitetene som alltid krever det (i henhold til datatilsynets liste).

2.7.3 Internkontroll

Revisjonskriterier

- Med bakgrunn i gjennomførte risikovurderinger, har kommunen iverksatt egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysningene skjer i samsvar med personvernforordningen.
- Kommunen har innhentet kunnskap om personopplysninger behandles etter personvernregelverket.
- Kommunen har sørget for å iverksette tiltak der det fremkommer at regelverket ikke etterleves.
- Kommunen sikrer at brudd på personopplysningssikkerheten meldes til Datatilsynet når det er risiko for personers rettigheter og frihet.
- Kommunen sikrer at den registrerte blir varslet, dersom bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter.
- Kommunen sikrer at brudd som ikke rapporteres til Datatilsynet, behandles og begrunnes i en intern avviksrapport.

Fakta

Det kommer frem av intervju at det per i dag ikke er gjennomført noen kontroll/årlige sikkerhetsrevisjoner av om virksomhetene ivaretar kravene i personvernregelverket og den oppgaven som er delegert ut til virksomhetene.

I dokumentet *Sikkerhetsleder- Personvernombud*, datert 17.12.2018 fremkommer det at personvernombudet skal gjennomføre årlige sikkerhetsrevisjoner og utarbeide rapport/referat etter gjennomføringen. Det kommer frem av alle vi intervjuet at det ikke har vært gjennomført årlige sikkerhetsrevisjoner på deres område. Det kommer også frem at personvernet ikke er en del av den overordnede risikovurderingen til kommunen. Ansatte har etterspurt en gjennomgang på personvernområdet, som hjelp til å få systemene på plass.

I kommunens rutiner vises det til at sikkerhetsansvarlig skal «påse at» personvernet blir ivaretatt. Det kommer frem av intervjuene at den årlige sikkerhetsrevisjonen er et av de temaene som personvernombud hadde planer om å ta opp i Sikkerhetsutvalget. Møtene i Sikkerhetsutvalget har imidlertid ikke blitt gjennomført som planlagt.

I kommunens *Retningslinjer for personvern og informasjonssikkerhet – ansatte*, datert 04.04.2019 står det *«En viktig del i sikkerhetsarbeidet, er en jevnlig kontroll med hvordan sikkerhetstiltakene og prosedyrene er kjent ute i organisasjonen. For å kontrollere sikkerhetsnivået i kommunen, kan det gjennomføres egenkontroller som spørreskjema innen alle virksomheter. Resultatet fra spørreundersøkelsen gir daglig ansvarlig og sikkerhetsleder viktig informasjon om områder der det er behov for mer innsats, f. eks behov for mer opplæring. Som medarbeider i kommunen vil du delta i disse egenkontrollene gjennom å svare på spørreskjema.»* Det foreligger ikke dokumentasjon på at det er utarbeidet et skjema på egenkontroll eller gjennomført slike egenkontroller per i dag.

Kommunen har en avviksmodul i Risk Manager på personvern. Denne har personvernombudet tilgang til og gir evt. en tilbakemelding dersom noe er feilført i avviksmodulen. Det er ikke etablert en rutine for hvem som skal følge opp dette eller noe fast rapporteringssystem. Dette er et av de områdene som Sikkerhetsutvalget skal ivareta.

Det kommer frem av intervjuene at alvorlige brudd på personvernregelverket blir meldt til Datatilsynet. Brudd på personvernregelverket, som kommunen ikke trenger å melde til Datatilsynet, blir ført på eget område i Risk manager.

Det kommer frem av intervjuene med både barnehagepedagogene og lærerne at dersom det hadde vært behov for å melde avvik på personvernområdet, så ville de gått til nærmeste leder. De kjenner Risk Manager og opplyser om at de melder andre typer avvik i dette systemet.

Rutinen for å registrere avvik på personvernregelverket er at den som oppdager avviket skal registrere det i Risk Manager. Nærmeste overordnede skal da vurdere registreringen. Personvernombudet får ikke noen melding eller informasjon når et avvik på personvernregelverket er registrert. Personvernombudet er avhengig av å bli kontaktet av den som har registrert avviket Dersom det er avvik som personvernombudet ikke blir orientert om, så tror personvernombudet at det er en fare for at avviket ikke blir meldt videre til Datatilsynet.

Vurderinger

Datatilsynet sier i sin veiledning at god internkontroll er med på å sikre at virksomheten behandler personopplysninger lovlig, sikkert og forsvarlig. Internkontroll skal være ledelsens verktøy for å ivareta sitt ansvar og demonstrere etterlevelse etter personvernregelverket, og de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte. Tiltakene skal dokumenteres og oppdateres ved behov. Det fremkommer av intervjuene at kommunen per i dag ikke har gjennomført de årlige sikkerhetsrevisjonene (internkontroll) og utarbeidet rapport/referat etter gjennomføringen, jf. egen rutine om dette. Dette begrunnes i at det ikke er tilstrekkelig ressurser til å gjøre dette arbeidet. Kommunen har derfor ikke innhentet tilstrekkelig kunnskap om personopplysninger behandles etter personvernregelverket i virksomhetene. Kommunen har dermed heller ikke sørget for å iverksette tiltak der det fremkommer at regelverket ikke etterleves.

På bakgrunn av informasjon som kommer frem av intervjuene og systemgjennomgangen er det vår vurdering at kommunen har meldt brudd på personopplysningssikkerheten til Datatilsynet, når det har vært risiko for personers rettigheter og frihet. Det er også vår vurdering at kommunen sikrer at den registrerte blir varslet, dersom bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter. Det fremkommer imidlertid at informasjon om avvik på personvernområdet ikke er så tilgjengelig som personvernombudet hadde ønsket. Personvernombudet er avhengig av at de som melder avvik også sender melding til personvernombudet om avviket. Alternativt må personvernombudet inn i avvikssystemet hyppig for å se om det er registrert avvik, da systemet ikke varsler personvernombudet om nye avvik, men kun ledere på området. Slik systemet fungerer i dag, er det etter vår oppfatning en viss risiko for at et brudd på personvernet, som skal meldes til Datatilsynet, ikke blir meldt innen fristen. Det er også en risiko for at brudd som ikke skal rapporteres til Datatilsynet, ikke blir registrert i en intern oversikt og begrunnet i en intern avviksrapport, slik regelverket krever.

I personvernforordningen artikkel 24 står det at behandlingsansvarlig skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov. Det er vår vurdering at kommunen per i dag ikke i tilstrekkelig grad har iverksatt egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysningene skjer i samsvar med personvernforordningen.

2.7.4 Opplæring i regelverket

Revisjonskriterier

- Kommunen må sette de ansatte i stand til å etterleve regelverket, ved blant annet å gi de ansatte opplæring

Fakta

Det fremkommer av intervjuene at personvernombudet har gjennomført noen samlinger om GDPR i kommunen. Kursene har vært rettet mot lederne i kommunen. Etter kursene får lederne tilgang til PowerPointen slik at de kan dele dette med sine ansatte. Personvernombudet opplyser at det er gjennomført opplæring for både Helse- og velferd og NAV i DPIA. Det er også gjennomført opplæring dersom noen har henvendt seg med ønske om opplæring.

I notat fra 05.07.2018 - *Oppgaver og fremdrift GDPR* - oversendt fra kommunen fremkommer det at det sommeren 2018 ble sendt et rundskriv - *Ny personvernlov, GDPR* til Kommunalsjefer, etatssjefer og virksomhetsledere i kommunen. Rundskrivet er datert 4.06.2018 og informerer om endringene i personvernlovgivingen, hva endringene betyr for Fredrikstad kommune og hvilke oppgaver som er lagt til henholdsvis seksjonene/etatene/virksomhetene og Seksjon økonomi og organisasjonsutvikling. Rundskrivet gir også informasjon om hvordan opplæringen vil bli organisert i kommunen.

I notatet - *Oppgaver og fremdrift GDPR* - fremkommer det at det også ble arrangert frokostmøter med alle lederne i kommunen i perioden juni, august og september 2018. PowerPoint fra disse frokostmøtene med lederne i kommunen viser at opplæringen omfatter flere av områdene som var nytt i personvernregelverket fra 2018, og tar for seg de områdene som kommunen må jobbe med og viser til hvem som skal sørge for å gjennomføre dette arbeidet på de ulike områder.

I dokumentet *Mål personvern og informasjonssikkerhet*, datert 09.12.2019 står det *«Informasjonssikkerheten i kommunen skal kontinuerlig etterprøves og forbedres. Medarbeidere skal ha tilstrekkelig kompetanse og gis nødvendig opplæring slik at tilfredsstillende informasjonssikkerhet opprettholdes.»*

I dokumentet *Retningslinjer for personvern og informasjonssikkerhet – ansatte,* datert 04.04.2019 står det «*God sikkerhet forutsetter god opplæring/kompetanse og motiverte ansatte. Som medarbeider i Fredrikstad kommune er det viktig at du har kjennskap til kommunens kvalitetssystem for informasjonssikkerhet og personvern. Du skal være kjent med hvem som har ansvar for hva i sikkerhetsarbeidet, du skal ha kjennskap til hvilke mål og strategier vi sammen skal jobbe etter, du skal være kjent med og forstå de prosedyrer og retningslinjer som er besluttet….»*

Det kommer frem av intervjuene at GDPR har vært tema på virksomhetsledermøter flere ganger. Administrasjonen hadde også et eget møte om GDPR for alle virksomhetslederne i seksjon for Utdanning og oppvekst.

Kommunen har hatt en samling med alle virksomhetslederne i Den blå grotte da GDPR kom. Av dokumentasjon mottatt fra Fredrikstad kommune 5.12.2019 fremkommer det en presentasjon kalt *rådmannsinnlegg på LUP 5. september 2018*. Innlegget gir informasjon om hvor kvalitetsdokumentene for personvern kan finnes og når og hvor det vil bli gitt opplæring i GDPR. Her står det at informasjon og opplæring i personvernregelverket gjennomføres med et frokostmøte om personvern og en opplæring i HMS og personvern i oktober. Det fremkommer at alle ledere blir oppfordret til å melde seg på. Det står også at *«I tillegg kommer personvernombudet til dere og informerer og bistår ved behov.»* Det blir også vist til Rundskriv nr. 3 datert 5. mai 2018.

Det kommer frem av intervjuene at ved nyansettelser blir den som ansettes informert om informasjonssikkerheten gjennom et e-læringskurs med tema *it-sikkerhet*. Det er IT-avdelingen som skal sørge for dette og personvernombudet er ikke blitt involvert. For de som har vært ansatt i mange år, er det daglig ansvarlig som er opplæringsansvarlig for nyheter og oppdateringer av regelverket etc.

I dokumentet Retningslinjer for personvern og informasjonssikkerhet – ansatte, datert 04.04.2019 står det «*Disse retningslinjene gjelder alle medarbeidere som behandler personopplysninger, både sensitiv papirbasert informasjon og personopplysninger som behandles ved hjelp av kommunens dataanlegg og datasystem……Innføring i sikkerhet og sikkerhetsrutiner er en del av introduksjonsprogrammet for nye medarbeidere, og vil som et ledd i kvalitetssikringen også bli gjennomgått for våre øvrige ansatte. I vår kommune gis denne opplæringen i form av obligatorisk e-læringskurs.»*

Det kommer frem av intervjuene at det tidligere ble gjennomført IT-kurs for alle nyansatte. Nå har de gått over til e-læring på alle områder. Digitaliseringssjefen mener det ikke blir like opplæring med e-læring, som med et kurs. Personvernombudet hadde også innlegg om personvernregelverket og oppgavefordelingen på de ulike områdene, på de tidligere avholdte kursene. Det kommer frem av intervjuene at opplæring i personvernregelverket ble svekket i overgangen til e-læringskurs og at det ikke gis en egen opplæring i GDPR ved nyansettelser.

I intervjuene kommer det frem at ledere mener at det er for lite lederopplæring på personvern/GDPR. Det burde vært mer fokus på dette ved LUP.

Det kommer frem av intervjuene at arkivet har gitt opplæring til både ledere og saksbehandlere i Ephorte og Elements. De går da bl.a. gjennom offentlighetsloven. Nyansatte ved arkivet har fadder, e-læring og kurs. Personvern blir nevnt i disse kursene, men det gjennomføres ikke noe konkret GDPR-kurs. Personvernombudet og byarkivaren har hatt superbrukere inne for opplæring. De har også hatt dette med de private barnehagene.

Avdelingsleder på servicetorget er kjent med at kommunen har et personvernombud og har fått opplæring i personvernregelverket. De hadde en e-læring for alle ansatte når GDPR ble innført. De hadde også informasjon om det på møter.

Det kommer frem av intervjuene at ansatte på HR-avdelingen har fått opplæring i personvernregelverket på samlinger i regi av KS og andre forteller at den opplæringen de har fått på personvern er på eksterne kurs om informasjonssikkerhet.

Digitaliseringssjefen sier at han ikke tror at det har vært gjennomført noen arbeidsgiveropplæring/lederopplæring overordnet på personvernregleverket/GDPR. IT informerer ansatte i kommunen om hvordan de benytter/ikke benytter personopplysninger, dersom de får en direkte forespørsler internt.

I intervjuene sier lærerne at de ikke har fått opplæring i GDPR/personvernregelverket fra kommunen. De kjenner ikke til at det er gjennomført e-læring på området. Skolens ledelse har informert om personvernregelverket til personalet på skolen. Særlig forholdet mellom arbeidsflyt og sikring av persondata, og hvordan opplysninger skal arkiveres for framtiden.

I intervjuene med barnehageansatte kommer det frem at alle nyansatte må gjennom et e-læringskurs som IT-avdelingen arrangerer, og de får en liten brosjyre hvor kommunen sier en del om IT-sikkerhet. I intervjuene kommer det frem at pedagogene ikke har fått opplæring i GDPR/personvern. De opplyser om at de er med i diskusjonsgrupper med andre barnehageansatte på Facebook og får en del innspill derfra. Som nyansatt får man en informasjonsbrosjyre og et e-

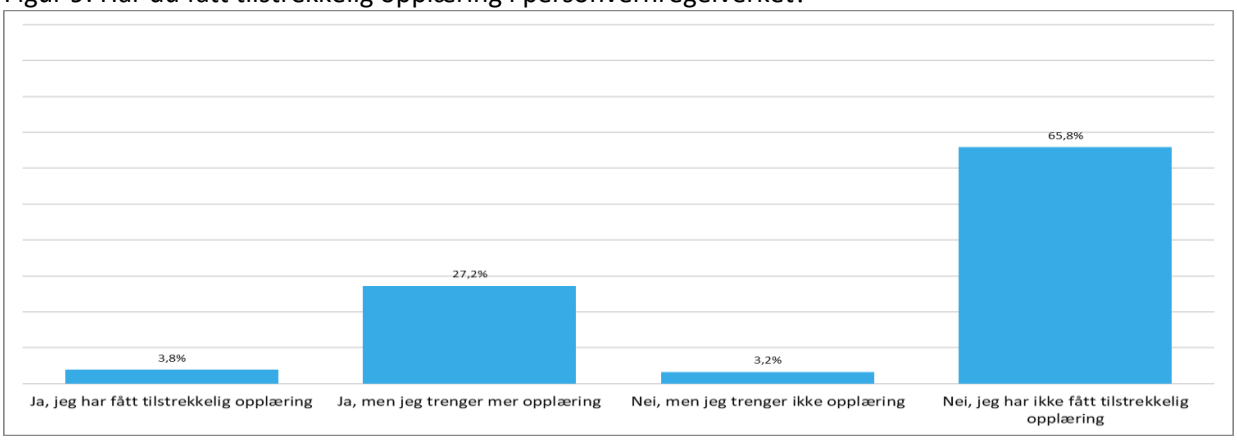
læringsprogram (kun de siste årene). Her klikker man seg gjennom, men de opplever ikke å ha lært så mye av det. De synes derfor ikke at de har fått et eierskap til det. Eventuelt tenker de at de kan søke etter informasjon på Frekit.

Det kommer frem at virksomhetsledere i barnehage har hatt et frokostmøte med opplæring i personvern for en stund siden. De fikk ingen dokumentasjon der. Dette var et møte som var åpent for alle og en måtte melde seg på selv. De trenger en konkret opplæring på praktiske ting, mer rettet mot deres virksomhet. Den opplæringen de fikk var for generell. De trenger folk i kommunen som kan dette og som kan gi dem konkrete svar.

I spørreundersøkelsen ble kommunes ledergruppe spurt om de mener at de har fått tilstrekkelig opplæring i personvernregelverket. Av de 25 som svarte på undersøkelsen mener 9 at de ikke har fått tilstrekkelig opplæring og 11 at de har fått opplæring, men trenger mer. Totalt 20 mener dermed at de trenger mer opplæring. 4 ledere mener de har fått tilstrekkelig opplæring.

I spørreundersøkelsen ble ansatte i skoler og barnehager spurt om de mener de har fått tilstrekkelig opplæring i personvernregelverket.

Figur 9: Har du fått tilstrekkelig opplæring i personvernregelverket?

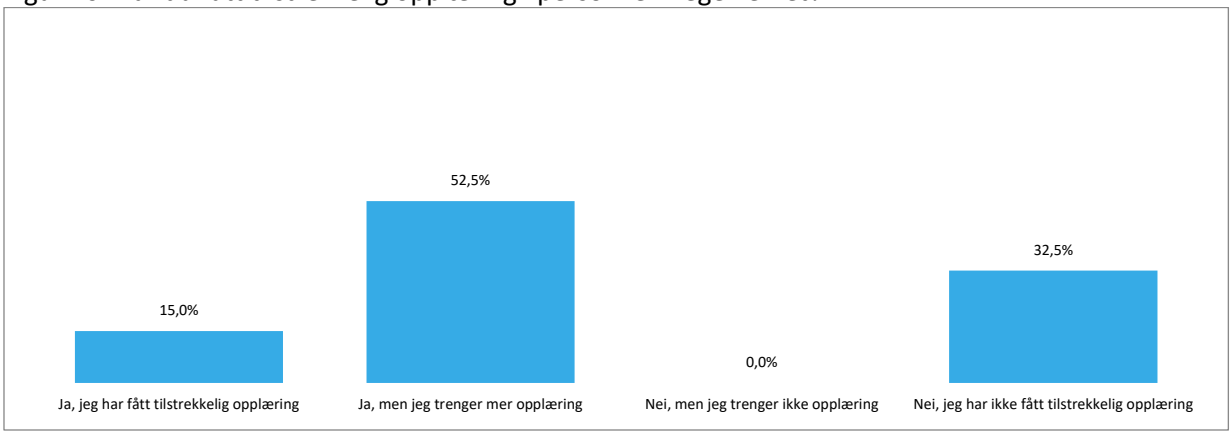


N=158

Av totalt 158 ansatte som svarte på dette spørsmålet, svarer 65,8 % av de ansatte i skolene og barnehagene at de ikke har fått tilstrekkelig opplæring. Kun 3,8 % mener at de har fått tilstrekkelig opplæring. Totalt 96,2 % mener at de har behov for mer opplæring.

Tilsvarende spørsmål ble stilt til virksomhetslederne.

Figur 10: Har du fått tilstrekkelig opplæring i personvernregelverket?

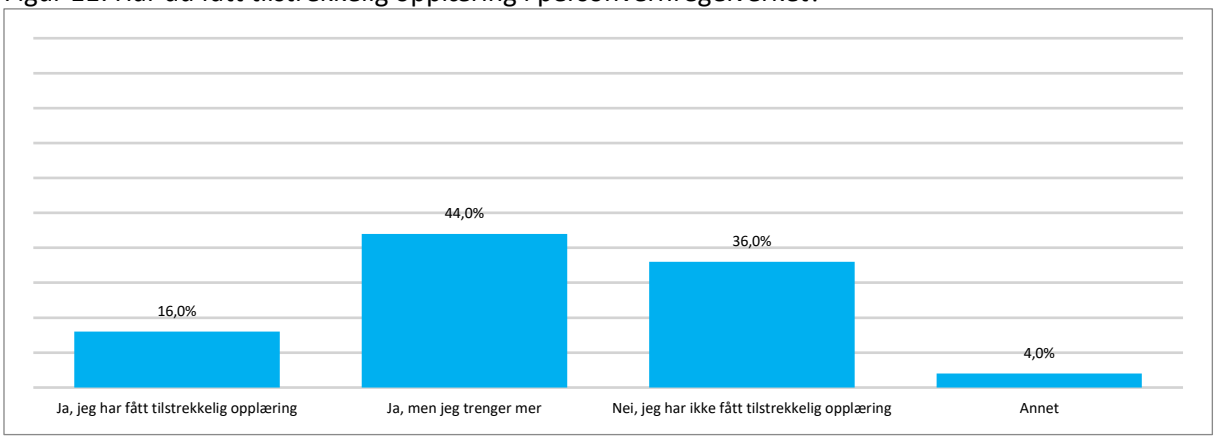


N=40

15 % av virksomhetslederne mener at de har fått tilstrekkelig opplæring, mens 85 % mener at de ikke har fått tilstrekkelig opplæring eller at de har fått opplæring, men trenger mer.

Tilsvarende spørsmål ble også stilt til kommunens ledergruppe.

Figur 11: Har du fått tilstrekkelig opplæring i personvernregelverket?



N=25

Totalt 20 av 25 av kommunens ledere, som har besvart undersøkelsen, sier at de har behov for mer opplæring.

I spørreundersøkelsen fremkommer det områder som oppleves som særlig utfordrende for ledere og ansatte i virksomhet skole og barnehage å håndtere med tanke på GDPR/personvern:

<u>Digitalt</u>

- Innhente og administrere samtykke fra foresatte og elever ved bruk av digitale læremidler/apper.
- Loggføring og kontroll av elevers internettbruk.
- Bruk av digitale verktøy for å kartlegge elevenes rett til et trygt og god skolemiljø.
- Gjennomføring av risikoanalyser for bruk av digitale læremidler.
- Digital kommunikasjon som bla e-post fra foreldre til barnehagen og skolen med sensitiv informasjon.
- Bruk av privat mobil i jobbsammenheng. Det oppleves som ukomfortabelt å bruke privat telefon med tanke på personvernet.

<u>Lagring</u>

- Lagring av elevinformasjon som er vurdert som ikke arkivverdig, bla notater fra utviklingssamtaler og elevsamtaler.
- Lagring av kommunikasjon, hvilke personopplysninger er relevante.
- Oppbevaring og sletting av opplysninger og informasjon om barn og familier som blir liggende i mange år etter at barnet er ferdig i barnehagen.
- Hvor lenge opplysninger kan lagres, og sletting av data.

<u>Deling og skjerming av personopplysninger</u>

- Deling av informasjon om sårbare elever og familier til andre fagområder innenfor virksomheten.
- Deling av opplysninger om utagerende elever, og elever med spesielle behov.
- Interne rutiner for sikring av at sensitiv informasjon ikke blir tilgjengelig for feil personer, f.eks utskrifter som blir liggende igjen på printer.

- For mange fagpersoner som har tilgang til enkeltsaker. Noen får tilgang til opplysninger de ikke trenger.
- Personvern i klassen om enkeltelever.
- Delt foreldreansvar (ved konflikt ennå ikke behandlet i rettsapparatet) og innsyn i opplysninger som gjelder barnet/eleven.

Annet

- Liten kapasitet satt av til å jobbe med personvern.
- Der det er en mangel på god nok vurderingskompetanse til at det er et reelt samtykke.
- Hvor mye en må informere ut om når det gjelder behandlingen av personopplysninger.

Vurderinger

PowerPoint fra frokostmøtene med lederne i kommunen viser at opplæringen omfatter de fleste områdene som er nytt i personvernregelverket fra 2018, og tar for seg de områdene som kommunen må jobbe med og viser til hvem som skal sørge for å gjennomføre dette arbeidet. På bakgrunn av intervjuene og spørreundersøkelsen er det vår vurdering at ikke alle i målgruppen har deltatt på opplæringen som ble gitt sommeren 2018. Det er også kun noen virksomheter/avdelinger som har benyttet seg av ytterligere opplæring etter tilbud fra personvernombudet.

På bakgrunn av intervjuer, spørreundersøkelsen, manglende føringer i protokoll og manglende vurderinger av DPIA er det vår vurdering at opplæringen ikke har vært tilstrekkelig. Det kan også være årsaken til at de heller ikke i tilstrekkelig grad har gitt opplæring videre nedover i organisasjonen/virksomheten.

Det har i liten grad vært opplæring av ansatte ute i barnehagene og på skole. For å gjøre ansatte tryggere på å håndtere personopplysninger bør kommunen gi mer konkret opplæring. Ansatte i skoler og barnehager opplever også at den opplæringen eller informasjonen om personvernregelverket som de har fått er av for generell karakter. Det er derfor vår vurdering at kommunen bør vurdere å spisse opplæringen mot kommunens ulike virksomheter.

2.7.5 Databehandlere

Revisjonskriterier

- Kommunen har en oversikt over de databehandlerne de benytter
- Kommunen har vurdert om opplysningene som databehandler krever, er adekvate, relevante og begrenset for formålet.
- Kommunen har utarbeidet avtaler med databehandlerne i henhold til kravene i regelverket.

Fakta

Det kommer frem av intervjuene at det er IT-avdelingen som har sørget for å få på plass databehandleravtalene. Det fremkommer også i dokumentasjon fra opplæringen av kommunens ledere i perioden juni-september 2018.

Det kommer frem av intervjuene at kommunen etablerer databehandleravtaler (eksterne) med leverandører som tilbyr systemer der det behandles personopplysninger. Det er

kommunaldirektørene som har ansvaret for at det inngås avtaler, men i praksis er det fagsystemeier i kommunen som gjør det. Digitaliseringssjefen har laget alle avtalene knyttet til programvarene. Kommunen bruker DIFI`s standardavtaler (2-3 siste årene). Kommunen har inngått flere 10-talls databehandleravtaler. Kommunen har en liste, men denne er ikke så oversiktlig. Det kan for eksempel være avtaler for flere systemer i en sak. Noen av databehandleravtalene ligger også i kjøpsavtalen. Digitaliseringssjefen mener imidlertid at de skal kunne lage en oversikt dersom Datatilsynet ber om det. Ikke alle datasystemer krever databehandleravtaler, fordi de ikke inneholder/behandler personopplysninger. Det kan være en utfordring internt, å skille mellom intern og ekstern databehandler. Noen store leverandører f.eks. Visma har så gode avtaler at disse kan brukes i stedet for at kommunen utarbeider egne avtaler.

Det kommer frem i intervjuene at databehandleravtalene er lagret i Ephorte/Elements. I intervjuene sier ansatte at det er ressurskrevende at alle små og store app'er skal risikovurderes og ha databehandleravtaler. På skolesiden har kommunen tatt opp denne utfordringen med Utdanningsdirektoratet og foreslått en sentral ordning, som en felles godkjenning av databehandleravtaler, som mange eller alle kommuner bruker. Det er databehandleravtaler på alle systemer, men de opplyser om at de ikke har mulighet til å kvalitetssikre samtlige avtaler.

Kommunen har i brev 9.12.2019 oversendt to databehandleravtaler. Databehandleravtale med SKOOLER inngått 11.11.2018, gjeldende for grunnskolene i kommunen og med Vigilo AS signert 27.02.2018, avtalen gjelder for både grunnskolene og barnehagene i kommunen.

Vurderinger

Det er vår vurdering at kommunen har en oversikt over de databehandlerne de benytter, selv om den ifølge kommunen selv ikke er så oversiktlig som den burde være. Kommunen har vurdert hvilke opplysninger som databehandlerne krever, om de er adekvate, relevante og begrenset for formålet. Det er også vår vurdering at kommunen har utarbeidet avtaler med databehandlerne i henhold til kravene i regelverket.

3 KONKLUSJON OG ANBEFALINGER

Problemstilling - Har kommunen implementert personvernregelverket?

Basert på våre vurderinger er det vår samlede konklusjon at kommunen ikke i tilstrekkelig grad har implementert personvernregelverket på alle områder.

Vi legger til grunn at kommunen har fått på plass flere elementer som er viktig i arbeidet med implementering av personvernregelverket, men funnene våre viser også at kommunen på flere områder har en jobb å gjøre.

Kommunen har en personvernerklæring som informerer brukerne av kommunens tjenester skriftlig, om behandlingen av personopplysninger. Kommunen gir imidlertid ikke tilstrekkelig informasjon om hvilke kategorier opplysninger som innhentes, hvor opplysningene hentes fra, hva som er formålet med behandlingen og hvor lenge de lagres. Kommunen gir informasjon på en kort og forståelig måte for mange av kommunens brukergrupper, informasjonen er imidlertid ikke i tilstrekkelig grad tilpasset alle målgrupper, som barn og unge. Det er også vår konklusjon at personvernerklæringen ikke er så lett tilgjengelig for brukerne av kommunens tjenester

Personvernerklæringen som brukere skal lese og samtykke til i kommunens skjemaløsning er ikke oppdatert til gjeldende personvernregelverk. Flere av kommunes skjemaer, hvor det skal og kan legges inn sensitive personopplysninger er usikret og informerer ikke om personvernet.

Videre har vi funnet at kommunen ivaretar personers rettigheter til innsyn, retting og sletting av opplysninger, samt overføring av opplysninger til en annen behandlingsansvarlig. Kommunens bruk og behandling av kameraovervåking er i henhold til retningslinjene.

Skolens praksis for å innhente samtykke er i tråd med Datatilsynets anbefalinger om at virksomheten bør ha en årlig rutine som sikrer at et gyldig samtykke er gitt. Det er vår oppfatning at dette ikke er en felles rutine for alle virksomhetene i kommunen, som for eksempel for barnehagene.

Kommunen har utarbeidet flere rutiner og retningslinjer på personvernområdet som er egnet til å ivareta personvernet når de blir implementert. Det er imidlertid behov for å rydde i begrepsbruken i rutinene mm. Begrepene informasjonssikkerhet, sikkerhet, IT sikkerheten og personvernet brukes litt overlappende. Det gjør det vanskelig for ansatte i organisasjonen å forstå hva som ligger til deres oppgaveområde og hva de ulike rutinene skal ivareta. Videre har kommunen ikke oppdatert prosedyrene og rutinene knyttet til organiseringen av sikkerhetsarbeidet i henhold til dagens organisering.

Kommunen har en behandlingsprotokoll i Risk Manager og har ført inn noen få behandlinger. Det er imidlertid en rekke behandlinger av personopplysninger, som kommunen ennå ikke har ført i protokollen.

De fleste av kommunens ledere har tenkt gjennom formålet med de personopplysninger de samler inn i virksomheten, og ser til at det kun samles inn personopplysninger som er relevante for formålet. Kommunen gjør en vurdering av om de innsamlede opplysningen i hvert tilfelle er adekvate, relevante og begrenset til formålet, der formålene er definert. Kommunen har imidlertid ikke i tilstrekkelig grad etablert en felles forståelse for hva som er å regne som personopplysninger og hva som ligger i begrepet behandling av personopplysninger. Det er ikke gjennomført en systematisk vurdering av de ulike formålene og de ulike kategoriene personopplysninger som samles inn i kommunen.

Personopplysninger som ikke er arkivpliktige skal slettes når formålet med at de ble lagret ikke lenger er oppfylt. Kommunen gjør vurderinger av hvilke personopplysninger som skal lagres og hvor lenge det skal lagres på mange områder. Det er imidlertid behov for veiledning og en gjennomgang i virksomhetene (skoler og barnehager) på hvilke personopplysninger som kan lagres, hvordan de skal lagres og til hvilket formål. Vi legger til at flere fagområder, eksempelvis skole og barnehage i langt mindre grad enn på helseområdet har fått bistand fra sentrale myndigheter til å etablere systemer for sikker lagring.

Kommunen sørger for tilgangskontroll og avgrensing av tilganger til ulike personopplysninger i sine systemer.

Kommunens rutiner for bruk av ulike kommunikasjonskanaler tar i for liten grad opp i seg flere vurderinger knyttet til personvern.

Kommunen har et personvernombud. Kommunen har opplyst om hvem som er personvernombud og kontaktopplysningene til personvernombudet både på sine nettsider og til Datatilsynet. Det er imidlertid ikke tydelig for kommunens ledere og virksomhetene hva som er deres oppgaver og hva som er personvernombudets oppgaver på ulike områder i arbeidet med regelverket. Det er vår oppfatning at slik oppgavene og forventningene til personvernombudet fremstilles på revisjonens tidspunkt, er ikke dette forenelig med den ressursen som er satt av for å ivareta oppgavene.

Personvernombudet rapporter til høyeste administrative nivå i kommunen. Kommunedirektøren leder sikkerhetsutvalget hvor saker skal legges frem og følges opp. Det er imidlertid vår vurdering at kommunen ikke har lagt til rette for at dette utvalget fungerer slik det er tenkt på området personvern.

Kommunen har gjennomført risikovurderinger av mange av systemene som kommunen benytter til å behandle personopplysninger. Det er imidlertid ikke gjennomført risikovurderinger/vurderinger av personvernkonsekvensene (DPIA) av alle behandlingene, der det kreves at det skal gjøres slike vurderinger i kommunen.

Kommunen har ikke gjennomført de årlige revisjonene (internkontroll) på personvernområdet, jf også egen rutine om dette. Det foreligger derfor ikke rapporter eller referater som viser resultatene av slike gjennomganger. Kommunen har ikke innhentet kunnskap om personopplysninger behandles etter personvernregelverket i kommunen ved bruk av slike gjennomganger.

Kommunen har etablert et avvikssystem der det også kan meldes avvik på personvernregelverket. Kommunen melder avvik til Datatilsynet, når det er behov for det.

Det er gjennomført opplæring på personvernregelverket, for å sette ansatte i stand til å ivareta kravene i regelverket. Opplæringen har imidlertid ikke vært tilstrekkelig eller konkret nok for mange ansatte i kommunen. Virksomhetene har heller ikke i tilstrekkelig grad etterspurt ytterligere opplæring fra personvernombudet.

Kommunen har en oversikt over de databehandlerne de benytter, og at de utarbeider databehandleravtaler med disse. Kommunen har også vurdert hvilke opplysninger som databehandlerne krever, om de er adekvate, relevante og begrenset for formålet.

Basert på våre vurderinger anbefaler vi at kommunen bør:

- sørge for å gi de registrerte informasjon om behandlingen av personopplysninger, herunder kategoriene personopplysninger, hvor opplysningene hentes fra, hva som er formålet med behandlingen og hvor lenge de lagres

- vurdere å gi informasjon om behandlingen av personopplysninger og personers rettigheter som i større grad er tilpasset og forståelig også for barn og unge
- utarbeide en oversikt og føre protokoll over de ulike behandlingene av personopplysninger i kommunen, hvordan og hvor opplysningene lagres, når de skal slettes, og hvordan personopplysningene brukes og hva som er formålet
- gjennomføre risikovurderinger av personvernkonsekvens DPIA, der det er nødvendig
- oppdatere personvernerklæringene i de digitale skjemaløsningene til gjeldende regelverk, sørge for at sensitive personopplysninger ikke kan føres i åpne skjemaløsninger og informere om personvernet der det skal eller kan føres sensitive personopplysninger.
- tydeliggjøre hva som er de ulike rollene i kommunen sitt ansvar i arbeidet med personvern og vurdere personvernets tilgjengelige ressurser i forhold til pålagte oppgaver og forventning
- oppdatere prosedyrer og rutiner knyttet til sikkerhetsorganiseringen i kommunen, slik at disse er i tråd med dagens sikkerhetsorganisering.
- vurdere å synliggjøre personvernregelverkets krav i større grad i rutiner og prosedyrer som berører personvern
- se til at det er et fungerende system for rapportering fra personvernombudet til kommunens øverste leder, enten gjennom kommunens sikkerhetsutvalg eller på annen måte
- iverksette et system for å innhente informasjon i virksomhetene for å vurdere om personvernregelverket etterleves og iverksette tiltak der det er nødvendig (internkontroll)
- gi mer tilgjengelig og målrettet opplæring til ansatte i organisasjonen på personvernregelverket

Rolvsøy, 27. mai 2020

Unn Elisabeth West
forvaltningsrevisor

Lene Brudal
oppdragsansvarlig revisor

4 KOMMUNEDIREKTØRENS UTTALELSE

FREDRIKSTAD KOMMUNE

ØSTRE VIKEN KOMMUNEREVISJON IKS

Råkollveien 103

1664 ROLVSØY

Unntatt offentlighet: Off.loven § 5, 1. ledd

Deres referanse	Vår referanse	Klassering	Dato
	2019/22243-11-114903/2020-EGOL	210	27.05.2020

Kommunedirektørens tilsvar til forvaltningsrevisjon på området personvern – GDPR

Generelt om rapporten
Forvaltningsrevisjonsrapporten er en viktig rapport som Fredrikstad kommune kan legge til grunn for forbedrings- og utviklingsarbeid for personvern. Det er tilfredsstillende å se det grundige arbeidet som ligger til grunn for rapporten. Vi ser at en del fungerer bra, og at vi samtidig har områder med forbedringspotensial. Kommunedirektøren finner det positivt at rapporten viser at Fredrikstad kommune har en tilfredsstillende organisasjon og rutiner på området. Dette viser at ansvaret tas på alvor i kommunen.

Med utgangspunkt i rapporten, kan forbedringsarbeidet i hovedsak konkretiseres til:
- styringssystemet
- dokumentasjonen
- opplæring.

I det følgende kommenterer kommunedirektøren noen funn i rapporten med vurderinger og forslag til tiltak:

Personvernerklæring
Revisjonen avdekker at kommunen ikke gir tilstrekkelig informasjon om hvilke kategorier av opplysninger som innhentes, hvor opplysningene hentes fra, hva som er formålet med behandlingen og hvor lenge de lagres. Videre at denne informasjonen ikke er lett tilgjengelig for brukere av kommunens tjenester.

Tiltak:
Det iverksettes gjennomgang av Personvernerklæringen, samt av hvorledes informasjonen om dette er tilrettelagt.

Seksjon for økonomi og organisasjonsutvikling
Besøksadresse: Nygaardsgt. 16, 1606 Fredrikstad
E-postadresse: postmottak@fredrikstad.kommune.no
Telefon: 69 30 60 00 Org.nr: 940039541
Postadresse: Postboks 1405, 1602 FREDRIKSTAD
Webadresse: www.fredrikstad.kommune.no
Tlf. saksbeh.: 69 30 62 26 Bankkonto: 5122 05 77000

Samtykke
Skolens praksis for å innhente samtykke er i tråd med Datatilsynets anbefalinger om at virksomheten bør ha en årlig rutine som sikrer at et gyldig samtykke er gitt. Det er revisjonens oppfatning at dette ikke er en felles rutine for alle virksomhetene i kommunen, som for eksempel for barnehagene.

Tiltak:
Personvernombudet starter et arbeid for å optimalisere rutinene for samtykkeerklæringer.

Begrepsbruk/rutiner
Revisjonen påpeker at det er etablert en rekke rutiner og retningslinjer, men at det er behov for å rydde i dokumentasjonen og begrepsbruken.

Tiltak:
Det er for tiden arbeid i gang med å optimalisere styringssystemet samt gjennomgå dokumentasjonshierarkiet. Dette gjelder spesielt avgrensningene mellom de konkrete personvernrutinene og de teknologiske rutinene.

Behandlingsprotokoll
Kommunen har en behandlingsprotokoll i Risk Manager og har ført inn noen få behandlinger. Det er imidlertid en rekke behandlinger av personopplysninger, som kommunen ennå ikke har ført i protokollen.

Tiltak:
Det er iverksatt arbeid med å forbedre systemet for behandlinger. Det vurderes etablering av en egen database. Samtidig vil det bli gjennomført risikovurderinger/vurderinger av personvernkonsekvensene (DPIA) av alle behandlingene.

Generell lagring av Personopplysninger
Kommunen har ikke i tilstrekkelig grad etablert en felles forståelse for hva som er å regne som personopplysninger og hva som ligger i begrepet behandling av personopplysninger. Det er ikke gjennomført en systematisk vurdering av de ulike formålene og de ulike kategoriene personopplysninger som samles inn i kommunen.

Tiltak:
På samme måte som under punktet om behandlingsprotokoll, iverksettes arbeid med en systematisk vurdering av hensikten med datalagringen. Herunder også rutiner for bistand til virksomheter.

Årlige revisjoner (internkontroll)
Kommunen har ikke gjennomført de årlige revisjonene (internkontroll) på personvernområdet, jf. også egen rutine for dette.

Tiltak:
Personvernombudet iverksetter årlige revisjoner.

Opplæring
Det er gjennomført opplæring på personvernregelverket, for å sette ansatte i stand til å ivareta kravene i regelverket. Opplæringen har imidlertid ikke vært tilstrekkelig eller konkret nok for mange ansatte i kommunen. Virksomhetene har heller ikke i tilstrekkelig grad etterspurt ytterligere opplæring fra personvernombudet.

Kommunen har et personvernombud. Kommunen har opplyst hvem som er personvernombud og kontaktopplysningene til personvernombudet både på sine nettsider og

til Datatilsynet. Det er imidlertid ikke tydelig for kommunens ledere og virksomhetene hva som er deres oppgaver og hva som er personvernombudets oppgaver på ulike områder i arbeidet med regelverket. Det er revisjonens oppfatning at slik oppgavene og forventningene til personvernombudet fremstilles på revisjonens tidspunkt, er ikke dette forenelig med den ressursen som er satt av for å ivareta oppgavene.

Tiltak:
Det skal etableres rutiner for bedret opplæring og informasjon, spesielt for ledere. Herunder også bedre rutiner der både interne og eksterne brukere får bedre kjennskap til *personvernombudet* og dennes ansvar og rutiner.

Sluttkommentar
Kommunedirektøren mener det er viktige funn som framkommer i revisjonsrapporten og vil følge dette opp med ulike tiltak i organisasjonen, blant annet som beskrevet ovenfor. Rapporten vil anvendes som en tiltaksliste i forbedringsarbeidet.

Avslutningsvis vil kommunedirektøren kommentere at Seksjon for utdanning og oppvekst etter denne forvaltningsrevisjonen, har utarbeidet en egen personvernerklæring for barn, skrevet på det registrerte barnets eget språk. Denne ligger nå ute på Fredrikstad kommune sin nettside, under *Barn, familie og utdanning*.

Personvernombudet samarbeider mye på fylkes- og landsnivå. Målet er å lette på personvernutfordringene i kommunene. Gjennom Digi Viken Øst – *DVØ fagnettverk informasjonssikkerhet*, *DVØ fagnettverk personvern* og *KS sitt strategiske nettverk for informasjonssikkerhet og personvern i kommunal sektor* drar vi veksler på hverandres kompetanse og vil utarbeide felles verktøy for å gjøre personvernarbeidet mer effektivt, med mindre risiko. Samlet kan vi blant annet stille større krav til at digitale verktøy i kommunal sektor har mer innebygd personvern og sikkerhet. Fredrikstad kommune samarbeider også med Utdanningsdirektoratet for å få på plass flere sentrale verktøy for å lette jobben med behandling av personopplysninger i skolen, slik at det i framtiden kun blir lokale tilpassinger som skal til for å fylle kravene i behandlingen.

Med hilsen

Dette dokumentet er elektronisk godkjent og sendes uten signatur

Nina Tangnæs Grønvold
kommunedirektør

5 DOKUMENTLISTE

Følgende dokumenter ligger til grunn for faktadelen i rapporten:
Dokumenter mottatt fra Fredrikstad kommune

- 1 E-post - prosedyren for bruk av e-post, godkjent 9.12.2019
- Innsyn i e-post og annet elektronisk materiale, godkjent 9.12.2019
- Skjema for innsyn i e-post og annet elektronisk materiale, godkjent 17.12.2018
- Adgang til utstyr, godkjent 17.12.2018
- Avvik personvern, godkjent 2.06.2019
- Daglig ansvarlig – informasjonssikkerhet (myndighet og ansvar), gyldig fra 16.04.2012, revideres innen 31.01.2013
- Innsynsbegjæring, godkjent 25.06.2019
- Digitaliseringssjefens ansvar og myndighetsområde, godkjent 20.05.2019
- Kameraovervåkning, godkjent 17.12.2018
- Skjema for utlevering av kameraopptak, godkjent 17.12.2018
- Låserutiner og adgangskontroll, godkjent 17.12.2018
- Organisasjonskart 2019
- Organisering av personvern- og informasjons-sikkerhetsarbeidet, godkjent 20.05.2019
- Personvernerklæring, godkjent 17.12.2018
- Passord (tilgangsbegrensning), gyldig fra 13.04.2012
- Retningslinjer for lagring på eksterne nettsteder – Fildelingstjenester, gyldig fra 2.10.2018
- Retningslinjer for personvern og informasjonssikkerhet – ansatte, godkjent 4.04.2019
- Retting og sletting av personopplysninger, godkjent 17.12.2018
- Risikovurdering informasjonssikkerhet og personvern, godkjent 2.06.2019
- Rutine for elektroniske plattformkurs, godkjent - udatert
- Signering av retningslinjer for ansatte, godkjent 4.04.2019
- Sikkerhetsleder- Personvernombud – stillingsbeskrivelse, godkjent 17.12.2018
- Mål for personvern og informasjonssikkerhet, godkjent 9.12.2019
- Taushetsplikt, godkjent 9.12.2019
- Etiske prinsipper – PowerPoint, 23.03.2017
- NOTAT – Oppgaver og fremdrift GDPR 2018/2019, udatert
- PowerPoint – Ny personvernlov GDPR til LA – 2018, 15.02.2018
- Rundskriv nr 3 – 2018 om GDPR distribuert 050618
- Rådmannsinnlegg på LUP 5.09.2018
- Revidert handlingsplan 2019-2022 og budsjett 2019, vedtatt av bystyret 6.12.2018
- E-post fra personvernombudet 5.12.2019
- Arkiveringsrutine for facebook og andre sosiale medier, godkjent 13.08.2019
- Retningslinjer for konflikthåndtering, godkjent 2.09.2019
- Saksbehandling i personalsaker som kan få arbeidsrettslige følger – arbeidstakers forhold, datert 14.11.2019

.
Dokumenter (digitale) fra kommunens hjemmeside:

- Personvernerklæring Fredrikstad kommune – skrevet ut 9.12.2019
- Innsynsbegjæring
- «Personvern og cookies» fra hjemmesiden
- Personvernavtalen knyttet til digitale søknader, skrevet ut 09.12.2019
- Henvisningskjema til fysio- og ergoterapitjenester, skrevet ut 09.12.2019

Systemgjennomsyn i kommunens lokaler:

- Risk Manager

o Meldinger om brudd på personvernregelverket per xxx

o Protokoll over behandlingsaktiviteter i Fredrikstad kommune per xxx

Fra skole

- Oversikt over ansatte med lederfunksjoner ved skolen med ansvar og oppgaver
- Oversikt over merkantilt ansatte ved skolen med oppgaver
- Oversikt over digitale plattformer skolen benytter
- Rutiner for innhenting og registrering av elevopplysninger, inkludert type opplysning (kategorier)
- Beskrivelse av rutiner ved fotografering og filming av elever i skolens regi.
- Rutiner for utlevering og/eller digital utsending av elevlister og elevopplysninger
- Beskrivelse av rutiner for arkivering og lagring av elevopplysninger
- Databehandleravtale – SKOOLER
- Databehandleravtale – VIGILO (både for skole og barnehage)

Fra barnehage

- Beskrivelse av ansatte med lederfunksjoner i barnehagen - ansvar og oppgaver
- Oversikt over digitale plattformer i barnehagen
- Beskrivelse av arkivering og lagring av dokumenter
- Rutine for håndtering av barnehagesøknader fra Vigilo
- Oppstart barnehage. Samtykke hjem - barnehage.
- Overgang barnehage - skole.
- Overføring av opplysninger fra barnehage til skole
- Overføring av dokumenter fra barnehage til barnehage

6 VEDLEGG

1. Utledning av revisjonskriterier
2. Definisjoner og begreper
3. Spørsmål i Questback – ledere
4. Spørsmål i Questback – rektorer, styrere, lærere og barnehagelærere

Vedlegg 1 - Utledning av revisjonskriterier

Utledning av revisjonskriteriene

Regelverk og veiledninger, som ligger til grunn for utledning av revisjonskriteriene er

Lov og forskrift

- Lov om behandling av personopplysninger (personopplysningsloven - popplyl), LOV-2018-06-15-38
- EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR]'
- Forskrift om kameraovervåking i virksomhet, FOR-2018-07-02-1107
- Prop. 56 LS (2017-2018)

Veiledninger og føringer

- https://www.datatilsynet.no/ - veiledninger på personvernregelverket
- *Personvern, taushetsplikt og meldeplikt – Regelverk for skolen*, Pedlex, ISBN: 978-82-8372-140-9
- *Personvern i skole og barnehage*, samlerapport juni 2014 – Datatilsynet
- *Veiledning om kontroll og overvåking i arbeidslivet – Arbeidstilsynet – Datatilsynet – Petroliumstilsynet og Partene i arbeidslivet*

Ved utøvelse av offentlig myndighet - samtykke

Offentlige myndigheters behandling av personopplysninger er i personvernforordningens fortale punkt 43 tatt frem som eksempel på et tilfelle der det kan være en skjevhet mellom den behandlingsansvarlige og den registrerte. Det kan føre til at det er usannsynlig at samtykket er avgitt frivillig blant annet med tanke på den registrertes behov for tjenester fra kommunen. For å kunne bruke samtykke som behandlingsgrunnlag må en gjøre en vurdering av om samtykket kan være frivillig for å kunne motta tjenestene eller for saksbehandlingen. Dersom samtykke ikke kan anses å være frivillig, er det ikke adgang til å bruke samtykke som behandlingsgrunnlag. I vurderingen må det tas hensyn til skjevheten mellom den behandlingsansvarlige og den registrerte, og eventuelle negative konsekvenser ved ikke å samtykke.

I personvernforordningens fortale punkt 42 står det samtykke ikke er å anse som frivillig dersom det ikke er reell valgfrihet, heller ikke dersom det å nekte samtykke er til skade for den registrerte. Kommunen må derfor i det enkelte tilfelle vurdere om det er aktuelt å benytte samtykke som behandlingsgrunnlag ved utøvelse av offentlig myndighet.

Behandling av personopplysninger

GDPR

Artikkel 5.Prinsipper for behandling av personopplysninger

«1. Personopplysninger skal

a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),

b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenlig med de opprinnelige formålene («formålsbegrensning»),

c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),

d) være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),

e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),

f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»).

2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar»).»

Veiledning fra Datatilsynet:

Datatilsynet sier i sin veiledning at selv om fødselsnummer ikke er å regne som sensitive personopplysninger, skal det sikres dersom det sendes per brev, e-post eller sms. Datatilsynet er i utgangspunktet ikke positive til at personopplysninger sendes på e-post. Dette fordi e-post er en «åpen» løsning og faren for feilsendelse i tillegg er stor. Dersom det er nødvendig å sende personopplysninger på e-post, så skal innholdet i e-post være kryptert.

Artikkel 6. Behandlingens lovlighet

«1. Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,

b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,

c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,

d) behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,

e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt, ……»

……

Formålet med behandlingen skal være fastsatt i nevnte rettslige grunnlag eller, når det gjelder behandlingen nevnt i nr. 1 bokstav e), være nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt. Nevnte rettslige grunnlag kan inneholde særlige bestemmelser for å tilpasse anvendelsen av reglene i denne forordning, blant annet de generelle vilkårene som skal gjelde for lovligheten av den behandlingsansvarliges behandling, hvilken type opplysninger som skal behandles, berørte registrerte, enhetene som personopplysningene kan utleveres til, og formålene med dette, formålsbegrensning, lagringsperioder samt behandlingsaktiviteter og framgangsmåter for behandling, herunder tiltak for å sikre lovlig og rettferdig behandling, slik som dem fastsatt med henblikk på andre særlige behandlingssituasjoner som nevnt i kapittel IX. Unionsretten eller medlemsstatenes nasjonale rett skal oppfylle et mål i allmennhetens interesse og stå i et rimelig forhold til det berettigede målet som søkes oppnådd.

4. Dersom behandlingen for et annet formål enn det som personopplysningene er blitt samlet inn for, ikke bygger på den registrertes samtykke eller på unionsretten eller medlemsstatenes nasjonale rett som utgjør et nødvendig og forholdsmessig tiltak i et demokratisk samfunn for å sikre oppnåelse av målene nevnt i artikkel 23 nr. 1, skal den behandlingsansvarlige for å avgjøre om behandlingen for et annet formål er forenlig med formålet som personopplysningene opprinnelig ble samlet inn for, blant annet ta hensyn til følgende:

a) enhver forbindelse mellom formålene som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen,

b) i hvilken sammenheng personopplysningene er blitt samlet inn, særlig med hensyn til forholdet mellom de registrerte og den behandlingsansvarlige,

c) personopplysningenes art, især om særlige kategorier av personopplysninger behandles, i henhold til artikkel 9, eller om personopplysninger om straffedommer og lovovertredelser behandles, i henhold til artikkel 10,

d) de mulige konsekvensene av den tiltenkte viderebehandlingen for de registrerte,

e) om det foreligger nødvendige garantier, som kan omfatte kryptering eller pseudonymisering.

Artikkel 9. Behandling av særlige kategorier av personopplysninger

«1. Behandling av personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, er forbudt.

2. Nr. 1 får ikke anvendelse dersom et av følgende vilkår er oppfylt:

a) Den registrerte har gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål, unntatt dersom det i unionsretten eller medlemsstatenes nasjonale rett er fastsatt at den registrerte ikke kan oppheve forbudet nevnt i nr. 1.

b) Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser.

c) Behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser dersom den registrerte fysisk eller juridisk ikke er i stand til å gi samtykke.

d) …

e) Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort.

f) Behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav eller når domstolene handler innenfor rammen av sin domsmyndighet.

g) Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.

h) Behandlingen er nødvendig i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller sosialtjenester, behandling eller forvaltning av helse- eller sosialtjenester og -systemer på grunnlag av unionsretten eller medlemsstatenes nasjonale rett eller i henhold til en avtale med helsepersonell og med forbehold for vilkårene og garantiene nevnt i nr. 3.

i) Behandlingen er nødvendig av allmenne folkehelsehensyn, f.eks. vern mot alvorlige grenseoverskridende helsetrusler eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester og legemidler eller medisinsk utstyr, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett der det fastsettes egnede og særlige tiltak for å verne den registrertes rettigheter og friheter, særlig taushetsplikt.

j) Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.

3. Personopplysningene nevnt i nr. 1 kan behandles for formålene nevnt i nr. 2 bokstav h) dersom opplysningene behandles av en fagperson som har taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett eller regler fastsatt av nasjonale vedkommende organer, eller under en slik persons ansvar, eller av en annen person som også har taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett eller regler fastsatt av nasjonale vedkommende organer.

4. Medlemsstatene kan opprettholde eller innføre ytterligere vilkår, herunder begrensninger, med hensyn til behandling av genetiske opplysninger, biometriske opplysninger eller helseopplysninger.»

a) Personopplysningsloven

b) Popplyl § 6. Behandling av særlige kategorier av personopplysninger i arbeidsforhold

«Personopplysninger som nevnt i personvernforordningen artikkel 9 nr. 1 kan behandles når det er nødvendig for å gjennomføre arbeidsrettslige plikter eller rettigheter.»

Popplyl § 12. Bruk av fødselsnummer og andre entydige identifikasjonsmidler

«Fødselsnummer og andre entydige identifikasjonsmidler kan bare behandles når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.»

Datatilsynet sier i sin veiledning at selv om fødselsnummer ikke er å regne som sensitive personopplysninger, skal det sikres dersom det sendes per brev, e-post eller sms. Datatilsynet er i utgangspunktet ikke positive til at personopplysninger sendes på e-post. Dette fordi e-post er en «åpen» løsning og faren for feilsendelse i tillegg er stor. Dersom det er nødvendig å sende personopplysninger på e-post, så skal innholdet i e-post være kryptert.

Popplyl § 31. Uekte kameraovervåkingsutstyr mv.

«Når kameraovervåking vil være i strid med personvernforordningen eller loven her, er det heller ikke tillatt å benytte uekte kameraovervåkingsutstyr eller ved skilting, oppslag eller lignende gi inntrykk av at kameraovervåking finner sted. Personvernforordningen kapittel VI og artikkel 83 nr. 4 samt kapittel 6, § 26 annet ledd og §§ 27 til 29 i loven her gjelder tilsvarende.

Med kameraovervåking menes vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkingskamera eller annet lignende utstyr som er fastmontert. Med uekte kameraovervåkingsutstyr menes utstyr som lett kan forveksles med en ekte kameraløsning.»

Vilkår for samtykke til behandling av personopplysninger

GDPR

Artikkel 7.Vilkår for samtykke

«1. Dersom behandlingen bygger på samtykke, skal den behandlingsansvarlige kunne påvise at den registrerte har samtykket til behandling av personopplysninger om vedkommende.

2. Dersom den registrertes samtykke gis i forbindelse med en skriftlig erklæring som også gjelder andre forhold, skal anmodningen om samtykke framlegges på en måte som gjør at den tydelig kan skilles fra nevnte andre forhold, i en forståelig og lett tilgjengelig form og på et klart og enkelt språk. Deler av en slik erklæring som er i strid med denne forordning, skal ikke være bindende.

3. Den registrerte skal ha rett til å trekke tilbake sitt samtykke til enhver tid. Dersom samtykket trekkes tilbake, skal det ikke påvirke lovligheten av behandlingen som bygger på samtykket før det trekkes tilbake. Før det gis samtykke, skal den registrerte opplyses om dette. Det skal være like enkelt å trekke tilbake som å gi samtykke.

4. Ved vurdering av om et samtykke er gitt frivillig skal det tas størst mulig hensyn til blant annet om oppfyllelse av en avtale, herunder om yting av en tjeneste, er gjort betinget av samtykke til behandling av personopplysninger som ikke er nødvendig for å oppfylle nevnte avtale.»

Artikkel 8. Vilkår for barns samtykke i forbindelse med informasjonssamfunnstjenester

«1. Dersom artikkel 6 nr. 1 bokstav a) får anvendelse i forbindelse med tilbud om informasjonssamfunnstjenester direkte til et barn, er behandling av et barns personopplysninger lovlig dersom barnet er minst 16 år. Dersom barnet er under 16 år, er slik behandling lovlig bare dersom og i den grad samtykke er gitt eller godkjent av den som har foreldreansvar for barnet.

For disse formål kan medlemsstatene ved lov fastsette en lavere aldersgrense, forutsatt at den ikke er lavere enn 13 år.

2. I slike tilfeller skal den behandlingsansvarlige treffe rimelige tiltak for å kontrollere at samtykke er gitt eller godkjent av den som har foreldreansvar for barnet, idet det tas hensyn til tilgjengelig teknologi.

3. Nr. 1 skal ikke påvirke medlemsstatenes alminnelige avtalerett, f.eks. reglene for gyldigheten, utformingen eller virkningen av en avtale som gjelder et barn.»

Personopplysningsloven

Popplyl §§ 5.Barns samtykke i forbindelse med informasjonssamfunnstjenester

«Aldersgrensen er 13 år for samtykke etter personvernforordningen artikkel 6 nr. 1 bokstav a i forbindelse med formål som nevnt i personvernforordningen artikkel 8 nr. 1.»

Fra Datatilsynets veileder https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/samtykkje-fra-mindrearige/

«Hovudregelen er at mindreårige som er fylt 15 år, sjølv kan samtykke til innhenting og bruk av eigne personopplysningar. For barn som ikkje er blitt 15 år, må dei føresette samtykke på vegne av barnet.
Tre unnatak
Det er tre aktuelle unnatak frå denne hovudregelen:

(1) Sensitive personopplysningar skal berre innhentast med samtykke frå foreldra fram til barna har fylt 18 år. Sensitive opplysningar er blant anna opplysningar om helse, om etnisk bakgrunn, livssyn, og seksuelle forhold

(2) For småkonkurransar og liknande, der enkle kontaktopplysningar berre skal brukast til eventuell premiering og deretter slettast, kan også mindre barn enn 15-åringar samtykke til deltaking sjølv. Her er det likevel ein føresetnad at opplysningane blir sletta etter premiering, at personverntrusselen er vurdert og klassifisert som særs låg, og at konkurransen er eigna for den aktuelle aldersgruppa.

(3) Bruk av nettenester og appar slik som Facebook, Instagram og Snap, er særskilt regulert i personvernforordninga artikkel 8 (kalla informasjonssamfunnstenester i lovteksten). I Norge er aldersgrensa for å samtykke sjølv til bruk av denne typen tenester satt til 13 år. Dersom barnet er under 13 år, må dei foresatte samtykke til bruken av tenesta.

Kommunens ansvar og forpliktelser

GDPR

Artikkel 24. Den behandlingsansvarliges ansvar

«1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

2. Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger.

3. Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller godkjente sertifiseringsmekanismer som nevnt i artikkel 42 kan brukes som en faktor for å påvise at den behandlingsansvarliges forpliktelser overholdes.»

Artikkel 25. Innebygd personvern og personvern som standardinnstilling

«1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.

2. Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.

3. En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.»

Artikkel 28. Databehandler

«1. Dersom en behandling skal utføres på vegne av en behandlingsansvarlig, skal den behandlingsansvarlige bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter.

2. Databehandleren skal ikke engasjere en annen databehandler uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den behandlingsansvarlige. Dersom det er innhentet en generell skriftlig tillatelse, skal databehandleren underrette den behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer.

3. Behandling utført av en databehandler skal være underlagt en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett som er bindende for databehandleren med hensyn til den behandlingsansvarlige, og der gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt. I nevnte avtale eller nevnte andre rettslige dokument skal det særlig angis at databehandleren

a) behandler personopplysningene bare på dokumenterte instrukser fra den behandlingsansvarlige, herunder med hensyn til overføring av personopplysninger til en tredjestat eller en internasjonal organisasjon, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt; i så fall skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, men mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning,

b) sikrer at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene konfidensielt eller er underlagt en egnet lovfestet taushetsplikt,

c) treffer alle tiltak som er nødvendig i henhold til artikkel 32,

d) overholder vilkårene nevnt i nr. 2 og 4 når det gjelder å engasjere en annen databehandler,

e) idet det tas hensyn til behandlingens art og i den grad det er mulig, bistår, ved hjelp av egnede tekniske og organisatoriske tiltak, den behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i kapittel III,

f) bistår den behandlingsansvarlige med å sikre overholdelse av forpliktelsene i henhold til artikkel 32-36, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren,

g) etter den behandlingsansvarliges valg, sletter eller tilbakeleverer alle personopplysninger til den behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert, og sletter eksisterende kopier, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at personopplysningene lagres,

h) gjør tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne artikkel er oppfylt, samt muliggjør og bidrar til revisjoner, herunder inspeksjoner, som gjennomføres av den behandlingsansvarlige eller en annen revisor på fullmakt fra den behandlingsansvarlige.

Når det gjelder første ledd bokstav h) skal databehandleren omgående underrette den behandlingsansvarlige dersom vedkommende mener at en instruks er i strid med denne forordning eller andre bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett……..

5. En databehandlers overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i artikkel 42 kan brukes som en faktor for å påvise at det foreligger tilstrekkelige garantier som nevnt i nr. 1 og 4 i denne artikkel.

6. Uten at det berører en individuell avtale mellom den behandlingsansvarlige og databehandleren, kan avtalen eller det andre rettslige dokumentet nevnt i nr. 3 og 4 i denne artikkel helt eller delvis bygge på standardavtalevilkårene nevnt i nr. 7 og 8 i denne artikkel, herunder når de inngår i en sertifisering som er gitt den behandlingsansvarlige eller databehandleren i henhold til artikkel 42 og 43……..

9. Avtalen eller det andre rettslige dokumentet nevnt i nr. 3 og 4 skal være skriftlig, herunder elektronisk……..»

Artikkel 29. Behandling som utføres for den behandlingsansvarlige eller databehandleren

«Databehandleren og enhver person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, skal behandle nevnte opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett.»

Artikkel 30. Protokoller over behandlingsaktiviteter

«1. Hver behandlingsansvarlig og, dersom det er relevant, den behandlingsansvarliges representant skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Nevnte protokoll skal inneholde følgende informasjon:

a) navnet på og kontaktopplysningene til den behandlingsansvarlige og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet,

b) formålene med behandlingen,

c) en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger,

d) kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner,

e) dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier,

f) dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger,

g) dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1……..

3. Protokollene nevnt i nr. 1 og 2 skal være skriftlige, herunder elektroniske.

4. Den behandlingsansvarlige eller databehandleren og, dersom det er relevant, den behandlingsansvarliges eller databehandlerens representant skal på anmodning gjøre protokollen tilgjengelig for tilsynsmyndigheten……..»

Risikovurdering og internkontroll (vurdering av personvernkonsekvenser)

GDPR

Artikkel 35. Vurdering av personvernkonsekvenser

«1. Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.

2. Den behandlingsansvarlige skal rådføre seg med personvernombudet, dersom et personvernombud er utpekt, i forbindelse med utførelsen av en vurdering av personvernkonsekvenser.

3. En vurdering av personvernkonsekvenser som nevnt i nr. 1 skal særlig være nødvendig i følgende tilfeller:

a) en systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen,

b) behandling i stor skala av særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1, eller av personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10, eller

c) en systematisk overvåking i stor skala av et offentlig tilgjengelig område.

4. Tilsynsmyndigheten skal utarbeide og offentliggjøre en liste over hvilke typer behandlingsaktiviteter som omfattes av kravet om vurdering av personvernkonsekvenser i henhold til nr. 1. Tilsynsmyndigheten skal oversende nevnte lister til Personvernrådet nevnt i artikkel 68.

5. Tilsynsmyndigheten kan også utarbeide og offentliggjøre en liste over hvilke typer behandlingsaktiviteter det ikke kreves at det utføres en vurdering av personvernkonsekvenser for. Tilsynsmyndigheten skal oversende nevnte lister til Personvernrådet.

6. Før listene nevnt i nr. 4 og 5 godkjennes, skal vedkommende tilsynsmyndighet anvende konsistensmekanismen nevnt i artikkel 63 dersom slike lister omfatter behandlingsaktiviteter som gjelder tilbud av varer eller tjenester til registrerte eller monitorering av deres atferd i flere medlemsstater, eller som i betydelig grad kan påvirke den frie utveksling av personopplysninger i Unionen.

7. Vurderingen skal minst inneholde

a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige,

b) en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene,

c) en vurdering av risikoene for de registrertes rettigheter og friheter som nevnt i nr. 1, og

d) de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at denne forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser.

8. Det skal tas behørig hensyn til de berørte behandlingsansvarliges eller databehandleres overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 ved vurderingen av konsekvensene av behandlingsaktivitetene som utføres av nevnte behandlingsansvarlige eller databehandlere, særlig med henblikk på en vurdering av personvernkonsekvenser.

9. Dersom det er relevant, skal den behandlingsansvarlige innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representanter uten at det berører vernet av kommersielle eller allmenne interesser eller sikkerheten ved behandlingsaktivitetene.

10. Dersom behandling i henhold til artikkel 6 nr. 1 bokstav c) eller e) har et rettslig grunnlag i unionsretten eller retten i medlemsstaten som den behandlingsansvarlige er underlagt, og nevnte rett regulerer den eller de aktuelle spesifikke behandlingsaktivitetene, og det allerede er utført en vurdering av personvernkonsekvenser som en del av en generell konsekvensvurdering i forbindelse med vedtakelse av nevnte rettslige grunnlag, får nr. 1-7 ikke anvendelse, med mindre medlemsstatene anser det nødvendig å utføre en slik vurdering før behandlingsaktivitetene.

11. Ved behov skal den behandlingsansvarlige foreta en gjennomgåelse for å vurdere om behandlingen utføres i samsvar med vurderingen av personvernkonsekvenser, i det minste dersom risikoen som behandlingen medfører, endres.»

Datatilsynets liste over behandlingsaktiviteter som alltid krever at det gjennomføres en DPIA (vurdering av personvernkonsekvensene)

https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/

Artikkel 36. Forhåndsdrøftinger

«1. Den behandlingsansvarlige skal rådføre seg med tilsynsmyndigheten før behandlingen dersom en vurdering av personvernkonsekvenser i henhold til artikkel 35 tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen……»

Artikkel 32. Sikkerhet ved behandlingen

«1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

- *a) pseudonymisering og kryptering av personopplysninger,*
- *b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,*
- *c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,*
- *d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.*

2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

3. Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i artikkel 42 kan brukes som en faktor for å påvise at kravene i nr. 1 i denne artikkel er oppfylt.

4. Den behandlingsansvarlige og databehandleren skal treffe tiltak for å sikre at enhver fysisk person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, behandler nevnte opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at vedkommende gjør dette.»

Artikkel 33. Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten

«1.Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet i samsvar med artikkel 55, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis.

2. Etter å ha fått kjennskap til et brudd på personopplysningssikkerheten skal databehandleren uten ugrunnet opphold underrette den behandlingsansvarlige.

Meldingen nevnt i nr. 1 skal minst

c) beskrive arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,
d) inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes,
e) beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
f) beskrive de tiltak som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

4. Dersom og i den grad det ikke er mulig å gi all informasjon samtidig, kan den gis trinnvis uten ytterligere ugrunnet opphold.

5. Den behandlingsansvarlige skal 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. Denne dokumentasjonen skal gjøre det mulig for tilsynsmyndigheten å kontrollere samsvar med denne artikkel.»

Artikkel 34.Underretning av den registrerte om brudd på personopplysningssikkerheten

«1.Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet.

2.Underretningen til den registrerte nevnt i nr. 1 i denne artikkel skal inneholde en klar og tydelig beskrivelse av arten av bruddet på personopplysningssikkerheten og minst informasjonen og tiltakene nevnt i artikkel 33 nr. 3 bokstav b), c) og d).

3.Underretningen til den registrerte nevnt i nr. 1 er ikke påkrevd dersom noen av følgende vilkår er oppfylt:

1) den behandlingsansvarlige har gjennomført egnede tekniske og organisatoriske sikkerhetstiltak, og disse tiltakene er blitt anvendt på personopplysningene som er berørt av bruddet på personopplysningssikkerheten, særlig tiltak som gjør personopplysningene uleselige for enhver person som ikke har autorisert tilgang til dem, f.eks. kryptering,
2) den behandlingsansvarlige har truffet etterfølgende tiltak som sikrer at det ikke lenger er sannsynlig at den høye risikoen for de registrertes rettigheter og friheter nevnt i nr. 1 vil oppstå,
3) det vil innebære en uforholdsmessig stor innsats. Dersom dette er tilfellet, skal allmennheten isteden underrettes, eller det skal treffes et lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte.

4. Dersom den behandlingsansvarlige ikke allerede har underrettet den registrerte om bruddet på personopplysningssikkerheten, kan tilsynsmyndigheten, etter å ha vurdert sannsynligheten for at bruddet vil medføre en høy risiko, kreve at den behandlingsansvarlige gjør dette, eller beslutte at ett eller flere av vilkårene nevnt i nr. 3 er oppfylt.»

Den registrertes rettigheter

GDPR

Artikkel 12. Klar og tydelig informasjon, kommunikasjon og nærmere regler om utøvelse av den registrertes rettigheter

1. Den behandlingsansvarlige skal treffe egnede tiltak for å framlegge for den registrerte informasjonen nevnt i artikkel 13 og 14 og all kommunikasjon i henhold til artikkel 15-22 og 34 om behandlingen på en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk, især når det gjelder informasjon som spesifikt er rettet mot et barn. Informasjonen skal gis skriftlig eller på en annen måte, herunder elektronisk dersom det er hensiktsmessig. På anmodning fra den registrerte kan informasjonen gis muntlig, forutsatt at den registrertes identitet bevises på andre måter.

2. Den behandlingsansvarlige skal legge til rette for at den registrerte kan utøve sine rettigheter i henhold til artikkel 15-22. I tilfellene nevnt i artikkel 11 nr. 2 skal den behandlingsansvarlige ikke nekte å etterkomme den registrertes anmodning om å utøve sine rettigheter i henhold til artikkel 15-22, med mindre den behandlingsansvarlige påviser at vedkommende ikke er i stand til å identifisere den registrerte.

3. Den behandlingsansvarlige skal informere den registrerte om tiltak som er truffet på grunnlag av en anmodning i henhold til artikkel 15-22, uten ugrunnet opphold og senest én måned etter mottak av anmodningen. Denne fristen kan ved behov forlenges med ytterligere to måneder, idet det tas hensyn til antall anmodninger og anmodningenes kompleksitet. Den behandlingsansvarlige skal informere den registrerte om enhver slik forlengelse senest én måned etter mottak av anmodningen sammen med en begrunnelse for forsinkelsen. Dersom den registrerte inngir anmodningen elektronisk, skal informasjonen om mulig gis elektronisk, med mindre den registrerte anmoder om noe annet.

4. Dersom den behandlingsansvarlige ikke treffer tiltak på anmodning fra den registrerte, skal den behandlingsansvarlige informere den registrerte uten opphold og senest én måned etter mottak av anmodningen om årsakene til dette og om muligheten for å inngi klage til en tilsynsmyndighet og for rettslig prøving.

5. Informasjon som gis i henhold til artikkel 13 og 14, og enhver kommunikasjon og ethvert tiltak som treffes i henhold til artikkel 15-22 og 34, skal være gratis. Dersom anmodninger fra en registrert er åpenbart grunnløse eller overdrevne, særlig dersom de gjentas, kan den behandlingsansvarlige enten

a) kreve et rimelig gebyr, idet det tas hensyn til administrasjonskostnadene for å gi informasjonen eller treffe de tiltak det anmodes om, eller

b) nekte å etterkomme anmodningen.

Den behandlingsansvarlige skal bære bevisbyrden for at en anmodning er åpenbart grunnløs eller overdreven.

6. Uten at det berører artikkel 11, kan den behandlingsansvarlige, dersom det hersker rimelig tvil om identiteten til den fysiske personen som inngir anmodningen nevnt i artikkel 15-21, anmode om ytterligere opplysninger som er nødvendige for å kunne bekrefte den registrertes identitet.

7. Informasjonen som skal gis de registrerte i henhold til artikkel 13 og 14, kan gis sammen med standardiserte ikoner for å gi en lett synlig, forståelig, lettlest og meningsfull oversikt over den tiltenkte behandlingen. Dersom ikonene presenteres elektronisk, skal de være maskinlesbare……..»

Datatilsynet sier i sin veileder om informasjon og åpenhet *«…må virksomheten kommunisere på en kortfattet, åpen, forståelig og lett tilgjengelig måte. Språket skal være klart og enkelt, særlig når informasjonen er spesifikt rettet mot barn.»*

Artikkel 13. Informasjon som skal gis ved innsamling av personopplysninger fra den registrerte

«1. Når personopplysninger om en registrert samles inn fra den registrerte, skal den behandlingsansvarlige på tidspunktet for innsamlingen av personopplysningene gi den registrerte følgende informasjon:

a) identiteten og kontaktopplysningene til den behandlingsansvarlige og eventuelt den behandlingsansvarliges representant,

b) kontaktopplysningene til personvernombudet, dersom dette er relevant,

c) formålene med den tiltenkte behandlingen av personopplysningene samt det rettslige grunnlaget for behandlingen,

d) dersom behandlingen er basert på artikkel 6 nr. 1 bokstav f), de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart,

e) eventuelle mottakere eller kategorier av mottakere av personopplysningene,…….#

2. I tillegg til informasjonen nevnt i nr. 1 skal den behandlingsansvarlige på tidspunktet for innsamling av personopplysninger gi den registrerte følgende ytterligere informasjon som er nødvendig for å sikre en rettferdig og åpen behandling:

a) det tidsrom personopplysningene vil bli lagret, eller dersom dette ikke er mulig, kriteriene som brukes for å fastsette dette tidsrommet,

b) retten til å anmode den behandlingsansvarlige om innsyn i og retting eller sletting av personopplysninger eller begrensning av behandlingen som gjelder den registrerte, eller til å protestere mot behandlingen samt retten til dataportabilitet,

c) dersom behandlingen er basert på artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), retten til når som helst å trekke tilbake et samtykke uten at det påvirker lovligheten av en behandling basert på et samtykke før samtykket trekkes tilbake,

d) retten til å klage til en tilsynsmyndighet,

e) om det foreligger et lovfestet eller avtalefestet krav om å gi personopplysninger eller et krav som er nødvendig for å inngå en avtale, samt om den registrerte har plikt til å gi personopplysningene og om mulige konsekvenser dersom vedkommende ikke gjør det,

f) forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte.

3. Dersom den behandlingsansvarlige har til hensikt å viderebehandle personopplysningene for et annet formål enn det opplysningene ble samlet inn for, skal den behandlingsansvarlige før nevnte viderebehandling gi den registrerte informasjon om nevnte andre formål og annen nødvendig informasjon som nevnt i nr. 2.

4. Nr. 1, 2 og 3 får ikke anvendelse dersom og i den grad den registrerte allerede har informasjonen.»

Artikkel 14. Informasjon som skal gis dersom personopplysninger ikke er blitt samlet inn fra den registrerte

1. Dersom personopplysninger ikke er blitt samlet inn fra den registrerte, skal den behandlingsansvarlige gi den registrerte følgende informasjon:

a) identiteten og kontaktopplysningene til den behandlingsansvarlige og eventuelt den behandlingsansvarliges representant,

b) kontaktopplysningene til personvernombudet, dersom dette er relevant,

c) formålene med den tiltenkte behandlingen av personopplysningene samt det rettslige grunnlaget for behandlingen,

d) de berørte kategoriene av personopplysninger,

e) eventuelle mottakere eller kategorier av mottakere av personopplysningene,……

2. I tillegg til informasjonen nevnt i nr. 1 skal den behandlingsansvarlige gi den registrerte følgende informasjon som er nødvendig for å sikre den registrerte en rettferdig og åpen behandling:

a) det tidsrom personopplysningene vil bli lagret, eller dersom dette ikke er mulig, kriteriene som brukes for å fastsette dette tidsrommet,

b) dersom behandlingen er basert på artikkel 6 nr. 1 bokstav f), de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart,

c) retten til å anmode den behandlingsansvarlige om innsyn i og retting eller sletting av personopplysninger eller begrensning av behandlingen som gjelder den registrerte, og til å protestere mot behandlingen samt retten til dataportabilitet,

d) dersom behandlingen er basert på artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), retten til når som helst å trekke tilbake et samtykke uten at det påvirker lovligheten av en behandling basert på et samtykke før samtykket trekkes tilbake,

e) retten til å klage til en tilsynsmyndighet,

f) fra hvilken kilde personopplysningene stammer fra, og, dersom det er relevant, om de stammer fra offentlig tilgjengelige kilder,

g) forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte.

3. Den behandlingsansvarlige skal gi informasjonen nevnt i nr. 1 og 2

a) innen en rimelig frist etter at personopplysningene er samlet inn, men senest innen én måned, idet det tas hensyn til de særlige forholdene som personopplysningene er behandlet under,

b) dersom personopplysningene skal brukes til å kommunisere med den registrerte, senest på tidspunktet for den første kommunikasjonen med vedkommende, eller

c) dersom det er planlagt at personopplysningene skal utleveres til en annen mottaker, senest når personopplysningene første gang utleveres.

4. Dersom den behandlingsansvarlige har til hensikt å viderebehandle personopplysningene for et annet formål enn det opplysningene ble samlet inn for, skal den behandlingsansvarlige før nevnte viderebehandling gi den registrerte informasjon om nevnte andre formål og annen relevant informasjon som nevnt i nr. 2.

5. Nr. 1-4 får ikke anvendelse dersom og i den grad

a) den registrerte allerede har informasjonen,……..

c) innsamling eller utlevering er uttrykkelig fastsatt i unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt, og som inneholder egnede tiltak for å verne den registrertes berettigede interesser, eller

d) dersom personopplysningene må holdes konfidensielle som følge av taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett, herunder en lovfestet taushetsplikt.»

I veilederen som omhandler kontroll og overvåking i arbeidslivet, utarbeidet av Datatilsynet i samarbeid med Arbeidstilsynet, Petroleumstilsynet og partene i arbeidslivet,står det at det er et grunnleggende prinsipp at alle har krav på personvern og privatliv – også på jobb.

Artikkel 15. Den registrertes rett til innsyn

«1. Den registrerte skal ha rett til å få den behandlingsansvarliges bekreftelse på om personopplysninger om vedkommende behandles, og, dersom dette er tilfellet, innsyn i personopplysningene og følgende informasjon:

a) formålene med behandlingen,

b) de berørte kategoriene av personopplysninger,

c) mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, særlig mottakere i tredjestater eller internasjonale organisasjoner,

d) dersom det er mulig, hvor lenge det forventes at personopplysningene vil bli lagret, eller, dersom dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden,

e) retten til å anmode den behandlingsansvarlige om retting eller sletting av personopplysninger eller begrensning av behandlingen av personopplysninger som gjelder den registrerte, eller til å protestere mot nevnte behandling,

f) retten til å klage til en tilsynsmyndighet,

g) dersom personopplysningene ikke er samlet inn fra den registrerte, all tilgjengelig informasjon om hvor personopplysningene stammer fra,

h) forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte.

2. Dersom personopplysningene overføres til en tredjestat eller til en internasjonal organisasjon, skal den registrerte ha rett til å bli underrettet om de nødvendige garantiene i henhold til artikkel 46 i forbindelse med overføringen.

3. Den behandlingsansvarlige skal gjøre tilgjengelig en kopi av personopplysningene som behandles. Dersom den registrerte anmoder om flere kopier, kan den behandlingsansvarlige kreve et rimelig gebyr basert på administrasjonskostnadene. Dersom den registrerte inngir anmodningen elektronisk, og med mindre den registrerte anmoder om noe annet, skal informasjonen gis i en vanlig elektronisk form.

4. Retten til å motta en kopi nevnt i nr. 3 skal ikke ha negativ innvirkning på andres rettigheter og friheter.»

Artikkel 16. Rett til retting

«Den registrerte skal ha rett til å få uriktige personopplysninger om seg selv rettet av den behandlingsansvarlige uten ugrunnet opphold. Idet det tas hensyn til formålene med behandlingen skal den registrerte ha rett til å få ufullstendige personopplysninger komplettert, herunder ved å framlegge en supplerende erklæring.»

Artikkel 17. Rett til sletting («rett til å bli glemt»)

«1. Den registrerte skal ha rett til å få personopplysninger om seg selv slettet av den behandlingsansvarlige uten ugrunnet opphold, og den behandlingsansvarlige skal ha plikt til å slette personopplysninger uten ugrunnet opphold dersom et av de følgende forhold gjør seg gjeldende:

a) personopplysningene er ikke lenger nødvendige for formålet som de ble samlet inn eller behandlet for,

b) den registrerte trekker tilbake samtykket som ligger til grunn for behandlingen, i henhold til artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), og det ikke finnes noe annet rettslig grunnlag for behandlingen,

c) den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 1, og det ikke finnes mer tungtveiende berettigede grunner til behandlingen, eller den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 2,

d) personopplysningene er blitt behandlet ulovlig,

e) personopplysningene må slettes for å oppfylle en rettslig forpliktelse i unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt,

f) *personopplysningene er blitt samlet inn i forbindelse med tilbud om informasjonssamfunnstjenester som nevnt i artikkel 8 nr. 1.*

2. Dersom den behandlingsansvarlige har offentliggjort personopplysningene og i henhold til nr. 1 har plikt til å slette personopplysningene, skal vedkommende, idet det tas hensyn til tilgjengelig teknologi og gjennomføringskostnadene, treffe rimelige tiltak, herunder tekniske tiltak, for å underrette behandlingsansvarlige som behandler personopplysningene, om at den registrerte har anmodet om at nevnte behandlingsansvarlige skal slette alle lenker til, kopier eller reproduksjoner av nevnte personopplysninger.

3. Nr. 1 og 2 får ikke anvendelse dersom nevnte behandling er nødvendig

a) *for å utøve retten til ytrings- og informasjonsfrihet,*

b) *for å oppfylle en rettslig forpliktelse som krever behandling i henhold til unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt, eller for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,*

c) *av hensyn til allmennhetens interesse på området folkehelse i samsvar med artikkel 9 nr. 2 bokstav h) og i) og artikkel 9 nr. 3,……..*

e) *for å fastsette, gjøre gjeldende eller forsvare rettskrav.»*

Artikkel 18. Rett til begrensning av behandling

«1. Den registrerte skal ha rett til å kreve av den behandlingsansvarlige at behandlingen begrenses dersom et av de følgende forhold gjør seg gjeldende:

a) *den registrerte bestrider riktigheten av personopplysningene, i en periode som gjør det mulig for den behandlingsansvarlige å kontrollere riktigheten av personopplysningene,*

b) *behandlingen er ulovlig og den registrerte motsetter seg sletting av personopplysningene og isteden anmoder om at bruken av personopplysningene begrenses,*

c) *den behandlingsansvarlige ikke lenger trenger personopplysningene til formålet med behandlingen, men den registrerte har behov for disse for å fastsette, gjøre gjeldende eller forsvare rettskrav,*

d) *den registrerte har protestert mot behandling i henhold til artikkel 21 nr. 1 i påvente av kontrollen av om hvorvidt den behandlingsansvarliges berettigede grunner går foran den registrertes.*

2. Dersom behandlingen er blitt begrenset i henhold til nr. 1, skal slike personopplysninger, bortsett fra lagring, bare behandles med den registrertes samtykke eller for å fastsette, gjøre gjeldende eller forsvare rettskrav eller for å verne en annen fysisk eller juridisk persons rettigheter eller av hensyn til viktige allmenne interesser i Unionen eller en medlemsstat.

3. En registrert som har oppnådd begrensning av behandlingen i henhold til nr. 1, skal underrettes av den behandlingsansvarlige før nevnte begrensning av behandlingen oppheves.»

Artikkel 19. Underretningsplikt i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling

«Den behandlingsansvarlige skal underrette enhver mottaker som har fått utlevert personopplysninger, om enhver retting eller sletting av personopplysninger eller begrensning av behandlingen utført i samsvar med artikkel 16, artikkel 17 nr. 1 og artikkel 18, med mindre dette viser seg å være umulig eller innebærer en uforholdsmessig stor innsats. Den behandlingsansvarlige skal underrette den registrerte om nevnte mottakere dersom den registrerte anmoder om det.»

Artikkel 20. Rett til dataportabilitet

«1. Den registrerte skal ha rett til å motta personopplysninger om seg selv som vedkommende har gitt til en behandlingsansvarlig, i et strukturert, alminnelig anvendt og maskinlesbart format og skal ha rett til å overføre nevnte opplysninger til en annen behandlingsansvarlig uten at den behandlingsansvarlige som personopplysningene er gitt til, hindrer dette, dersom

a) behandlingen er basert på samtykke i henhold til artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a) eller en avtale i henhold til artikkel 6 nr. 1 bokstav b), og

b) behandlingen utføres automatisk.

2. Når den registrerte utøver sin rett til dataportabilitet i henhold til nr. 1, skal vedkommende, når det er teknisk mulig, ha rett til å få overført personopplysningene direkte fra en behandlingsansvarlig til en annen.

3. Utøvelse av rettigheten nevnt i nr. 1 i denne artikkel berører ikke artikkel 17. Nevnte rettighet får ikke anvendelse på behandling som er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.»

Artikkel 77. Rett til å klage til en tilsynsmyndighet

«1. Uten at det berører annen administrativ eller rettslig prøving, skal enhver registrert ha rett til å klage til en tilsynsmyndighet, særlig i den medlemsstat der vedkommende har sitt vanlige bosted, har sitt arbeidssted eller der den påståtte overtredelsen har funnet sted, dersom den registrerte anser at behandlingen av personopplysninger som gjelder vedkommende, er i strid med denne forordning.»

Lov om elektronisk kommunikasjon

Ekomloven § 2-7 b.Bruk av informasjonskapsler/cookies

«Lagring av opplysninger i brukers kommunikasjonsutstyr, eller å skaffe seg adgang til slike, er ikke tillatt uten at brukeren er informert om hvilke opplysninger som behandles, formålet med behandlingen, hvem som behandler opplysningene, og har samtykket til dette. Første punktum er ikke til hinder for teknisk lagring av eller adgang til opplysninger:

1. utelukkende for det formål å overføre kommunikasjon i et elektronisk kommunikasjonsnett

2. som er nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel.»

Personvernombud

Artikkel 37. Utpeking av et personvernombud

1. Den behandlingsansvarlige og databehandleren skal utpeke et personvernombud når

a) behandlingen utføres av en offentlig myndighet eller et offentlig organ, bortsett fra domstoler som opptrer innenfor rammen av sin domsmyndighet,……..

3. Dersom den behandlingsansvarlige eller databehandleren er en offentlig myndighet eller et offentlig organ, kan det utpekes ett personvernombud for flere av nevnte myndigheter eller organer, idet det tas hensyn til deres organisasjonsstruktur og størrelse……

5. Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området samt evne til å utføre oppgavene nevnt i artikkel 39.

6. Personvernombudet kan være en ansatt hos den behandlingsansvarlige eller databehandleren eller utføre oppgavene på grunnlag av en tjenesteavtale.

7. Den behandlingsansvarlige eller databehandleren skal offentliggjøre kontaktopplysningene til personvernombudet og meddele disse til tilsynsmyndigheten.»

Artikkel 38. Personvernombudets stilling

«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.

2. Den behandlingsansvarlige og databehandleren skal støtte personvernombudet i forbindelse med utførelsen av oppgavene nevnt i artikkel 39 ved å stille til rådighet de ressurser som er nødvendig for å utføre nevnte oppgaver, samt gi tilgang til personopplysninger og behandlingsaktiviteter og gjøre det mulig for vedkommende å opprettholde sin dybdekunnskap.

3. Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet ikke mottar instrukser om utførelsen av nevnte oppgaver. Vedkommende skal ikke avsettes eller straffes av den behandlingsansvarlige eller databehandleren for å utføre sine oppgaver. Personvernombudet skal rapportere direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige eller databehandleren.

4. De registrerte kan kontakte personvernombudet angående alle spørsmål om behandling av deres personopplysninger og om utøvelsen av de rettighetene de har i henhold til denne forordning.

5. Personvernombudet skal være bundet av taushetsplikt eller en plikt til konfidensiell behandling av opplysninger ved utførelse av sine oppgaver i samsvar med unionsretten eller medlemsstatenes nasjonale rett.

6. Personvernombudet kan utføre andre oppgaver og ha andre plikter. Den behandlingsansvarlige eller databehandleren skal sikre at nevnte oppgaver eller plikter ikke fører til en interessekonflikt.»

Artikkel 39. Personvernombudets oppgaver

«1. Personvernombudet skal minst ha følgende oppgaver:

a) *informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning, og i henhold til andre av Unionens eller medlemsstatenes bestemmelser om vern av personopplysninger,*

b) *kontrollere overholdelsen av denne forordning, av andre av Unionens eller medlemsstatenes personvernregler og den behandlingsansvarliges eller databehandlerens personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene, og tilhørende revisjoner,*

c) *på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den i henhold til artikkel 35,*

d) *samarbeide med tilsynsmyndigheten,*

e) *fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, herunder forhåndsdrøftingene nevnt i artikkel 36, og ved behov rådføre seg med tilsynsmyndigheten om eventuelle andre spørsmål.*

2. Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.»

Utledede revisjonskriterier

Har kommunen implementert personvernregelverket?
Med hensyn til art, omfang, formål og sammenhengen behandlingen av personopplysninger utføres i, samt risikovurderinger skal kommunen gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandling av personopplysninger utføres i samsvar med forordningen, jf. art. 24. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov. Tiltak skal iverksettes både på tidspunktet når det blir bestemt hvilke midler som skal brukes til behandling av personopplysninger og ved selve behandlingen av personopplysningene, jf. pvf art. 25

Lovlig, rettferdig og gjennomsiktig

Revisjonskriterier

- Kommunen behandler personopplysninger på en lovlig, rettferdig og åpen måte med hensyn til den registrerte.
- Kommunen skal gi den registrerte informasjon om behandlingen av personopplysninger, skriftlig herunder elektronisk. Informasjonen skal være tilpasset målgruppa, for eksempel barn på ulike alderstrinn.
- Kommunen fører en protokoll over behandlingsaktiviteter som utføres under deres ansvar.
- Protokollene skal være skriftlige, herunder elektroniske. Protokollen inneholder
    - navnet på og kontaktopplysningene til den behandlingsansvarlige og personvernombudet
    - formålene med behandlingen,
    - en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger,
    - kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til
    - dersom det er mulig, planlagte tidsfrister for sletting av de forskjellige kategoriene av opplysninger,
    - evt. generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1……
- Kommunen har innhentet samtykke til de nødvendige kategoriene personopplysninger.
- Kommunen bruker kameraovervåking i henhold til retningslinjene.
- Kommunen har sørget for å ikke benytte uekte kameraovervåkingsutstyr eller ved skilting, oppslag eller lignende gi inntrykk av at kameraovervåking finner sted.

4.1.2 Personers rettigheter

Revisjonskriterier

- Kommunen skal sørge for å overføre nevnte opplysninger til en annen behandlingsansvarlig når den registrerte ber om det og det er teknisk mulig (dataportabilitet).
- Kommunen ivaretar retten til innsyn i personopplysningene (hvor de kommer fra, hvordan de behandles og en kopi av registrerte opplysninger).
- Kommunen sørger for at personer får utført rettighetene gratis.
- Kommunen informerer om rettighetene og om partsinnsyn etter forvaltningsloven.
- Kommunen sikrer at den registrerte mottar personopplysninger om seg selv som vedkommende har gitt til kommunen, i et strukturert, alminnelig anvendt og maskinlesbart format.
- Kommunen begrunner avslag om innsyn skriftlig og gir en presis henvisning til unntakshjemmelen.

Formålsbegrenset

Revisjonskriterier

- Kommunen sikrer at personopplysningene kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål og at opplysningene ikke viderebehandles utover formålet.
- Kommunen vurderer hvilke formål personopplysningene samles inn til.
- Kommunen vurderer om det valgte formålet er forenelig med det personopplysningene opprinnelig ble samlet inn til.
- Kommunen har en oversikt over de ulike kategoriene personopplysninger som er registrert til ulike formål.
- Kommunen har kunnskap om personopplysninger benyttes til andre formål enn det de er samlet inn til.

Dataminimering

Revisjonskriterier

- Kommunen gjør en vurdering av om de innsamlede opplysningen i hvert tilfelle er adekvate, relevante og begrenset til formålet.
- Kommunen har vurdert om personopplysningene er nødvendig for å utøve lovpålagte oppgaver – utøve offentlig myndighet.
- Kommunen har vurdert når det er behov for behandling av særlige kategorier personopplysninger.

Riktighet

Revisjonskriterier

- Kommunen sikrer at personopplysningene er korrekte og om nødvendig oppdaterte.
- Kommunen ser til at personer får korrigert opplysningene dersom de ikke er korrekte – uten ugrunnet opphold.
- Kommunen ser til at personer som ber om at opplysninger om seg blir sperret eller slettet, uten ugrunnet opphold, får utført dette. Dette gjelder dersom opplysningene
    - ikke lenger er nødvendig for formålet
    - bygger på samtykke og personen trekker samtykke, forutsatt at opplysningene ikke er grunnlag for en behandling
    - har blitt behandlet ulovlig (innsigelse)

Lagringsbegrensing

Revisjonskriterier

- Kommunen sikrer at personopplysningene lagres slik at det ikke er mulig å identifisere de registrerte lengere enn det som er nødvendig for formålet som personopplysningene behandles for.
- Kommunen sletter personopplysninger uten ugrunnet opphold dersom personopplysningene ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for.

Integritet og konfidensialitet

Revisjonskriterier

- Kommunen sikrer at personopplysningene behandles på en måte som gir tilstrekkelig sikkerhet for personopplysningene.
- Kommunen gjør en vurdering av hvilke ansatte som skal ha autorisert tilgang til hvilke personopplysninger. Personopplysningene skal være kryptert for ansatte som ikke har autorisert tilgang.
- Kommunen gjennomfører egnede tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering.
- Kommunen iverksetter egnede tekniske og organisatoriske tiltak både når det blir bestemt hvilke midler som skal brukes til behandling av personopplysninger og ved selve behandlingen av personopplysningene.
- Kommunen iverksetter egnede retningslinjer for vern av personopplysninger.

Ansvarlighet

4.7.1 Databehandlere

Revisjonskriterier

- Kommunen har en oversikt over de databehandlerne de benytter
- Kommunen har vurdert hvilke opplysninger som databehandler krever, er adekvate, relevante og begrenset for formålet.
- Kommunen har utarbeidet avtaler med databehandlerne i henhold til kravene i regelverket.

4.7.2 Personvernombud

Revisjonskriterier

- Kommunen har et personvernombud, som har rammer og oppgaver i henhold til regelverket.
- Kommunen har offentliggjort kontaktopplysningene til personvernombudet og meldt disse til Datatilsynet.
- Kommunen sørger for at personvernombudet blir involvert i saker om personvern på riktig måte og til rett tid.
- Kommunen stiller til rådighet de ressurser som er nødvendig for å utføre nevnte oppgaver.
- Kommunen gir personvernombudet tilgang til personopplysninger og behandlingsaktiviteter, og gjør det mulig for vedkommende å opprettholde sin dybdekunnskap.
- Kommunen sikrer at personvernombudet ikke mottar instrukser om utførelsen av nevnte oppgaver. Vedkommende skal ikke avsettes eller straffes av kommunen eller databehandleren for å utføre sine oppgaver.
- Personvernombudet rapporterer direkte til det høyeste ledelsesnivået i kommunen

4.7.3 Risikovurdering - personvernkonsekvens

Revisjonskriterier

- Kommunen har gjennomført en risikovurdering av personopplysningssikkerheten før alle behandlinger igangsettes.
- Kommunen har gjennomført en vurdering av personvernkonsekvensene (DPIA) i henhold til Datatilsynets liste.

4.7.5 Opplæring i regelverket

Revisjonskriterier

- Kommunen må sette de ansatte i stand til å etterleve regelverket, ved blant annet å gi de ansatte opplæring i
    - behandling av personopplysninger
    - vilkår for samtykke til behandling av personopplysninger
    - når og hvordan melde avvik og behandling av avviksmeldinger
    - evt. gjennomføring av risikovurdering
    - ivaretakelse av registrertes rettigheter
    - hvem som er personvernombud, kontaktinformasjon og ombudets oppgaver og rolle i kommunen

4.7.4 Internkontroll

Revisjonskriterier

- Med bakgrunn i den gjennomførte risikovurderingen, har kommunen iverksatt egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysningene skjer i samsvar med personvernforordningen.
- Kommunen har innhentet kunnskap om personopplysninger behandles etter personvernregelverket.
- Kommunen har sørget for å iverksette tiltak der det fremkommer at regelverket ikke etterleves.
- Kommunen sikrer at brudd på personopplysningssikkerheten meldes til Datatilsynet når det er risiko for personers rettigheter og frihet.
- Kommunen sikrer at den registrert blir varslet, dersom bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter.
- Kommunen sikrer at brudd som ikke rapporteres til Datatilsynet, behandles og begrunnes i en intern avviksrapport.

Vedlegg 2 – Definisjoner og begreper

1. **«personopplysninger»** enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»);
2. **«behandling»** enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,
3. **«begrensning av behandling»** merking av lagrede personopplysninger med det som mål å begrense behandlingen av disse i framtiden,
4. **«pseudonymisering»** behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person,
5. **«register»** enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier, enten samlingen er plassert sentralt, er desentralisert eller spredt på et funksjonelt eller geografisk grunnlag,
6. **«behandlingsansvarlig»** en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,
7. **«databehandler»** en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige,
8. **«mottaker»** en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som personopplysninger utleveres til, enten det dreier seg om en tredjepart eller ikke. Offentlige myndigheter som kan motta personopplysninger innenfor rammen av en særskilt undersøkelse i samsvar med unionsretten eller medlemsstatenes nasjonale rett, skal imidlertid ikke anses som mottakere; nevnte offentlige myndigheters behandling av slike opplysninger skal være i samsvar med gjeldende regler om vern av personopplysninger i henhold til formålet med behandlingen,
9. **«tredjepart»** enhver annen fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ enn den registrerte, den behandlingsansvarlige, databehandleren og de personer som under den behandlingsansvarlige eller databehandlerens direkte myndighet har fullmakt til å behandle personopplysninger,
10. **«samtykke»** fra den registrerte enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende,
11. **«brudd på personopplysningssikkerheten»** et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet,
12. **«genetiske opplysninger»** personopplysninger om en fysisk persons nedarvede eller ervervede genetiske egenskaper som gir unik informasjon om den aktuelle fysiske personens fysiologi eller helse, og som særlig er framkommet etter analysering av en biologisk prøve fra den aktuelle fysiske personen,
13. **«biometriske opplysninger»** personopplysninger som stammer fra en særskilt teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper, og

som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person, f.eks. ansiktsbilder eller fingeravtrykksopplysninger,

14. **«helseopplysninger»** personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand,
15. **«hovedvirksomhet»**:
    a) når det gjelder en behandlingsansvarlig med virksomheter i mer enn én medlemsstat, stedet for dennes hovedadministrasjon i Unionen, med mindre avgjørelser om formål og midler i forbindelse med behandlingen av personopplysninger treffes i en annen av den behandlingsansvarliges virksomheter i Unionen, og sistnevnte virksomhet har myndighet til å få gjennomført nevnte avgjørelser, i dette tilfellet skal virksomheten som har truffet slike avgjørelser, anses for å være hovedvirksomheten,
    b) når det gjelder en databehandler med virksomheter i mer enn én medlemsstat, stedet for dennes hovedadministrasjon i Unionen eller, dersom databehandleren ikke har noen hovedadministrasjon i Unionen, databehandlerens virksomhet i Unionen der hoveddelen av behandlingsaktivitetene i forbindelse med aktivitetene ved en databehandlers virksomhet finner sted, i den grad databehandleren er underlagt særlige forpliktelser i henhold til denne forordning,
16. **«representant»** en fysisk eller juridisk person som er etablert i Unionen, som den behandlingsansvarlige eller databehandleren har utpekt skriftlig i henhold til artikkel 27, og som representerer den behandlingsansvarlige eller databehandleren med hensyn til de forpliktelser de har i henhold til denne forordning,
17. **«foretak»** en fysisk eller juridisk person som utøver økonomisk virksomhet, uavhengig av foretakets rettslige form, herunder partnerskap eller sammenslutninger som regelmessig utøver økonomisk virksomhet,
18. **«konsern»** et foretak som utøver kontroll, og dets kontrollerte foretak,
19. **«tilsynsmyndighet»** en uavhengig offentlig myndighet som er opprettet av en medlemsstat i henhold til artikkel 51,
20. **«relevant og begrunnet innsigelse»** en innsigelse mot et utkast til avgjørelse om hvorvidt det foreligger en overtredelse av denne forordning eller om hvorvidt et planlagt tiltak som gjelder den behandlingsansvarlige eller databehandleren, er i samsvar med denne forordning, og som tydelig viser betydningen av risikoene som utkastet til avgjørelse utgjør med hensyn til de registrertes grunnleggende rettigheter og friheter og, dersom det er relevant, den frie flyten av personopplysninger i Unionen,
21. **«informasjonssamfunnstjeneste»** en tjeneste som definert i artikkel 1 nr. 1 bokstav b) i europaparlaments- og rådsdirektiv (EU) 2015/1535,

Vedlegg 3 - Spørsmål i Questback

Til ledergruppen i Fredrikstad kommune

•**Personvern i Fredrikstad kommune - ledergruppen**

1) * Hvilken seksjon i Fredrikstad kommune er du ansatt i?

- Økonomi og organisasjonsutvikling
- Innovasjon og styring
- Teknisk drift
- Utdanning og oppvekst
- Helse og velferd
- Kultur, miljø og byutvikling

Denne informasjonen vises kun i forhåndsvisningen

Actions vil skje for følgende alternativer:

Nei : Vis avslutningsmeldingen

2) * Behandler dere personopplysninger i virksomhetene/enhetene i din seksjon?

- Ja
- Nei
- Vet ikke

3) * Har dere gjort en overordnet eller felles vurdering av hvilke personopplysninger dere har behov for i virksomhetene/enhetene i din seksjon?

- Ja
- Nei
- Vet ikke

4) * Har dere vurdert om dere har rettslig grunnlag til å behandle personopplysningene?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Har dere vurdert om dere har rettslig grunnlag til å behandle personopplysningene? inneholder noen av disse alternativene

- Ja

5) * Hva tenker du er det rettslige grunnlaget for databehandling i din seksjon/enhet?

6) * Hvor god kunnskap har du om behandlingen av personopplysninger i virksomheter/enheter som hører til din seksjon?

- Svært god
- God
- Ikke så god
- Ingen kunnskap

7) * Har dere en oversikt over hvilke type formål dere henter personopplysninger til?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Har dere en oversikt over hvilke type formål dere henter personopplysninger til? inneholder noen av disse alternativene

- Ja

8) * Hvor finner du denne oversikten?

9) * Benyttes personopplysninger til andre formål enn de er samlet inn for?

- Ja
- Nei
- Vet ikke

10) * Informerer dere brukerne av tjenestene i virksomhetene, enhetene i din seksjon om behandlingen av personopplysningene?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Informerer dere brukerne av tjenestene i virksomhetene, enhetene i din seksjon om behandlingen av personopplysningene? inneholder noen av disse alternativene

- Ja

Her kan du velge flere alternativer

11) * Hva informerer dere om?

☐ Hvilke personopplysninger som lagres
☐ Hvordan personopplysningene blir brukt
☐ Hva formålet med lagringen er
☐ Personers rettigheter i personvernlovgivningen
☐ Annet

Dersom spørsmålet Informerer dere brukerne av tjenestene i virksomhetene, enhetene i din seksjon om behandlingen av personopplysningene? inneholder noen av disse alternativene

- Nei

12) * Hvorfor informerer dere ikke brukerne om behandlingen av personopplysningene?

13) * Kjenner du til hvilke personopplysninger dere må ha samtykke for å innhente?

○ Ja
○ Nei

14) * Hentes det inn personopplysninger som er "kjekt å vite", men som ikke er direkte relevant for formålet i virksomhetene, enhetene i din seksjon?

○ Ja
○ Nei
○ Vet ikke

Dersom spørsmålet Hentes det inn personopplysninger som er "kjekt å vite", men som ikke er direkte relevant for formålet i virksomhetene, enhetene i din seksjon? inneholder noen av disse alternativene

- Ja
-

15) * Benyttes samtykke ved innhenting av slike opplysninger?

- Ja
- Nei
- Vet ikke

16) * Har dere gjort vurderinger av hvem som skal ha tilgang til de ulike personopplysningene i virksomhetene, enhetene og i din seksjon?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Har dere gjort vurderinger av hvem som skal ha tilgang til de ulike personopplysningene i virksomhetene, enhetene og i din seksjon? inneholder noen av disse alternativene

- Ja

17) * Hva er begrunnelsen for at noen skal ha tilgang til ulike typer personopplysninger?

Særskilte kategorier personopplysninger er for eksempel opplysninger om:
- Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
- At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- Helseforhold
- Seksuelle forhold

18) * Har dere oppgaver i virksomhetene, enhetene i din seksjon, som medfører behov for særskilte kategorier personopplysninger (f.eks. informasjon om etnisk opprinnelse, helseinformasjon politisk oppfatning etc.)

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Har dere oppgaver i virksomhetene, enhetene i din seksjon, som medfører behov for særskilte kategorier personopplysninger

(f.eks. informasjon om etnisk opprinnelse, helseinformasjon politisk oppfatning etc.) inneholder noen av disse alternativene

- Ja

19) * Kjenner du til hvordan de særskilte kategoriene personopplysningene er sikret?

- Ja
- Nei

20) * Er det gjennomført en risikovurdering for konsekvensen ved behandling av personopplysningene på ditt fagområde?

- Ja
- Nei

21) * Er det ført protokoll over de behandlingsaktivitetene som gjennomføres av personopplysninger på ditt fagområde?

- Ja
- Nei
- Vet ikke

22) * Hvordan informerer dere (kommuneadministrasjonen og/eller virksomhetene) om retten til innsyn, retting og sletting av personopplysninger?

Dersom spørsmålet Hvilken seksjon i Fredrikstad kommune er du ansatt i? inneholder noen av disse alternativene

- Kultur, miljø og byutvikling
- Helse og velferd
- Utdanning og oppvekst

23) * Informerer dere barn og unge om rettighetene på personvernområdet på en sånn måte at det er forståelig?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Hvilken seksjon i Fredrikstad kommune er du ansatt i? inneholder noen av disse alternativene

- Kultur, miljø og byutvikling

- Helse og velferd
- Utdanning og oppvekst

24) * Finnes det en egen personvernerklæring tilpasset barn og unge

- Ja
- Nei
- Vet ikke

Her kan du velge flere alternativer.

25) * Hvilke kanaler brukes på ditt fagområde til å kommunisere med brukere av kommunens tjenester og evt. pårørende?

- [ ] E-post
- [ ] SMS
- [ ] Chat
- [ ] Kommunens hjemmeside eller andre plattformer
- [ ] Sikker melding/post
- [ ] Andre systemer

26) * Hvordan lagres, arkiveres og slettes data her?

27) * Finnes det kameraovervåking i virksomhetene eller enhetene knytte til din seksjon?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Finnes det kameraovervåking i virksomhetene eller enhetene knytte til din seksjon? inneholder noen av disse alternativene

- Ja

28) * Er kameraovervåkingen behandlet og ført i protokoll for slike behandlinger?

- Ja
- Nei

29) * Kjenner du til personvernombudets oppgaver?

- Ja
- Delvis
- Nei

30) * Kjenner du til om personvernombudet har blitt involvert i saker på ditt fagområde?

- Ja
- Nei
- Vet ikke

31) * Kjenner du til områder der personvernombudet burde vært involvert, men ikke ble det?

- Ja
- Nei

32) * Mener du at du har fått tilstrekkelig opplæring i personvernregelverket?

- Ja, jeg har fått tilstrekkelig opplæring
- Ja, men jeg trenger mer
- Nei, jeg har ikke fått tilstrekkelig opplæring
- Annet

33) * Er det områder i personvernlovgivningen du opplever særlig utfordrende å ivareta?

34) Har du andre kommentarer eller innspill til arbeidet med personvern eller til spørreundersøkelsen?

Til ansatte i skoler og barnehager, og alle rektorer og styrere

Personvern Fredrikstad - skoler og barnehager

1) * Hvilken virksomhet jobber du i?

- Barnehage
- Skole

2) * Hvilken funksjon har du?

- Styrer eller rektor
- Merkantilt ansatt
- Pedagog/mellomleder/fagarbeider/assistent eller annen funksjon

Dersom spørsmålet Hvilken virksomhet jobber du i? inneholder noen av disse alternativene

- Skole

3) * Har skolen du jobber på ungdomstrinn (8-10)?

- Ja
- Nei

Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene

- Merkantilt ansatt
- Styrer eller rektor

Vi spør her om behandlingen av personopplysninger for barn og ungdom i skoler og barnehager.

4) * Har dere gjort en vurdering av hvilke personopplysninger dere har behov for på din skole/barnehage?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene

- Merkantilt ansatt
- Styrer eller rektor

5) * Har dere vurdert hvorfor dere har behov for disse personopplysningene (formål)?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene

- Merkantilt ansatt
- Styrer eller rektor

6) * Hvor god kunnskap har du om hvilke personopplysninger som ansatte i din virksomhet henter inn om barn og unge?

- Svært god
- God
- Ikke så god
- Lite kunnskap

Dersom spørsmålet Har skolen du jobber på ungdomstrinn (8-10)? inneholder noen av disse alternativene

- Ja

7) * Informerer dere elevene om rettighetene på personvernområdet på en sånn måte at det er forståelig?

- I stor grad
- I noen grad
- I liten grad
- Vi informerer ikke elevene om rettighetene på personvernområdet
- Vet ikke

Dersom spørsmålet Har skolen du jobber på ungdomstrinn (8-10)? inneholder noen av disse alternativene

- Ja

8) * Har skolen/kommunen utarbeidet en egen personvernerklæring tilpasset barn og unge?

- Ja
- Nei
- Vet ikke

9) * Har dere en felles praksis for hva som kan hentes inn av personopplysninger i din virksomhet?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Har skolen du jobber på ungdomstrinn (8-10)? inneholder noen av disse alternativene

- Ja

Alternativ: - Både foreldre og elever

Dersom spørsmålet Har skolen du jobber på ungdomstrinn (8-10)? inneholder noen av disse alternativene

- Ja

10) * Hvem blir informert om at personopplysninger om elever blir lagret?

- Foreldrene
- Elevene
- Både foreldre og elever
- Vet ikke
- Andre

Her kan du velge flere alternativ.

11) * Hva informerer dere om?

- [ ] Hvilke personopplysninger som lagres
- [ ] Hvordan personopplysningene blir lagret og sikret
- [ ] Hvorfor dere har behov for disse personopplysningene
- [ ] Personers rettigheter i personvernlovgivningen
- [ ] Vet ikke

12) * Kjenner du til hvilke personopplysninger dere må ha samtykke for å innhente?

- Ja
- Nei

13) * Henter dere noen ganger inn personopplysninger som er "kjekt å vite", men som ikke er direkte relevant for formålet?

- Ja
- Nei

Dersom spørsmålet Henter dere noen ganger inn personopplysninger som er "kjekt å vite", men som ikke er direkte relevant for formålet? inneholder noen av disse alternativene

- Ja

14) * Ber dere om samtykke til å hente inn slike opplysninger fra foreldre og/eller elever?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Hvilken virksomhet jobber du i? inneholder noen av disse alternativene

- Skole

15) * Kontrollerer/loggfører skolen elevenes Internett-bruk?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Kontrollerer/loggfører skolen elevenes Internett-bruk? inneholder noen av disse alternativene

- Ja

16) * Opplyser dere elevene og foreldrene om at dere loggfører internettbruken?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene

- Merkantilt ansatt
- Styrer eller rektor

17) * Har dere gjort vurderinger av hvem som skal ha tilgang til de ulike personopplysningene på skolen/i barnehagen?

- Ja
- Nei
- Vet ikke

Dersom spørsmålet Hvilken virksomhet jobber du i? inneholder noen av disse alternativene

- Skole

og

Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene

- Pedagog/mellomleder/fagarbeider/assistent eller annen funksjon

18) * Hvilke personopplysninger om elever har du tilgang til i arkivet?

- Alle opplysningene om alle elevene ved skolen
- Alle opplysningene om elevene som tilhører mitt team/avdeling
- Alle opplysningene om de elevene jeg har et fagansvar for
- Kun opplysninger som er nødvendige.

Dersom spørsmålet Hvilken virksomhet jobber du i? inneholder noen av disse alternativene

- Barnehage

og

Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene

- Pedagog/mellomleder/fagarbeider/assistent eller annen funksjon

19) * Hva har du tilgang til når det gjelder opplysninger om barna i arkivet?

☐ Alle opplysninger om barna i barnehagen
☐ Alle opplysninger om barna på min avdeling
☐ Avgrensede opplysninger om alle barna i barnehagen
☐ Avgrensede opplysninger om barna på min avdeling

20) * Har skolen/barnehagen papirarkiv som inneholder opplysninger om barna/ungdommene

○ Ja
○ Nei
○ Vet ikke

Her kan du velge flere alternativer.

21) * Hvilke kanaler bruker du til å kommunisere med foreldre og/eller elever

☐ e-post
☐ SMS
☐ Chat
☐ virksomhetens nettside/andre plattformer
☐ sikker melding/post
☐ andre kanaler

22) * Har dere prosedyrer for lagring og sletting av personopplysninger fra disse kanalene?

○ Ja
○ Nei
○ Vet ikke

Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene

- Merkantilt ansatt
- Styrer eller rektor

23) * Finnes det kameraovervåking på din skole/barnehage?

- Ja
- Nei

24) * Kjenner du til personvernombudets oppgaver?

- Ja
- Delvis
- Nei

25) * Mener du at du har fått tilstrekkelig opplæring i personvernregelverket?

- Ja, jeg har fått tilstrekkelig opplæring
- Ja, men jeg trenger mer opplæring
- Nei, men jeg trenger ikke opplæring
- Nei, jeg har ikke fått tilstrekkelig opplæring

Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene

- Merkantilt ansatt
- Styrer eller rektor

26) * Kjenner du til om det er gjennomført en risikovurdering for konsekvensen ved behandling av personopplysningene i skolene/barnehagene?

- Ja
- Nei

27) Er det områder i personvern (GDPR) du opplever særlig utfordrende å ivareta? Evt hvilke?