østfold kommunerevisjon IKS

Personvern

Halden kommune

Forvaltningsrevisjonsrapport

Rolvsøy, 18. november 2019

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. I en fase med nye regler er dette ekstra viktig for å sikre at kommunen etterlever de nye reglene.

Østfold kommunerevisjon fikk i oppdrag å gjennomføre forvaltningsrevisjon på området kommunens implementering og ivaretakelse av det nye personvernregelverket. Vi har da 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 og ansatte på en utvalgt skole. Det er innhentet dokumentasjon fra både administrativt nivå i kommunen 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 avdelingsledere, enhetsledere og lærere på en skole.

Spørreundersøkelsen ble totalt sendt til 54 ansatte og ledere i kommunen, herunder til 14 rektorer i grunnskolene og styrere for barnehagene. Ved utløp av svarfristen var det 31 av 54 som hadde besvart undersøkelsen. Det gir en svarprosent på 57 %. Ved gjennomgang av respondentene viste det seg at det kun var 5 av 19 lærere som hadde svart på undersøkelsen, og vi valgte dermed å ta bort denne gruppen i analysen av svarene. Dette på bakgrunn av at svarprosenten fra denne gruppen var så lav at det ville bli vanskelig å trekke noen generelle slutninger på et så lite grunnlag. Faktagrunnlaget som bygger på spørreundersøkelsen har derfor reelt sett en svarprosent på 74 %, og gir et godt grunnlag for analysen, som presenteres i rapporten.

Det er vår vurdering at kommunen kom noe sent i gang med å gi opplæring og implementere det nye personvernregelverket. Kommunen har imidlertid i 2019 intensivert arbeidet og jobber nå samtidig på flere områder for å få personvernregelverket på plass. Det jobbes parallelt med å hente inn opplysninger i organisasjonen for å få ferdig en behandlingsprotokoll, utarbeide oversikter over databehandlere og etablere databehandleravtaler, gi opplæring i personvernregelverket, DPIA og implementere et oppdatert internkontrollsystem osv. Det gjenstår fremdeles mye arbeid på de fleste områder før kommunen kan si at personregelverket er implementer i kommunen. Det er imidlertid vår konklusjon at kommunen nå prioriterer dette arbeidet og tar ansvar på området.

Revisjonen anbefaler at kommunen bør

- sørge for å informere om hvordan de behandler personopplysningene på en måte som gjør informasjonen forståelig for alle målgrupper, som for eksempel for barn og unge.
- behandle de ulike typene kommunikasjonskanaler som ansatte benytter som sms, chat, e-post osv, vurdere lagring og sletting av personopplysninger og personvernkonsekvens
- ha en gjennomgang av hvilke kategoriene personopplysninger som det må innhentes samtykke til på de ulike fagområdene.
- etablere felles rutiner for enhet- skole, når det gjelder tilgangsavgrensing til fysiske arkiv.
- sikre at personopplysninger ikke lagres lenger enn det som er nødvendig og forsvarlig for den enkelte sak
- se til at det gjøres en vurdering av om opplysninger eller deler av opplysninger skal slettes eller pseudonymiseres ved lagring av ikke arkivverdige personopplysninger, og vurdere om formålet for lagring av opplysningene er et annet enn ved registreringen
- videreføre arbeidet med databehandleravtaler, slik at kommunen har avtale med alle databehandlere
- se til at personvernombudet rapporterer til høyeste ledelsesnivå i kommunen
- gjennomføre en behandling av sine webkameraer og informere kommunens innbyggere om hensikten med og bruken av disse
- videreføre arbeidet med behandlingene, slik at alle behandlinger er registrert i protokollen og at det er vurdert om det er høy risiko for personvernkonsekvens
- videreføre arbeidet med å vurdere personvernkonsekvens (DPIA) der risikoen er høy
- etablere og implementere interkontroll på personvernområdet
- sørge for at opplæring blir prioritert nedover i organisasjonen

Kommunen bør legge enda større vekt på opplæring av alle ansatte og i den forbindelse ansvarliggjøring de ulike ledernivåene på opplæringsområdet. Dette for å sørge for at ansatte i enhetene, som jobber tett på brukerne av kommunens tjenester, får nødvendig kompetanse i regelverket og bedre kunnskap om kommunens rutiner på området.

Kommunen bør i større grad involvere avdelingslederne i arbeidet med å få på plass en behandlingsprotokoll og i vurderingen av personvernkonsekvenser på ulike områder. Det er vår vurdering at involvering av lederne på de ulike fagområdene vil sikre kvaliteten på behandlingene knyttet til det enkelte formål, sikre at alle behandlinger av personopplysninger blir registrert. Det vil også medføre at avdelingslederne får et større eierforhold til arbeidet med personvernregelverket på sitt fagområde.

Vi takker Halden kommune og den utvalgte skolen for samarbeidet og god tilrettelegging for gjennomføring av revisjonen.

1 INNLEDNING

1.1 Bakgrunn

Østfold kommunerevisjon utfører forvaltningsrevisjon, jfr. kommunelovens § 78 og forskrift om revisjon kapittel 3. Forvaltningsrevisjon innebærer blant annet å kontrollere at forvaltningens aktiviteter foregår i samsvar med gjeldende regelverk og kommunestyrets vedtak.

Kommunestyret i Halden fastsatte 15. februar 2018, forvaltningsrevisjonsplan for 2018-2019. Personvern er det neste prosjektet i planen. Kontrollutvalget i Halden godkjente plan for gjennomføring av prosjektet 18.06.2019, i - sak PS 2018/14.

I vedtatt forvaltningsrevisjonsplan for Halden kommune 2018-2019 fremkommer det at 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, ansvar og rutiner, samt riktig bruk av IKT systemene.

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. I en fase med nye regler er dette ekstra viktig for å sikre at kommunen etterlever de nye reglene.

1.2 Problemstilling og avgrensing

Østfold kommunerevisjon fikk i oppdrag å gjennomføre forvaltningsrevisjon på området kommunens implementering og ivaretakelse av det nye personvernregelverket. I prosjektplan er det lagt opp til to problemstillinger:

- Har kommunen implementert personvernregelverket?
- Har kommunen sikret at de ansatte etterlever regelverket?

Å sikre at de ansatte etterlever regelverket er en forutsetning for implementering, og revisjonen har derfor valgt å presentere problemstillingene samlet i kapittel 4. Revisjonskriteriene bygger på de syv grunnkravene i personvernregelverket (listet opp nedenfor) og vi har valgt å bygge opp rapporten etter disse kriteriene. Kommunens arbeid for å sikre at de ansatte etterlever regelverket faller inn under kriteriet/kapittel 4.7 om ansvarlighet, herunder kapittel *4.7.4 Opplæring i regelverket.*

Grunnkravene i personvernregelverket:
1. Lovlig, rettferdig og gjennomsiktig
2. Formålsbegrenset
3. Dataminimering
4. Riktighet
5. Lagringsbegrensing
6. Integritet og konfidensialitet
7. Ansvarlighet

Prosjektets ramme i antall timer tilsier at det ikke er rom for å gjennomføre en revisjon av alle enheter og områder på personvern i kommunen. Kontrollen ble avgrenset til å vurdere at systemer, registreringer og avtaler finnes, og en stikkprøve av disse. Revisjonen har gjennomført undersøkelsen på administrativt nivå, samtidig hadde kommunen et ønske om at revisjonen skulle se

nærmere på underliggende enheter, for å belyse hvordan regelverket er implementert helt ut til kommunens utøvende tjenester. Det er grunnskolen i kommunen som er valgt ut.

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 gått inn i systemene for registrering av personopplysninger for å vurdere 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 databehandleravtaler, hvordan de går frem og har oversikt.

Kommunen er organisert ved at rådmannen har en egen stab med ulike funksjoner og støttefunksjoner for intern drift. Kommunen har følgende kommunalavdelinger: Undervisning og oppvekst, Helse og omsorg og Teknisk. Kommunalavdelingene produserer tjenester til kommunens innbyggere. Hver kommunalavdeling har en kommunalsjef. I hver kommunalavdeling er det en fagleder for de underliggende enhetene. Hver enhet har en enhetsleder. Det er 11 grunnskoler i kommunen, som ledes av 10 rektorer. Det er seks barnehager i kommunen, som ledes av 5 styrere

Definisjoner og begrepsforklaringer er å finne i vedlegg 3.

2 GJENNOMFØRING AV PROSJEKTET

Østfold kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med «Standard for forvaltningsrevisjon» (RSK 001). Dette innebærer blant annet at rapporten skal skille klart mellom fakta, og revisjonens vurderinger og konklusjoner.

2.1 Prosjektets fremdrift

Oppstartsmøtet ble gjennomført 5. juni 2019. Arbeidsutkastet til rapporten ble sendt til Halden kommune 21. oktober 2019. Høringsmøtet ble gjennomført 7. november 2019. Endelig rapport ble sendt på offisiell høring til kommunen 11. november 2019. Vi mottok rådmannens høringsuttalelse 18. november 2019. Rådmannens høringsuttalelse er å finne i kapittel 7 i denne rapporten.

2.2 Metode

Fakta er en gjengivelse av informasjon som revisjonen har fått tilgang til gjennom datainnsamlingen. Informasjonen er hentet fra dokumenter, system gjennomsyn, spørreundersøkelse og verifiserte intervjuer. Der vi konkluderer, vil alltid vurderingene bygge på skriftlig dokumentasjon eller informasjon som kommer fra mer enn én kilde.

For å få et bredere grunnlag å vurdere på, har vi gjennomført en spørreundersøkelse. Spørreundersøkelsen retter seg mot ulike ledernivå i kommunens kommunalavdelinger og enheter. For å se nærmere på enhet skole, er kommunalsjef undervisning og oppvekst intervjuet. Det er sendt en spørreundersøkelse til alle rektorene på skolene i kommunen. Det er gjennomført intervjuer med et utvalg ansatte på en valgt skole og alle kontaktlærerne fikk tilbud om å delta i spørreundersøkelsen.

Metodene som er benyttet i gjennomføringen av denne revisjonen er intervjuer med et utvalg av kommunens ansatte på administrativt nivå og ansatte på en utvalgt skole. Det er innhentet dokumentasjon fra både administrativt nivå i kommunen 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 avdelingsledere, enhetsledere og lærere på en skole.

2.3 Dokumentanalyse

Dokumentanalysen bygger på dokumenter som vi har mottatt fra administrativt nivå i kommunen og den utvalgte skolen. Vi har også innhentet informasjon fra kommunens og enhetenes nettsider.

Dokumentliste er å finne i vedlegg 2.

2.4 Intervjuer

Det er gjennomført intervjuer med kommunens personvernombud, ansatte i rådmannens stab og støtte funksjoner, samt intervjuer med ledelse og ansatte på grunnskoleområdet. Det er totalt gjennomført 10 intervjuer.

- Personvernombud
- Arkiv – to ansatte
- Kommunikasjon og service
- IT
- Personal og organisasjon
- Kommunalsjef undervisning og oppvekst
- Rektor skole
- Merkantil skole
- Lærer skole

Referatene er skrevet under intervjuene, og oversendt den som ble intervjuet i etterkant, for verifisering. Det følger av revisjonens metodikk at verifiserte referater er fakta på lik linje med annen dokumentasjon.

2.5 Spørreundersøkelse

Det er gjennomført en spørreundersøkelse med de ulike ledernivåene i kommunen, dette inkluderer enhetslederne, og med lærere ved den utvalgte skolen. Undersøkelsen er gjennomført i Questback, og spørsmålene er å finne i vedlegg 5. Spørreundersøkelsen ble totalt sendt til 54 ansatte og ledere i kommunen, herunder til 14 rektorer i grunnskolene og styrere for barnehagene. Ved utløp av svarfristen var det 31 av 54 som hadde besvart undersøkelsen. Det gir en svarprosent på 57 %. Ved gjennomgang av respondentene viste det seg at det kun var 5 av 19 lærere som hadde svart på undersøkelsen, og vi valgte dermed å ta bort denne gruppen i analysen av svarene. Dette på bakgrunn av at svarprosenten fra denne gruppen var så lav at det ville bli vanskelig å trekke noen generelle slutninger på et så lite grunnlag. Faktagrunnlaget som bygger på spørreundersøkelsen har derfor reelt sett en svarprosent på 74 %, og gir et godt grunnlag for analysen, som presenteres i rapporten.

2.6 Systemgjennomsyn

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

2.7 Validitet og reliabilitet

Vi har 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.

På denne bakgrunn mener vi at rapporten fremstiller kommunen på en mest mulig riktig måte, og at vi har et godt grunnlag for våre konklusjoner og anbefalinger.

Undersøkelsen er gjennomført av Karianne Åsheim og Unn Elisabeth West i perioden 05.06.2019 til 29.10.2019.

3 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*

For utledningen av revisjonskriteriene, se vedlegg 1. Revisjonskriterier fremkommer punktvis under hvert tema. Revisjonskriterier ble også oversendt kommunen i forkant av oppstartsmøtet 16.07.2019, med muligheter for innspill fra kommunen. Kommunen hadde ingen kommentarer til kriteriene.

4 IMPLEMENTERING AV PERSONVERNREGLEMENTET

4.1 Lovlig, rettferdig og gjennomsiktig

4.1.1 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

Halden kommune informerer enkeltpersoner om hvordan de behandler personopplysninger blant annet gjennom en personvernerklæring. Personvernerklæringen gir kommunens innbyggere informasjon om hvem som er behandlingsansvarlig, hva kommunen behandler av personopplysninger, formålet med behandlingen av personopplysninger om den enkelte, hva som er det rettslige grunnlaget for behandlingen, hvordan personopplysningene samles inn, beskyttes og lagres. I personvernerklæringen fremkommer det også opplysninger om den enkeltes rettigheter.

Kommunens personvernerklæring var lagt under *Selvbetjening* på kommunens nettsider (per 04.10.19). Etter intervjuene første dag la kommunen personvernerklæringen også ut på første side. Den er nå å finne i et eget menyvalg på kommunens nettsider. På kommunens selvbetjeningsside blir brukerne opplyst om at de bør lese personvernerklæringen før de benytter skjemaer i selvbetjeningen. Det er en link til personvernerklæringen under denne informasjonen.

Ved gjennomgang av kommunens nettsider fant revisjonen også en annen personvernerklæring, som var knyttet til de elektroniske søknadsskjemaene på kommunens nettsider. Denne personvernerklæringen var ikke oppdatert etter gjeldende regelverk og hadde et annet innhold (per 30.09.19). I intervjuene kom det frem at dette hadde kommunen selv oppdaget. Den oppdaterte Personvernerklæringen ble sendt til Kommuneforlaget for oppdatering 26.09.2019 og den ble byttet ut i de elektroniske skjemaene den 01.10.19.

For å benytte de elektroniske søknadsskjemaene, har kommunen lagt inn som krav, at søkerne må bekrefte at Personvernerklæringen er lest før det er mulig å fylle ut skjemaene. Det kommer frem av intervjuene at personvernerklæringen også blir levert som vedlegg til alle papirskjema som blir benyttet. Den er da stiftet fast til søknadsskjemaet.

Kommunen har utarbeidet en Prosedyre for behandling av personopplysninger etter GDPR. I punkt 6. i denne prosedyren fremkommer det at *«Kommunens personvernerklæring skal være lett tilgjengelig og skrevet på en forståelig måte. All informasjon om hvordan kommunen behandler personopplysninger skal være tilpasset målgruppa, for eksempel barn på ulike alderstrinn»*. I intervjuene kommer det frem at kommunens personvernerklæring er ment å gjelde for alle områder og alle brukere i kommunen. Revisjonen kunne ikke finne at kommunen hadde utarbeidet informasjon som var tilpasset for eksempel barn og unge på området. I intervjuene fremkom det at kommunen vil vurdere om den gjeldende personvernerklæringen var tilstrekkelig tilpasset alle målgrupper i kommunen.

I kommunens personvernerklæring informeres det om at kommunen i noen tilfeller behandler personopplysninger basert på samtykke. Dette er en generell opplysning. I intervjuene sier ansatte at de vurderer når det er behov for samtykke for å behandle noen typer personopplysninger.

Det kommer frem av intervjuene at de har drøftet hva det er behov for samtykke til. Noen enheter er flinke til å be om samtykke til innhenting av særskilte personopplysninger, som ikke er påkrevd for å utføre oppgavene. Kommunen har ikke en felles rutine på å be om særskilte opplysninger, men ansatte sier i intervjuene at det burde de kanskje ha.

Det har blitt drøftet om noen personopplysninger kan hentes inn med samtykke, som for eksempel fra en skole om dette med seksuell legning. Etter en kort drøfting konkluderte skolen selv med at det er opplysninger de ikke har bruk for.

I spørreundersøkelsen sier 88,5 % av de lederne vi har spurt at de kjenner til hvilke personopplysninger de må ha samtykke til, for å innhente. 11,5 % svarer at de ikke kjenner til hvilke personopplysninger som de må ha samtykke til for å innhente.

<u>Kameraovervåking</u>
Det kommer frem av dokumentasjonen at kommunen har utarbeidet en oversikt over kommunens kameraovervåking. Det er oppført at det er kameraovervåking åtte steder i kommunen, alle er varslet med skilting. I intervjuene sier personvernombudet at hun har sendt ut forespørsel til alle enheter og bedt dem rapportere inn hvor det er kameraovervåking, hvor mange kameraer, hensikten med overvåkingen mm. Personvernombudet opplyser imidlertid om at hun ved en tilfeldighet har oppdaget et sted med kommunal kameraovervåking, som ikke er rapportert inn. Personvernombudet har også oppdaget at det har vært skiltet kameraovervåking et sted som det ikke er kameraovervåking. I intervjuene fremkommer det at Personvernombudet har sørget for å registrere det ikke-rapporterte kameraet og gitt enheten med skilting uten kamera, beskjed om at skiltet må fjernes.

I gjennomgangen av kommunens nettsider fremkommer det at kommunen har flere webkameraer plassert ulike steder i kommunen. I intervjuene sies det at det ikke er gjort en vurdering av lovligheten av disse kameraene. Det er heller ikke lagt ut informasjon om lovligheten, og formålet med disse kameraene.

<u>Ansatte</u>
Av behandlingsprotokollen kommer det frem at ansatte blir opplyst om behandlingen av

personopplysninger i arbeidsavtaler, stillingsbeskrivelser, arbeidsplaner og annet, som knytter seg til et ansettelsesforhold. Dette blir bekreftet i intervjuene.

Det blir sagt i intervjuene at kommunen ikke har fag- eller styringssystemer, der det er mulig å overvåke de ansatte. Det er mulig å se hvor mange utskrifter de ansatte tar, da dette går via adgangskortet til den ansatte. Det er mulig å se hvor mange e-poster som går inn og ut, mottagere, avsendere, tittel og når det er levert, men ikke innholdet. Det er ikke mulig å se hvilke nettsider den ansatte er inne på. På filområdet kan de se på hvem som eier et dokument. Opplysningene blir ikke satt sammen på noen måte.

I intervjuene kommer det frem at kommunen loggfører ansattes inn- og utganger i kommunens bygg, der det kreves identifikasjonskort for gjennomgang. Denne loggføringen oppbevares i tre måneder før den slettes. Sporing av adganger skjer kun når dørene er låst og mange av dørene er åpne på dagtid. I dokumentet *Sikkerhetspolitikk for bruk av IT i Halden kommune*, står det om adgangskontroll i pkt 1.29. Her fremkommer det informasjon om at det er adgangskontroller og hvilken enhet som administrerer adgangskontrollsystemet. Det fremkommer ikke opplysninger om at sporing av adganger loggføres og oppbevares.

Adgangskontrollen er behandlet og registrert i protokoll for behandling av personopplysninger. De ansatte er ikke informert om loggføringen, ei heller formålet med å registrere disse opplysningene. Det kommer frem av intervjuene at Servicesenteret har diskutert dette med personvernombudet, og vil vurdere hvordan de skal informere ansatte om dette.

Protokoll

I oversendt dokumentasjon fra kommunen foreligger det to eksempler på behandlingsaktiviteter – kameraovervåking på Wiels plass og ansettelser. Det fremkommer at det er gjort en vurdering av lovligheten av innsamlingen av personopplysningene gjennom en beskrivelse av det rettslige grunnlaget for behandlingen. I intervjuene kommer det frem at nye rutiner nå tilsier, at kommunen skal gjøre en vurdering av det rettslige grunnlaget ved innhenting av alle typer personopplysninger. I intervjuene sier ansatte at de er godt i gang med dette arbeidet, men de er ennå ikke helt i mål med å protokollføre alle behandlingsaktivitetene i kommunen.

Da kommunen startet å føre behandlingene av personopplysninger inn i protokollen var det GDPR-gruppen som hadde ansvar for denne oppgaven. Personvernombudet mener at avdelingslederne og/eller enhetslederne, som kjenner sitt område best, burde ha ansvaret for å føre behandlingene i protokollen. Per i dag har ikke alle enhetene lagt inn behandlingene de har ansvar for. Personvernombudet opplyser om at de er ferdig med registreringene på helse, er i gang med skole. De har også en del på kameraovervåking, servicesenteret og politisk sekretariat. Det fremkommer av intervjuene at barnevernsområdet ikke er ferdig, men at de mener å ha god oversikt over det videre arbeidet med registreringene.

Revisjonen fikk se gjennom protokollen i kommunens lokaler 08.10.19. Protokollen er å finne i Risk Manager. Det fremkommer av protokollen at de hittil har registrert 91 behandlinger, hvorav 56 er behandlet og 35 ennå ikke er behandlet. Det kommer frem av intervjuene at kommunen fremdeles oppdager nye behandlinger som må registreres i protokollen, og at antallet behandlinger vil kunne øke frem mot årsskiftet. På noen områder ser de at det er utfordrende å avgjøre på hvilket detaljeringsnivå behandlingen skal registreres. For å få bedre oversikt vil kommunen gjøre en jobb med å dele inn behandlingene på de ulike kommunale områdene.

Kommunens behandlingsprotokoll inneholder opplysninger om

- Behandlingsansvarlige
- kategorier av registrerte
- hjemmelsgrunnlaget
- formålet
- hvor opplysningene hentes fra
- hva som blir registrert av opplysninger
- hvordan opplysningene skal brukes
- hvordan den registrerte er informert om behandlingen
- opplysninger om lagring og evt overføring av opplysninger
- tilganger
- retting og sletting av personopplysninger

Flere av de vi intervjuet sa at de opplever at kommunens ledelse – rådmannen – har prioritert arbeidet med personvern. De opplever nå å få lov til å bruke tid til å gjøre en god jobb på området. De sier at de er på god vei til å få implementert personvernregelverket, men at det fremdeles er en del arbeid som gjenstår.

Enhet – grunnskole

Som nevnt innledningsvis har kommunen ønsket at revisjonen også skal se nærmere på enhet - grunnskole i denne revisjonen.

I intervjuene kommer det frem at det er ulikt hva skolene informerer om når det kommer til behandling av personopplysninger. I intervjuene med ansatte i en utvalgt skole fremkommer det at denne typen informasjon som regel blir kommunisert muntlig ved innskriving på skolen, som regel i første klasse. Etter en gjennomgang av nettsidene til skolene i kommunen ser vi at ingen skoler har valgt å kommunisere formålet og rettigheter mv. ved behandling av personopplysninger på nettsidene sine. Det er en link på førstesiden på skolenes nettsider om personvern og cookies. Den omhandler kun bruk av nettsidene, og er en standard utarbeidet av Moava AS, som er databehandler på dette området. I intervjuene sier kommunalsjef undervisning og oppvekst at det bør utarbeides en egen personvernerklæring for skolene også.

I intervjuene sier ansatte i skolen at de opplever å ha god oversikt over hvilke særskilte kategorier personopplysninger de skal be om samtykke for å innhente. De ber for eksempel foreldre om samtykke for å innhente for eksempel opplysninger om elevene har allergier. Det er foreldrene som fyller ut skjema med personopplysninger selv.

I intervjuene kommer det frem at kommunalsjef undervisning og oppvekst ennå ikke er involvert i arbeidet med behandlingene på sitt fagområde. Kommunalsjefen kjenner til behandlingsprotokollen og sier at kommunen vil jobbe med å få protokollen på plass.

Vurderinger

Personvernregelverket sier at informasjon om behandling av personopplysninger skal gis skriftlig eller på annen måte, herunder elektronisk. Virksomheten må derfor selv finne en passende måte å gi

informasjonen på, innenfor visse rammer. Plikten til å behandle personopplysninger på en åpen måte, innebærer at virksomheten må gi kort og forståelig informasjon om hvordan de behandler personopplysningene. Det stilles også krav til hvordan det kommuniseres med enkeltpersoner. 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 måter. For at behandlingen skal være lovlig må det finnes et rettslig grunnlag for behandlingen av personopplysningene. Dette området er vurdert under formålsbegrenset.

Det er vår vurdering at kommunen i sin personvernerklæring gir opplysninger om de ulike sidene ved innhenting og behandling av personopplysninger, og personers rettigheter på en kortfattet og forståelig måte for mange i målgruppen. Under revisjonen la kommunen personvernerklæringen til den overordnede menyen på kommunens nettsider. Det er nå vår vurdering at kommunens personvernerklæring fremstår som lett tilgjengelig og åpen informasjon til mange av brukerne av kommunens tjenester.

Det er imidlertid vår vurdering at informasjonen ikke er klar og tydelig for alle målgrupper i kommunen. Dette gjelder blant annet for barn og unge. 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.*» Kommunen har utarbeidet en *Prosedyre for behandling av personopplysninger etter GDPR.* I punkt 6. i denne prosedyren fremkommer det at «*Kommunens personvernerklæring skal være lett tilgjengelig og skrevet på en forståelig måte. All informasjon om hvordan kommunen behandler personopplysninger skal være tilpasset målgruppa, for eksempel barn på ulike alderstrinn*». Det er vår vurdering at opplysningene i den overordnede 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 og lagres. Heller ikke når det gjelder barn og unges rettigheter.

Vi ser at kommunen jobber med å oppdatere rutiner, dokumenter og informasjon i tråd med den nye personvernlovgivningen. Under revisjonen oppdaget kommunen selv at personvernerklæringen knyttet til de elektroniske søknadsskjemaene ikke var oppdatert etter gjeldende regelverk og rettet opp i dette. Det ser vi som svært positivt.

<u>Samtykke</u>
I kommunens personvernerklæring informeres det generelt om at kommunen i noen tilfeller behandler personopplysninger basert på samtykke.

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.

Intervjuene viser at ansatte vurderer når det er behov for samtykke for å behandle noen typer personopplysninger. Det kommer imidlertid frem av spørreundersøkelsen at 11,5 % av kommunens ledere som har besvart spørreundersøkelsen, ikke kjenner til hvilke personopplysninger som de må ha samtykke til for å innhente. Etter vår oppfatning kan dette indikere manglende opplæring på området, eller at enhetene ikke har gjort en konkret vurdering av personopplysninger de innhenter. Det fremstår som om de ansatte opplever en usikkerhet på dette området.

Kameraovervåking

For å sikre at kommunen bruker kameraovervåking i henhold til retningslinjene og sørge for å ikke benytte for eksempel skilting og oppslag eller lignende for å gi inntrykk av at kameraovervåking finner sted, er det nødvendig at kommunen har en oversikt over all kameraovervåking og skilting av dette. Det er vår vurdering at kommunes personvernombud har jobbet for å få inn informasjon om kommunal kameraovervåking og varsling av kameraovervåking, slik at regelverket kan overholdes. Vi mener det er uheldig at ikke alle enhetene følger opp anmodningen om å melde inn om det er kameraovervåking i deres enhet, og det kan se ut til at ledere av enheter med kameraovervåking og/eller skilting ikke er orientert godt nok om regelverket på dette området.
Kommunen har ikke tatt med webkameraene[1] i sine vurderinger. Det er vår vurdering at kommunen også bør gjennomføre en behandling av sine webkameraer og blant annet vurdere om deter mulig å identifisere personer eller ikke. Formålet med webkameraene og eventuell muligheten/ikke mulighet til å identifisere personer mm bør formidles til kommunens innbyggere på kommunens nettside.

Ansatte

I veileder om kontroll og overvåking i arbeidslivet, står det at det er et grunnleggende prinsipp at alle har krav på personvern og privatliv – også på jobb.

Kommunens loggføring av ansattes bevegelser i kommunens bygg, der det kreves identifikasjonskort er en adgangskontroll. Selv om hensikten med adgangskontroll kan være innlysende, skal det være skriftlig nedfelt hva som er formålet med behandlingen på lik linje med andre typer behandlinger av personopplysninger. På bakgrunn av intervjuene og gjennomgang av protokoll for behandlinger, er det vår vurdering at kommunen har håndtert adgangskontrollen etter personvernregelverket. Vi mener imidlertid at ansatte bør informeres om loggføringen, bruken og hensikten med adgangskontrollen. Som et minimum bør dette beskrives i kommunens dokument Sikkerhetspolitikk for bruk av IT i Halden kommune, om adgangskontroll.

Protokoll

Kommunen sier selv at de hittil har registrert 91 behandlinger, hvorav 56 er behandlet og 35 ennå ikke er behandlet. Kommunen sier også at det fremdeles oppdages nye behandlinger som må registreres i protokollen. Vi støtter personvernombudet i vurderingen av at avdelingslederne og/eller enhetslederne, som kjenner sitt område best, burde ha et større ansvar for å føre behandlingene på sitt fagområde i protokollen. Det vil etter vår vurdering føre til en mer effektiv og kvalitetsmessig sikring av føringene i behandlingsprotokollen.

Det er vår vurdering at kommunen har kommet godt i gang med å føre protokoll over behandlingsaktiviteter som utføres under deres ansvar. Protokollen er skriftlig. Etter revisjonens oppfatning gjenstår det fremdeles en del arbeid på området.

Enhet - skole

I personvernforordningen artikkel 12 om den registrertes rettigheter står det, «*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*, …….». Det er derfor vår vurdering at det ikke er tilstrekkelig å kun informere foreldre og elever muntlig ved innskriving i skolen, på første trinn.

[1] Et webkamera er et digitalt kamera som brukes til å kommunisere med andre over internett eller som et overvåkningskamera slik at man kan gå inn på en nettadresse å se.

4.1.2 Personers rettigheter

Revisjonskriterier

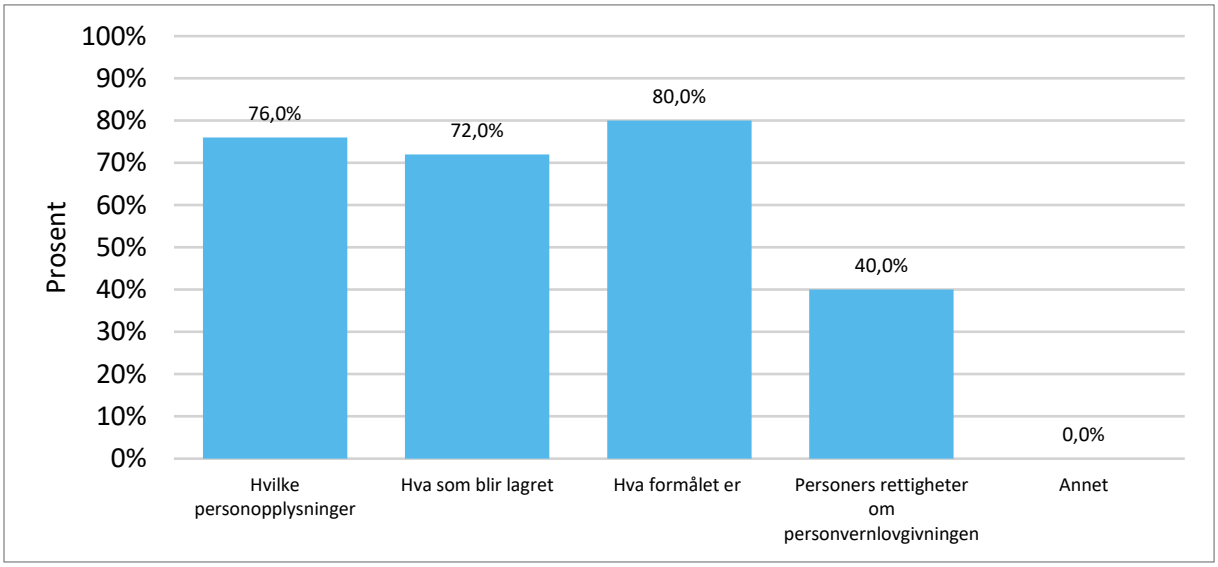
- Kommunen skal sørge for å overføre nevnte opplysninger til en annen behandlingsansvarlig når den registrerte ber om det og det er teknisk mulig (dataportabilitet).
- Kommunen ivaretar retten til innsyn i personopplysningene (hvor de kommer fra, hvordan de behandles og en kopi av registrerte opplysninger).
- 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.

Fakta

Det fremkommer av kommunens personvernerklæring at det der er opplyst om enkeltpersoners rettigheter. Kommunen har utarbeidet et eget skjema for innsyn i personopplysninger - *Skjema innsyn*. Dette skjema finnes som lenke i personvernerklæringen.

I spørreundersøkelsen kommer det frem at det er noe variasjon i hva kommunens ledere informerer brukerne av kommunens tjenester om, når det gjelder behandlingen av personopplysninger og personers rettigheter. Som vist i figur 4 har 40 % svart at de opplyser om personers rettigheter, mens 80 % svarer at de informerer om formålet med behandlingen.

Figur 4: Hva informerer dere brukere og pårørende om når det gjelder hvordan dere lagrer og bruker personopplysninger?



Antall respondenter: 25

Kommunen har utarbeidet *Prosedyre for svar på forespørsel om innsyn i egne personopplysninger GDPR*. Det fremkommer ikke når denne er utarbeidet, og ikke om den er godkjent på nåværende tidspunkt. I prosedyren står det «*Post/arkiv er ansvarlig for registrering av innsynsforespørselen i sak/arkiv-systemet, og å sende til kommunalsjefen(e). Kommunalsjefene er ansvarlig for å be sine ledere om å finne frem dokumentasjonen som etterspørres fra innbyggeren, for deretter å oversende*

til personvernombudet. Enhetslederne er ansvarlig for at enhetene svarer opp til rett tid, slik at fristen for svar til innbyggeren kommer til rett tid (senest innen 30dager). Personvernombudet er ansvarlig for sammenstilling av dokumentene, og å sende disse samlet til innbyggeren via Svar Ut. Personvernombudet fører logg over innsynsbegjæringer, slik at det er oversiktlig når Datatilsynet kommer på tilsyn.»

I intervjuene kommer det frem at personvernombudet ikke kjenner til at de har mottatt innsynskrav på personopplysninger etter at hun startet i jobben våren 2018.

Enhet - skole

Ansatte på skolen informerer i intervjuene om at de har hatt innsynskrav fra elever som vil se mappen sin. De har også foreldre som ber om innsyn i opplysningene i mappene om sine barn. Dersom det er saker som skolen ikke har kunnet gi innsyn i, sender skolen de som ber om innsyn videre til kommuneadministrasjonen.

Vurderinger

På bakgrunn av det som kommer frem i intervjuene og gjennomgangen av kommunens nettsider, er det vår vurdering at kommunen gir brukerne av kommunens tjenester informasjon om behandlingen av personopplysninger. Av spørreundersøkelsen kan det imidlertid se ut til at det er få som opplyser om personers rettigheter i tilknytning til dette. Det er vår vurdering at når kommunen informerer om hvilke personopplysninger kommunen samler inn, behandlingen av personopplysninger og formålet, bør det samtidig informeres om personers rettigheter til innsyn, retting og sletting.

Skjema for innsyn i egne personopplysninger kan med fordel også lenkes i listen for selvbetjening med andre skjemaer, som innsyn i kommunens dokumenter.

4.2 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 forenelig med det personopplysningene opprinnelig ble samlet inn til.
- Kommunen har kunnskap om personopplysninger benyttes til andre formål enn det de er samlet inn til.

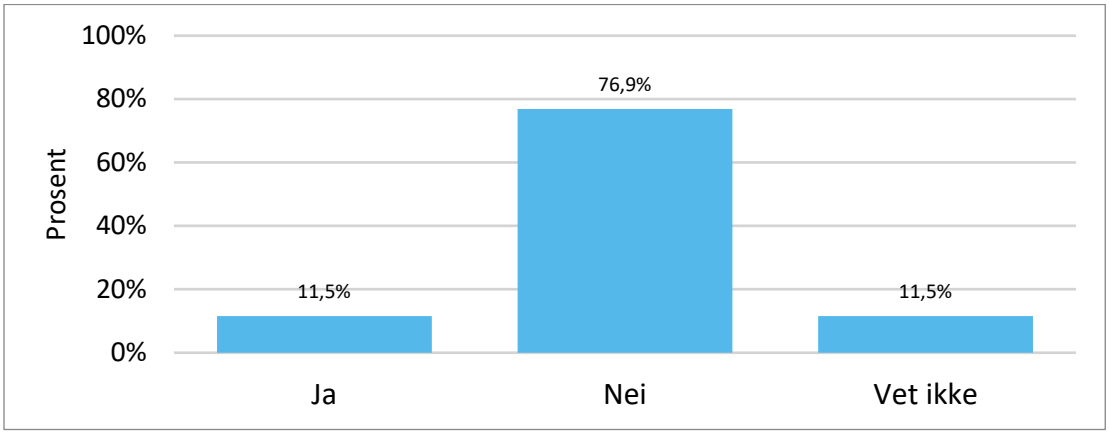
Fakta

I protokollen over behandlingsaktivitetene i kommunen fremkommer en beskrivelse av formålet med innhentingen av opplysninger. I intervjuene kommer det frem at kommunen gjør en vurdering av formålet med innhenting av alle personopplysninger.

Personvernombudet opplyser om at de har lagt inn felt for beskrivelse av formålet inn i malen for behandlinger i protokollen. Hver enhet må fylle ut formålet med behandlingen selv. Det administrasjonen vet om formålet er allerede forhåndsutfylt, men resten må enhetene fylle ut selv.

76,9 % av kommunens ledere, som deltok i spørreundersøkelsen, svarer at de kun henter inn opplysninger som er relevant for formålet. Det er også noen som sier de samler inn opplysninger som er «kjekt å vite» og noen som ikke vet om det kun samles inn personopplysninger som er relevante for formålet. Se figur 1.

Figur 1: «Samler dere inn personopplysninger som er "kjekt å vite", men som ikke er direkte relevant for formålet?»



Antall respondenter: 26

I kommunens *Prosedyre for behandling av personopplysninger etter GDPR*, pkt 5 om personvernprinsipper står det «kommunen skal ikke registrere flere opplysninger enn det som er nødvendig for formålet». I dokumentet «Sikkerhetspolitikk for behandling av personopplysninger, pkt 3.2.2 står det «*Opplysninger i offentlige registre hvor registrering er pliktig, skal være lovhjemlet*»

Når det gjelder innhenting av personopplysninger fra de ansatte så kommer det frem i intervjuene at det innhentes kun opplysninger som er nødvendig for at kommunen skal kunne ivareta arbeidsgivers plikter og ansattes rettigheter. Dette er informasjon til lønnsbehandlinger, HMS, tilganger til ulike systemer og annet som en arbeidsgiver har behov for, for å kunne ivareta de ansatte og kommunens oppgaver.

Vurderinger

På bakgrunn av resultatene fra spørreundersøkelsen og intervjuene er det vår vurdering at kommunen på de fleste områder kun samler inn opplysninger som er relevante for formålet. Det er imidlertid 23 % av lederne som deltok i spørreundersøkelsen, som svarer «vet ikke» eller «ja» til at de samler inn opplysninger som ikke er relevant for formålet. Det kan være flere årsaker til at de svarer dette. En årsak kan være manglende opplæring i hva som er relevant for formålet. Etter vår vurdering henger dette sammen med at 23 % også sier at de ikke har vurdert om de har rettslig grunnlag til å behandle personopplysningene de samler inn.

Det er vår vurdering at kommunen ikke i tilstrekkelig grad har sørget for at opplysninger kun samles inn for relevante og lovlige formål.

4.3 Dataminimering

Revisjonskriterier

- Kommunen gjør en vurdering av om de innsamlede opplysningen 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.
- Kommunen bruker fødselsnummer eller andre entydige identifikasjonsmidler kun når det er saklig behov for sikker identifisering.

Fakta

I dokumentet *Sikkerhetspolitikk for behandling av personopplysninger* står det i pkt. 3.2.6 at opplysninger som ikke lenger er nødvendig for formålet skal slettes eller sperres. Det blir her også vist til at en må ta hensyn til blant annet arkivlovens krav om oppbevaring av dokumentasjon når det blir gjort en vurdering av å slette personopplysninger og dokumenter. I kommunens protokoll, under hver behandlingsaktivitet er det en link til sletterutiner. I intervjuene med avdelingsleder og enhetsleder i kommunen kommer det frem at de kjenner dokumentet og har blitt informert om at det er førende for behandling av personopplysninger.

Det kommer frem av intervjuene at personvernombudet og arkivleder samarbeider mye. De opplever å ha god kontroll på hva som er arkivverdige personopplysninger og hva som kan slettes.

Vurderinger

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.

Det er vår vurdering at kommunen har etablert rutiner for at opplysninger som ikke lenger er nødvendig for formålet skal slettes eller sperres. På bakgrunn av det som fremkommer under punkt 4.2 om formålsbegrensning og lagring av personopplysninger om ansatte er det imidlertid vår vurdering at rutinen ikke er implementert i tilstrekkelig grad i virksomheten.

4.4 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

I dokumentet *Sikkerhetspolitikk for behandling av personopplysninger* står det i pkt. 3.2.5 og 3.2.6 at opplysningene skal være korrekte og ajourførte og at feilaktige personopplysninger skal endres, slettes eller sperres.

I kommunens personvernerklæring blir det informert om at personer har rett til å få rettet opp i feilaktige eller mangelfulle personopplysninger.

I intervjuene kommer det frem at brukere av kommunens tjenester ofte tar kontakt med post/arkiv når det gjelder uriktige personopplysninger. Arkiv har en kontrollfunksjon når det gjelder å kontrollere at personopplysninger er riktig registrert i arkivsystemene. Brukerne oppdager som regel feilføringer selv.

Vurderinger

Det er vår vurdering at kommunen har en rutine som skal sikre at opplysninger blir rettet dersom det blir oppdaget feil, mangler eller den registrerte ber om det. Fakta viser også at kommunen gjennomfører slik retting når det blir oppdaget av kommunen selv eller når den registrerte ber om det.

4.5 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 personvernerklæring fremkommer det et punkt om at personopplysningene lagres i kommunens fagsystemer og at opplysningene lagres så lenge det er nødvendig for formålet de er samlet inn for. I intervjuene vises det også til Bevarings- og kassasjonsplan for Halden kommune.

Denne gir en oversikt over de dokumenter som kommunen må bevare etter Arkivloven, Arkivforskriften og Riksarkivarens forskrift. Den gir videre en oversikt over dokumenter kommunen velger å bevare, i tillegg til de som er pålagt. Den gir også en oversikt over dokumenter kommunen kan slette/kassere og frist for kassasjon. Planen har ingen henvisninger til personvernlovgivningen, når det gjelder lagringsbegrensinger eller bevaring. I saker det ikke er et krav om arkivering i henhold til regelverket, gjør kommunen selv en vurdering om de skal bevare eller kassere dokumentasjonen. Det fremkommer ikke om det blir gjort en vurdering av hver enkelt sak knyttet til lagring eller sletting av personopplysninger som ikke har krav om arkivering.

Arkivleder informerer om at arkivet veileder mye om kassasjon og bevaring knyttet til papirarkiv ut til enhetene.

Det kommer frem av protokollen at opptakene fra kameraovervåkingen automatisk slettes etter syv dager. Dersom opptakene er å anse som dokumentasjon i politiets arbeid med oppklaring av straffbare forhold, kan grunnlag for å oppbevare opptakene være lenger enn syv dager.

I kommunens dokument *Sikkerhetspolitikk for behandling av personopplysninger* er det utarbeidet en oversikt over de ulike kategoriene personopplysningene som behandles i kommunen og hvor disse er lagret.

Ansatte

Det kommer frem av intervjuene at kommunen har diskutert om advarsler til ansatte skal slettes eller ikke slettes. Kommunen har vurdert at de skal beholde opplysningene på ubestemt tid. Dette fordi det kan komme rettssaker i ettertid, eller ansatte kan bli tilsatt igjen.

I AKAN-saker, varslingssaker og annet, bruker personal HR Norge sine retningslinjer ang. hvor lenge info skal oppbevares (i 2 år). Det blir opplyst i intervjuene at når ansatte slutter eller går av med pensjon, så blir AKAN saker slettet umiddelbart. Kommunen håper å få lagt inn noen automatiske varslinger i ephorte nå og senere i Elements, når dette verktøyet skal tas i bruk.

Vurderinger

Det er vår vurdering at kommunen gjennomgår og gjør en vurdering av om og når personopplysninger om ansatte skal slettes. Det gjelder også mer sensitive opplysninger som personopplysninger i blant annet AKAN-saker. Kommunen sier at de har vurdert å bevare alle advarsler til ansatte på ubestemt tid, på grunn av muligheter for en evt. rettsak eller at vedkommende kan søke jobb i kommunen igjen. Det er vår vurdering at dersom det er grunn til å tro at det kan oppstå arbeidsrettssak i ettertid, må arbeidsgiver kunne beholde personalmappen, med dokumentasjon om for eksempel advarsler. I slike tilfeller har arbeidsgiver en berettiget interesse til å oppbevare dokumentasjonen frem til alle søksmålsfrister er utløpt. I tilfeller der ansettelsesforholdet blir avsluttet ved avskjed, kan det være grunnlag for at arbeidsgiver kan beholde informasjon om dette i lengere tid. Datatilsynet anfører at arbeidsgiver må vurdere konkret hvor lenge det er nødvendig og forsvarlig å beholde opplysningene i det enkelte tilfelle. Dersom en advarsel ikke får noen konsekvens, er det vår vurdering at opplysningen ikke lenger er nødvendig for formålet og må slettes.

Det er vår anbefaling at kommunen bør gjennomgå Bevarings- og kassasjonsplan for Halden kommune i lys av den nye personvernlovgivningen. Dette gjelder på de områdene det ikke er en plikt

til arkivering i henhold til regelverket og kommunen selv vurderer om de vil bevare eller kassere dokumentasjonen. Eksempelvis bør kommunen vurdere hvor lenge advarsler, varsler, anmerkninger osv., skal lagres. Tilsvarende gjelder anmerkninger i skole. Kommunen må gjøre en vurdering i hvert enkelt tilfelle om og hvor lenge disse opplysningene skal oppbevares. Formålet med oppbevaringen er sentral i denne vurderingen. Dersom formålet er å dokumentere noe som fikk en konsekvens eller kan få en konsekvens på et senere tidspunkt, kan det være aktuelt å lagre opplysningene, da er formålet med lagringen et annet enn det opplysningene ble samlet inn til i første omgang. Dersom opplysningene ikke har fått eller kan få konsekvenser, skal de slettes hvis de ikke er arkivpliktige eller av historisk, vitenskapelig eller statistisk betydning.

4.6 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

I dokumentet *Sikkerhetspolitikk for behandling av personopplysninger* står det *«…Informasjon om informasjonssystemet og om sikkerhetstiltak skal også sikres mot uautorisert endring når dette er nødvendig for informasjonssikkerheten*. *Halden kommune har tiltak mot ødeleggende programvare som for eksempel "datavirus" som kan ødelegge integriteten*. I det samme dokumentet finnes det en oversikt over de fagsystemene som personopplysningene registreres i, for de ulike avdelingene og enhetene i kommunen. Det fremkommer også en kolonne som angir hvilke sikringstiltak som er gjort og hvor lagringen av opplysningene fysisk sett befinner seg.

I intervjuene kommer det frem at kommunen også har papirdokumenter med personopplysninger. Servicesenteret ligger i en sikker sone dvs. lokalene er sikret med adgangskontroll og bare enkelte ansatte har tilgang til denne sonen, her ligger bl.a. alle innkomne søknader før kommunen får sendt dem videre. Papirene oppbevares i en papirperm som er låst inn. Papirpermene oppbevares avskjermet med et nøkkelsystem. Det er kun saksansvarlig som har tilgang til opplysningene og dokumentene er sikret med et nøkkellås system med flere sluser for avgrenset tilgang. I intervjuene sier ansatte at de også har gjort tiltak for å sikre innsyn mellom besøkssonene og ansatte, slik at besøkende ikke ser PC-skjermene der det kan fremkomme personopplysninger.

I intervjuene sier ansatte at både de ulike fagsystemene og arkiv- og dokumentsystemet ephorte med personopplysninger, har tilgangsavgrensing. Også her er det kun den som er ansvarlig saksbehandler som har tilgang til å se personopplysningene i sine saker. Det gjelder også for tilganger

til personalmappene. For ansatte i arkivet er det også gitt tilgangsavgrensing. Det er kun arkivansatte med ansvar for de ulike typene saker som har tilgang til å registrere og lagre dokumenter i disse.

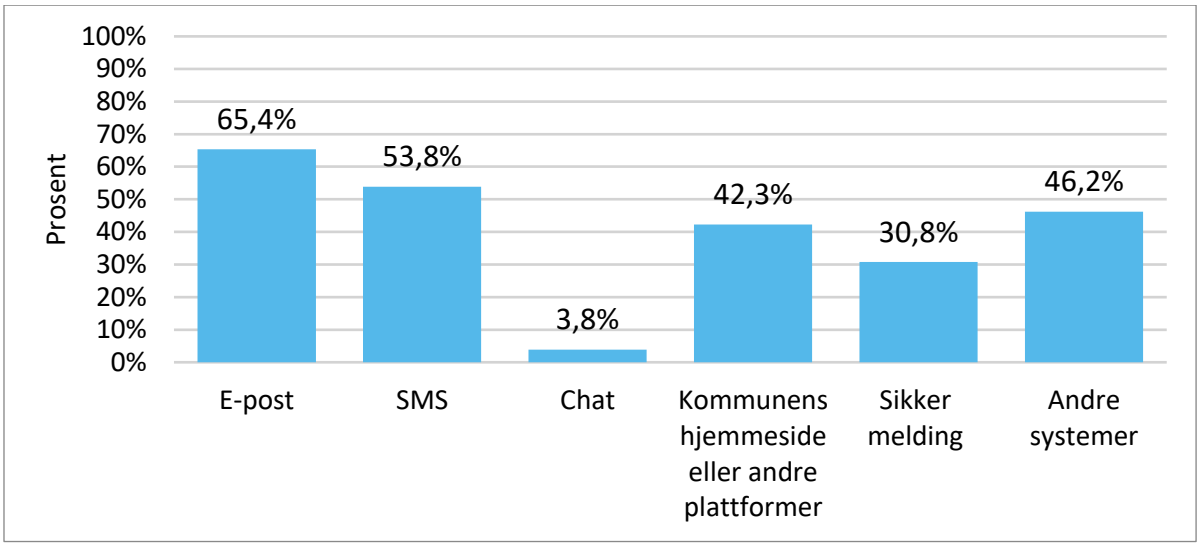
IT-avdelingen er involvert i arbeidet med å gi tilganger i sak-/arkivsystemet ephorte og samarbeider med arkiv på dette. Det er kommunalsjefene, som har ansvaret for å vurdere hvem som skal ha tilgang til hva. Dette fremkommer i kommunens arkivrutine.

Halden kommune har satt IT-drift til selskapet Visolit. Det kommer frem av intervjuene at dette gjør at kommunen må ha ekstra god oversikt over de opplysninger som blir innhentet og lagt i systemet. Per i dag bruker kommunen et elektronisk tilgangsskjema hvor det innhentes opplysninger fra den ansatte om navn, ansattnr., hvor i kommunen den ansatte jobber, om det er en nyansatt og hvilke tilganger de skal ha i de ulike systemene. I dokumentet *Sikkerhetspolitikk for bruk av IT* står det «*Visolit er ansvarlig for den systemtekniske sikkerheten. Halden kommune er ansvarlig for å sjekke at den systemtekniske sikkerheten er slik Visolit beskriver at den skal være. Dette er en del av Halden kommunes egenkontroll.*»

Arkivet gir tilganger til arkivkjernen på sikker sone, men ikke tilganger i de forskjellige fagsystemene. Arkivet vurderer hva som er arkivverdig post, som skal registreres i ephorte. I intervjuet med ansatte på arkivet fremkommer det at arkivet går gjennom alle dokumenter og sjekker at alt er som det skal være for eksempel om dokumentene som er unntatt offentlighet har riktige koder.

I spørreundersøkelsen ble 26 av kommunens ledere spurt om de på deres fagområde kommuniserte med bruker og evt. pårørende på e-post, sms, chat mm.

Figur 2: «Hvilke kanaler brukes på ditt fagområde til å kommunisere med brukere og evt. pårørende?»



Antall respondenter: 26

Som svarene i figur 2 viser bruker de ansatte flere måter å kommunisere med brukere og evt. pårørende på. Over halvparten av respondentene svarer at de bruker sms.

I kommunens *Prosedyre for behandling av personopplysninger etter GDPR*, pkt 5 om personvernprinsipper, står det «*Personopplysninger skal gjennom egnede organisatoriske og tekniske tiltak beskyttes mot uautorisert eller ulovlig tilgang, utilsiktet tap, ødeleggelse eller skade*»

Kommunen har ikke noe system for overføring av informasjon fra sms til sak/arkiv per i dag. IT-sjefen sier at det ikke bør benyttes sms i saksbehandlingen. I dagens gamle ephorte er det ikke mulighet til å importere sms'er, men nå som kommunen snart skal over i Elements vil det bli tilgang på denne funksjonen. Arkivleder sier at det er svært sjeldent de ser at sms arkiveres i arkivsystemet.

Det kommer også frem av intervjuene at kommunen har jobbet mye med å få ansatte til å slutte å bruke «gule lapper», særlig med tanke på nedtegning av personopplysninger på disse. Det kommer også frem i intervjuene med ansatte i enhetene.

Flere av de vi intervjuet på administrativt nivå sier at de er bekymret for noen ansattes bruk av e-post med personopplysninger. Det vises til at kommunen har en «Bruker- og taushetserklæring», hvor det blant annet står det at man ikke skal sende sensitive opplysninger på e-post. Denne signerer alle ansatte ved tilsetting, men noen gjemmer seg bak at de ikke har signert denne erklæringen. Det fremkommer av dokumentet *Sikkerhetspolitikk for behandling av personopplysninger* og av intervjuene, at ansatte skal sette seg inn i og signere taushetserklæringen. Det er etterspurt at kommunen må gjennomføre en DPIA[2] på e-postsystemet.

Kommunen har imidlertid retningslinjer for bruk av e-post i prosedyren *Sikkerhetspolitikk for bruk av IT i Halden kommune*. I pkt 1.17 i denne prosedyren står det «*E-poster skal ikke inneholde sensitive (særlige kategorier av) personopplysninger eller andre sensitive opplysninger. Skal e-posten inneholde personopplysninger må det ikke være mulig å linke innholdet til bestemte personer (pseudonymisering)….».*

På området Rus og psykiatri er ansatte bekymret for at brukerne ikke er kapable til å bruke Digipost. De ansatte ønsker å kommunisere mer på sms. Det er da den enkelte ansatte som har ansvar for konfidensialiteten i dette, samt avdelingsleder. Kommunen har ikke utarbeidet rutiner på dette området enda, men de vil ta det med videre i GDPR-gruppa.

<u>Enhet – skole</u>

Det kommer frem av intervjuene med ansatte på skolen at det deles ut klasselister på papir til kontaktlærerne. I første omgang gis listene til lærerne og de deler videre ut til foreldre. Det er ikke fødselsnummer på disse listene. Det er i hovedsak kun navn og telefonnummer, men ved noen skoler har de også opplysninger om e-postadresser.

Ansatte opplyser om at skolen ikke samler inn opplysninger som bare er «kjekt å ha». Det blir presisert at skolen ikke henter inn informasjon om trosretning eller annen sensitiv informasjon som ikke er nødvendig for å utføre de lovpålagte oppgavene.

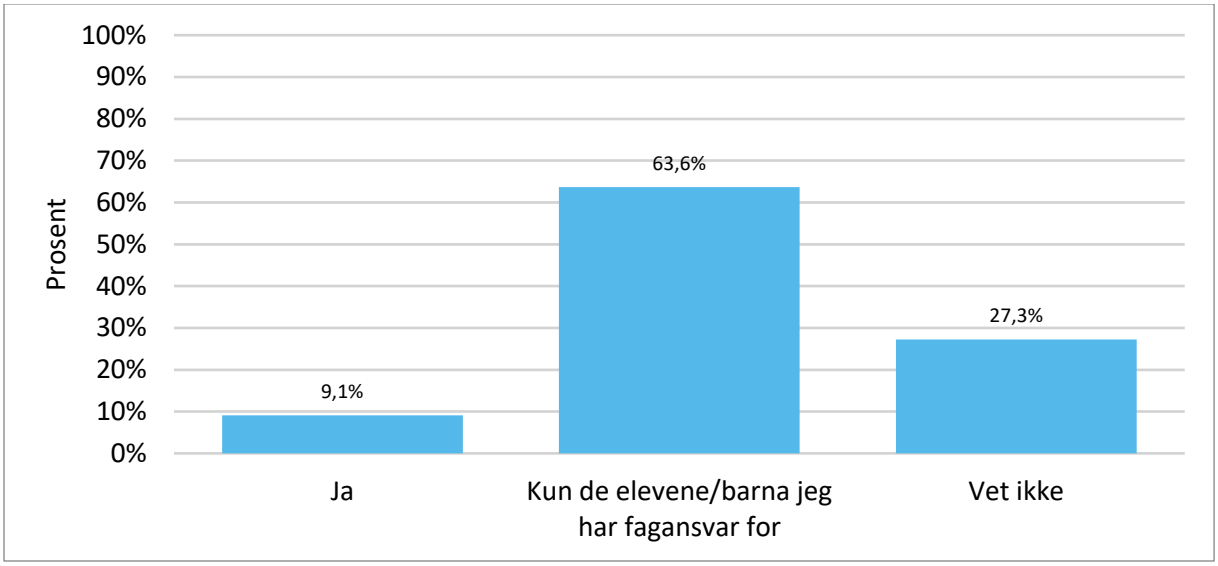
Det kommer frem i intervjuene at kontaktlærerne kommuniserer med foreldre og elever via ulike kanaler. Foreldre og elever kan sende sensitive personopplysninger via sms, Messenger eller e-post. Det kan også være personopplysninger knyttet til elever som bør arkiveres. Det fremkommer av

[2] En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i løsningen ivaretas.

intervjuene og dokumentasjon fra skolen at det ikke er innført en rutine for behandling av personopplysninger som kommer inn via sms, Messenger, chat eller liknende i dag. Dette blir bekreftet i intervjuene med kommunalsjefen. Det kommer frem av intervjuene at dersom skolene får inn sensitive opplysninger på e-post, har skolene rutine for å slette de sensitive opplysningene i svaret tilbake. Noen ansatte i skolen opplever at det er en utfordring å motta sensitive personopplysninger på egen telefon, da slik informasjon ikke alltid blir mottatt i arbeidstiden. Det kommer frem av intervjuene at skolen, vi så på i revisjonen, har sett at dette er en utfordring og vil innføre klassetelefoner for å forsøke å bøte på denne utfordringen.

I spørreundersøkelsen har rektorer på skolene og styrere i barnehagene svart på hvordan tilgangen til elev-/barnemappene er avgrenset. Som vist i figur 3 kommer det frem av spørreundersøkelsen at 63 % av rektorene og styrere i barnehagene svarer at ansatte kun har tilgang til opplysningene om de elevene/barna de har et fagansvar. 9,1 % sier at de ansatte har tilgang til alle elev-/barnemapper og 27,3 % av rektorene og styrerne sier at de ikke vet.

Figur 3: «Har lærerne/ansatte tilgang til alle elevmappene/opplysninger om det enkelte barn?»



Antall respondenter: 11

Det kommer frem av intervjuene at det i tillegg til det digitale arkivet i ephorte også finnes fysiske arkiv på skolene. På den enheten vi så på i revisjonen, kom det frem av intervjuene at lærerne ikke har tilgang til de digitale elevmappene i ephorte, da dette må gå via merkantilt ansatt på skolen. Når merkantilt ansatt ikke er tilstede har lærerne derfor ikke tilgang til de digitale emappene i ephorte. Skolen har rutine på at lærerne skal signere for hvilke elevmapper de tar ut av det fysiske arkivet. Dette kan de gjøre også når merkantilt ansatt ikke er tilstede.

Det kommer frem av intervjuene med kommunalsjefen at det har ikke vært gjort en jobb med de fysiske arkivene på skolene, etter at den nye personvernlovgivningen trådte i kraft. Kommunalsjefen sier at det er kommunen sentralt som har ansvaret for en felles rutine for avgrensing tilgangen til personopplysninger i skolene.

Avvik/brudd på personvernregelverket

Det kommer frem av intervjuene at det er meldt avvik/brudd på personvernregelverket. Alle brudd skal registreres i avviksmodulen i Risk Manager. Det er den som oppdager og eier bruddet som

rapporterer på dette. Personvernombudet står som tredjeperson i Risk Manager og er daglig inne i avviksmodulen for å kontrollere evt. brudd. Alle brudd som er meldt i avviksmodulen hittil er meldt videre til Datatilsynet. Når det meldes inne et brudd, sender personvernombudet en e-post til den som eier avviket om at de skal informere brukeren/den registrerte om hva som har skjedd.

Personvernombudet sier at de ikke har mottatt meldinger om brudd på personvernregelverket, der de har vurdert at de ikke behøver å melde det til Datatilsynet. Personvernombudet sier at da ville de lagt meldingen inn i avviksmodulen i Risk Manager. Det fremkommer av kommunens *Prosedyre for behandling av personopplysninger etter GDPR* pkt 6, *«avvik innenfor informasjonssikkerhet og personvern kalles sikkerhetsbrudd, og skal meldes i Risk Manager. Ved sikkerhetsbrudd som har ført til at menneskers personvern har blitt krenket, skal Datatilsynet varsles innen 72 timer. Dette gjelder ikke dersom det er lite trolig at sikkerhetsbruddet vil medføre en risiko for personers rettigheter og friheter. Personvernombudet skal involveres i slike saker, og er også den som melder videre til Datatilsynet når det er påkrevd (se «prosedyre for håndtering av alvorlige sikkerhetsbrudd»)».* I *Prosedyre for håndtering av alvorlige sikkerhetsbrudd* er fremgangsmåten for behandling av bruddet beskrevet i pkt 4. Personvernombudet sier at de vil sørge for å skrive ned hvilke vurderinger de har gjort dersom de mener at det ikke er nødvendig å melde avviket til Datatilsynet.

Revisjonen hadde en gjennomgang av avviksmodulen og ble vist hvor og hvordan bruddene ble registrert. Per i dag er alle typer avvik listet opp samlet. I samtaler med IT-sjefen og personvernombudet sier de at de ser for seg at dette skal systematiseres mer. Personvernombudet sier at det kommer mange avvik på ting som ikke er personvern, og de vet ikke om alt med personvern meldes heller. Det er sendt ut informasjon om hvordan avvik/brudd skal meldes, men om det blir lest og fulgt opp har de fremdeles ikke oversikt over.

Vurderinger

Det er vår vurdering at kommunen har utarbeidet rutiner og retningslinjer som skal ivareta personers integritet og konfidensialitet. Det er iverksatt tiltak for å sikre at personopplysninger ikke uautorisert blir endret i de ulike systemene for lagring av slike opplysninger, f.eks. ved at det kun er arkivansatte med ansvar for de ulike typene saker som har tilgang til å registrere og lagre dokumenter i disse.

Det er også vår vurdering at kommunen har iverksatt tiltak for å avgrense tilgang til personopplysninger i ulike program og fagsystemer, også der det finnes papirarkiv med slike opplysninger. Vi ser det som positivt at kommunen også har hatt fokus på å redusere ansattes bruk av «gule lapper» som kan inneholde personopplysninger.

Det kommer frem av intervjuer og spørreundersøkelsen at det benyttes ulike kanaler til å kommunisere med brukerne av kommunens tjenester. Det er også områder der det er ønskelig å benytte sms som kommunikasjonskanal. Vi ser at det kan være et behov i kommunen for bruk av ulike kanaler, for å nå ulike brukergrupper. Det er imidlertid vår vurdering at kommunen må ha en bevisst bruk av de ulike kanalene. Kommunen har en prosedyre for bruk av e-post når det gjelder personopplysninger. Vi mener imidlertid at kommunen også må ha en plan og en fremgangsmåte for å sikre forsvarlig behandling av personopplysninger på kanaler som kommunen ikke ønsker å benytte i sin kommunikasjon.

Behandlingsansvarlig bør beslutte på hvilke områder kommunen kan benytte sms, chat, e-post mm 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 per sms bør

dokumenteres og danne grunnlag for beslutningen. I dette må også kommunen gjøre en vurdering av lagring og sletting av personopplysninger.

Det kom frem av intervjuene at det er tilfeller der ansatte sender personopplysninger på e-post. Det er etter vår vurdering et brudd på personvernregelverket. Oversendelse av personopplysninger er i seg selv en «behandling» som krever et behandlingsgrunnlag etter GDPR. 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.

Det kommer frem av intervjuene at kommunen per i dag ikke har mottatt meldinger om avvik/brudd, som de har vurdert at er av ens lik karakter at de ikke bør melde til Datatilsynet. Det er vår vurdering at kommunen melder brudd på personvernregelverket til Datatilsynet og vurderer konsekvensen for den registrerte og varsler denne når det er nødvendig.

Enhet – skole

Det fremkommer i veilederen om personvern, taushetsplikt og meldeplikt i skolen at skoleeier skal sørge for at bare de som trenger personopplysningene, har tilgang til dem. Skoleeier skal ha et bevisst forhold til hvem som får og hvem som ikke får tilgang til systemer med personopplysninger. Jo mer sensitive personopplysningene er, jo mer skal de sikres. En elev-/barnemappe kan inneholde sensitive personopplysninger, så som saker om spesialundervisning og elevenes skolemiljø. Det er vår vurdering at det å ha et fysisk arkiv som inneholder personopplysninger på samtlige elever/barn, uten ytterligere kontroll eller avgrensing av tilgang, ikke er en tilstrekkelig tilgangsstyring.

På bakgrunn av det som kommer frem i dokumentasjon, intervjuene og spørreundersøkelsen er vår vurdering at rutinene for behandling av personopplysninger om elever ikke er oppdatert i henhold til personvernregelverket for alle skolene i kommunen. Kommunen bør vurdere å etablere en felles rutine for skolene, blant annet når det gjelder ansattes tilgang til ulike personopplysninger. Dette vil også gjelde for barnehagene i kommunen.

4.7 Ansvarlighet

4.7.1 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

Det fremkommer av dokumentasjon og kontakten med kommunen, at de har et personvernombud. Personvernombudet var fra våren 2018 i en 54% stilling, men er fra mars 2019 utvidet til 100%. Personvernombudet har tatt videreutdanning i personvernregelverket.

Kommunen har offentliggjort kontaktopplysningene til personvernombudet på sine nettsider. I personvernerklæringen gir kommunen også informasjon om hva som er personvernombudets oppgaver, ombudets uavhengighet og taushetsplikt.

I spørreundersøkelsen og intervjuer fremkommer det at alle vi har spurt, kjenner til at kommunen har et personvernombud. Det kommer imidlertid frem at ikke alle ansatte ute i enhetene vet hvem som er personvernombud, eller hvordan og når de kan kontakte ombudet.

Det kommer frem av intervjuene at personvernombudet opplever å stå fritt i sitt arbeid med personvernregelverket. Personvernombudet mottar ikke instrukser om hvordan arbeidet som personvernombud skal utføres. Personvernombudet sier i intervjuet at hun opplever at hun har tilstrekkelig med ressurser nå som hun jobber fulltid med dette. Den første tiden var det fokus på å tilegne seg kompetanse på området. Etter at stillingen som personvernombud ble utvidet til en fulltidsstilling i mars 2019 har det vært lettere å få kontinuitet i arbeidet med personvernregelverket.

I intervjuet sier flere av de vi intervjuet på administrativt nivå, at det er fint at kommunen har fått et personvernombud. Det å ha noen som er kompetente på personvernlovgivningen, som en kan drøfte med oppleves som svært nyttig.

Kommunen har også etablert en GDPR-gruppe, som er ledet av personvernombudet. Gruppen ble etablert for ca. to år siden og har møter hver 14. dag. Gruppen består av representanter fra hver kommunalavdeling og skal jobbe med informasjon om personvern og GDPR i samarbeid med personvernombudet. Gruppen fungerer mest som diskusjonsforum.

Personvernombudet sier i intervjuene at hun ikke blir involvert tidlig nok i saker og at ansatte fremdeles må bli minnet på personvernregelverket, for eksempel gjennomføring av DPIA. Personvernombudet sier at ansatte ennå ikke har fått personvernregelverket inn i sine rutiner.

I dokumentasjonen fra kommunen fremkommer det at personvernombudet rapporterer til kommuneadvokaten. Kommuneadvokaten er i rådmannens stab.

Vurderinger

Kommunen har et personvernombud og har offentliggjort og meldt inn kontaktopplysningene om personvernombudet. Det er vår vurdering at kommunen under revisjonen har gjort opplysningene om personvernombudet lettere tilgjengelig for brukerne av kommunens systemer ved at de nå er å finne på førstesiden av kommunens nettsider, jf pvf artikkel 37.

Det er vår vurdering at personvernombudet har kompetanse på regelverket og er godt inneforstått med de oppgavene som er lagt til et personvernombud. Implementeringen av personvernregelverket er et omfattende arbeid i en kommune. Det er vår vurdering at med et personvernombud i 100 %

stilling, GDPR-gruppa og avdelingsledere som samarbeider om regelverket, så har personvernombudet tilstrekkelig ressurser til å utføre oppgaven.

Vi ser at personvernombudet har tilgang til personopplysninger og behandlingsaktiviteter, og det er vår vurdering at det er mulig for personvernombudet å opprettholde sin dybdekunnskap om virksomheten. Det er også vår vurdering at personvernombudet ikke mottar instrukser på hvordan arbeidet med personvern skal gjennomføres i kommen.

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». Senere under punkt 3 står det at *«Personvernombudet skal rapportere direkte til høyeste ledelsesnivå hos den behandlingsansvarlige eller databehandleren».* I en kommune er det rådmann/kommunedirektør som er det høyeste ledernivå. Det er derfor vår forståelse av artikkel 38 at personvernombudet skal rapportere direkte til rådmann/kommunedirektør og ikke til kommuneadvokaten, slik det informeres om at det er i dag. Dette for å sikre at personvernombudet ikke mottar instrukser eller på annen måte vanskeliggjør ombudets uavhengighet.

4.7.2 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 Prosedyre for behandling av personopplysninger etter GDPR pkt 6 står det at kommunen i forkant av enhver ny behandling av personopplysninger skal vurdere og dokumentere risiko. Behandlingen skal registreres i protokollen. Dersom en behandling utgjør en stor risiko for personvernet (dvs. gjelder mange registrerte eller store mengder sensitive opplysninger), må det gjennomføres en vurdering av personvernkonsekvenser (DPIA) før behandlingen iverksettes. Behandlingsansvarlig skal involvere personvernombudet i vurderingen av personvernkonsekvenser. Dersom vurderingen viser at risikoen er stor og ikke kan reduseres, må Datatilsynet kontaktes for forhåndsdrøftinger.

I definisjonen på hvem som er behandlingsansvarlig skriver kommunen i sin prosedyre «Den som bestemmer formålet med behandlingen. Rådmann er øverste behandlingsansvarlig i kommunen. Ansvaret kan delegeres til kommunalsjefene/enhetslederne for de ulike kommunalområdene.»

I dokumentasjonen oversendt fra Halden kommune foreligger det en mal for vurdering av personvernkonsekvens (DPIA) i Halden kommune. I intervjuene fremkommer det at kommunen har startet arbeidet med å vurdere personvernkonsekvens av nye behandlinger av personopplysninger.

Det kommer frem i intervjuene at personvernombudet er rådgiver i enkeltsaker om personvern. Hun får noen henvendelser med spørsmål om avvik og DPIA. Kommunen har etablert en gruppe som består av personvernombudet, beredskapsansvarlig i kommunen, en fra IT avdelingen og an fra den konkrete avdelingen som sakene gjelder. Denne gruppen jobber med vurdering av personvernkonsekvenser og ROS analyser. Gruppen trekker inn de fagområdene der de ser det er et risikoområde. De har jobbet med enhetsleder og ansatte i NAV, blant annet med en ny elektronisk

søkeportal (Digisos). Da gjennomførte de en DPIA på dette. De har oppdaget at det noen ganger er mangelfull informasjon i utkastet til databehandleravtalene, fra de som leverer programvaren.

I intervjuene fremkommer det at kommunen har planer om å ta i bruk KS-læring[3] og at risikovurderinger rundt personvernsikkerheten og DPIA er under arbeid.

Vurderinger

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.

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. Vi ser at kommunen gjør vurderinger av personvernkonsekvenser i henhold til de nevnte kriterier.

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.

Datatilsynet har utarbeidet en liste over områder der det må gjøres en vurdering av personvernkonsekvensen.

Vi ser at kommunen har igangsatt arbeidet med å gjennomføre risikovurdering av behandlingskonsekvensene og vurderinger av personvernkonsekvensene (DPIA). Med bakgrunn i at kommunen ennå ikke har en samlet oversikt over alle behandlingsaktivitetene i virksomheten, har kommunen heller ikke gjennomført en risikovurdering av alle behandlingsaktivitetene.

4.7.3 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.

Fakta

[3] KS-læring er e-læringssystemet Halden kommune benytter

I kommunens dokument Sikkerhetspolitikk for behandling av personopplysninger pkt 2.5 om egenkontroll står det «*Virksomheten skal periodisk kontrollere arbeidet med informasjonssystemet og informasjonssikkerheten. ……Gjennomføringen og oppfølgingen av egenkontrollen skal utføres av avdelingsleder.»* Det fremkommer av dokumentet hva som skal kontrolleres og når dette skal gjøres. I pkt. 2.1 om ansvar står det «*Personvernombudet vil foreta uanmeldte kontroller ute i avdelingene*».

Det opplyses i intervjuene at alle ansatte i kommunen har tilgang på både dokumentet *Sikkerhetspolitikk for behandling av personopplysninger i Halden kommune* og *Sikkerhetspolitikk for bruk av IT i Halden kommune.* Begge er å finne på Intranettet og begge dokumentene er oppdatert etter GDPR. Ikke alle ansatte, av de vi intervjuet, hadde satt seg inn i disse dokumentene.

I dokumentasjon fra kommunen står det at internkontrollen og egenkontrollen ligger i årshjulet, og at dette skal suppleres med nye personvernregler slik at det blir en naturlig del av daglig drift.

I intervjuene sier personvernombudet at de er i prosess med å utarbeide risikovurderinger og egenkontroll. Egenkontroll er en oppgave som GDPR-gruppa skal jobbe med framover. De skal jobbe med å legge inn de momentene fra GDPR som er påkrevd.

Vurderinger

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.

Kommunen planlegger å legge opp til at avdelingsleder har ansvaret for egenkontrollen og så vil personvernombudet gjennomføre stikkprøvekontroll . Det er vår vurdering at kommunens planer om å gjennomføre uanmeldte kontroller ute i avdelingene kan være en måte å sikre internkontrollen. Personvernombudet har oversikt over alle områder det meldes om brudd på personvernregelverket, oversikt over DPIA og har god kunnskap om regelverket på området, noe som gir god oversikt over risikoområdene i håndteringen av personopplysninger.

Det er vår vurdering at kommunen er klar på at de må oppdatere internkontrollsystemet i henhold til det nye personvernregelverket. Internkontroll er som regel den delen av systemet som implementeres etter at regelverkets andre bestemmelser er på plass. Implementeringen av det nye personvernregelverket i alle deler av kommunens virksomheter er et omfattende arbeid.

Det er vår vurdering at det per i dag ikke er etablert en internkontroll som gjør at kommunen kan påvise at behandlingene fullt ut utføres i samsvar med forordningen.

4.7.4 Opplæring i regelverket

Revisjonskriterier

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

Fakta

I oversendt dokumentasjon fremkommer det en oversikt over ansatte som hittil har fått opplæring i GDPR i kommunen. Oversikten viser at mange ledere (enhetsledere og avdelingsledere) har fått opplæring i GDPR per dags dato. Det er imidlertid noen ledere som ikke har deltatt på opplæring. Personvernombudet opplever at noen ledere ikke prioriterer opplæringen i en ellers hektisk hverdag. Det kommer frem av intervjuene at det ikke er lagt ut ansvar til ledernivåene om videre opplæring av saksbehandlere og ansatte i enhetene.

Av intervjuene fremkommer det at personvernombud jobber for at alle ansatte skal få opplæring i personvernlovgivingen. IT-sjefen er med i dette arbeidet. Arbeidet med opplæringen startet i GDPR-gruppen før personvernombudet ble ansatt. Rådmannens ledergruppe fikk opplæring før sommeren 2018. Deretter fikk kommunalsjefene opplæring og så enhetslederne. Alle ansatte har stående tilbud om å ta kontakt for å få opplæring, og hjelp til enkeltsaker. Det siste de har gjennomført av opplæring er et kurs med ekstern foreleser i personvernlovgivningen og offentlighetsloven. Kurset var åpent for alle ansatte, men det var få som prioriterte å delta på kurset. Personvernombudet mener at langt flere burde ha deltatt på kurset, da hun har fått mange tilbakemeldinger fra ansatte om at dette er områder de ikke kan så mye om. Fra de som har fått opplæring har det kommet mange spørsmål i etterkant. Personvernombudet sier at det har vært særlig utfordrende å få skole i gang med arbeidet på personvern. Nå har de imidlertid kommet på banen. I spørreundersøkelsen sier 23 av 26 avdelingsledere og enhetsledere at de har fått opplæring.

I intervjuene sier noen av de som har fått opplæring at de opplever større trygghet i behandlingen av personopplysninger. I intervjuet sier personvernombudet, at det er ofte de som har fått opplæring i regelverket som henvender seg med spørsmål om personvernregelverket.

Personvernombudet sier at avdelingslederne har ansvaret for at sine ansatte får opplæring. Hun har bedt dem ta kontakt med henne som personvernombud, men med lav respons. Hun sier at det kanskje hadde vært lurt å delegert denne oppgaven videre, f.eks. velge ut noen fra hver avdeling som er spesielt interessert i personvern.

<u>Enhet – skole</u>
I intervjuene kommer det frem at kommunalsjefen er bevisst på at opplæringen av ansatte er et lederansvar. Det fremkommer imidlertid av intervjuene at ansatte i skolene ennå ikke har fått opplæring i personvernregelverket. Oversikten viser at noen av de merkantile i skolene har fått opplæringen. Det kommer frem av oversikten at rektorene skal få opplæring i RLG[4]. Rektoren vi snakket med i intervjuene hadde ikke fått opplæring i personvernregelverket.

I intervjuene kommer det frem at kommunen i løpet av kort tid vil starte opp e-læring for alle ansatte i kommunen via KS-læring.

Vurderinger

Vi ser at det fremdeles er noen ledere som ikke har gjennomført opplæringen i GDPR og mange ansatte ute i enhetene har ennå ikke fått opplæring. Personvernombudet er på tilbudssiden og ansatte har stående tilbud om å ta kontakt for å få opplæring og hjelp til enkeltsaker. Det er imidlertid vår vurdering at det kan være vanskelig for en ansatt å ta imot tilbudet om opplæring, dersom lederen ikke synliggjør at de prioriterer opplæringen i personvernregelverket.

[4] Rektors ledergruppe (RLG)

Mengde og typer personopplysninger som behandles varierer mellom fagområdene. Det er allikevel vår vurdering at alle ansatte bør gjennom en slik opplæring uavhengig av fagområdet og at opplæring av ansatte bør ha prioritet i kommunens videre arbeid. Det er derfor positivt at kommunen nå setter i gang en e-læring for alle ansatte. Det er vår vurdering at opplæring i regelverket er grunnleggende for å kunne ivareta brukernes rettigheter på området. Vi mener også at opplæring i regelverket vil kunne lette arbeidet med implementeringen av kommunens prosedyrer og rutiner på området.

Det er vår vurdering at kommunen har kommet godt i gang med opplæringen innen personvernlovgivningen. Selv om vi samtidig mener at kommunen burde ha fullført den grunnleggende opplæringen av alle ansatte per i dag, ettersom ny lov om behandling av personopplysninger ble vedtatt 15. juni 2018 og trådte i kraft 20. juli 2018.

4.7.5 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.

Fakta

Kommunen har oversendt 26 databehandleravtaler som dokumentasjon. Det er blant annet databehandler avtaler med andre offentlige instanser, interesseorganisasjoner, virksomheter som leverer ulike nettverksløsninger osv. I intervjuene kommer det frem at det som regel er databehandlerne som utformer avtalen. Ansatte vi snakket med som har ansvar for databehandleravtaler sier at de går nøye gjennom avtalene før de aksepteres. De opplyser at det er flere tilfeller der de mener at avtalene er for «tynne» eller der databehandler ber om opplysninger som kommunen stiller spørsmål ved. Kommunen tar da kontakt med databehandler for avklaring og ytterligere informasjon. Det opplyses om at de gjør en egenvurdering av alle databehandleravtalene.

I intervjuene fremkommer det at det er Kommuneforlaget som er databehandler for kommunens nettside. Fagavdelingene bestiller hva de skal ha av skjemaer og så utformer Kommuneforlaget dem etter bestilling fra servicesenteret. Det er lenge siden de inngikk databehandleravtalen med Kommuneforlaget og i intervjuene sier ansatte i kommunen at det kan hende det er på tide å gjennomgå den i lys av nytt regelverk. Etter intervjuet har Halden kommune fått tilsendt en oppdatert utgave av databehandleravtalen med Kommuneforlaget, som skal signeres. Det fremkommer av intervjuene at kommunen om ikke lenge, skal ha ut anbud for en ny leverandør av publiseringsløsning for nettsider til kommunen.

I intervjuene informerer personvernombudet om at de har en oversikt over alle databehandlere de bruker i kommunen. Denne er å finne i en egen mappe i Ephorte. Personvernombudet har opplevd at avtale med nye databehandlere har vært gjort i enkelte avdelinger, uten at personvernombudet har vært involvert. Personvernombudet er tydelig på at det ikke kommer til å skje igjen. Kommunen har ikke utarbeidet rutine på dette enda, men det skal utarbeides en rutine sammen med staben i kommunen. Personvernombudet opplyser om at kommunen gjør egne vurderinger av behovet for personopplysninger i avtalene med databehandlerne. Rådmann signerer alle avtaler. I intervjuene kommer det frem at kommunen også har diskutert om de skal inngå en felles databehandleravtale knyttet til fotografering i skolen.

IT-sjefen opplyser om at enhetene ikke kan inngå avtaler om for eksempel nye læringsplattformer. IT styrer hva hver enkelt kan få tilgang til og ansatte kan ikke lenger laste ned alt de ønsker. Det må derfor avklares med IT-avdelingen dersom noen ønsker å laste ned en app. Da må avtalene gjennomgås, en DPIA gjennomføres osv. Listen over databehandlere er ennå ikke helt komplett, kommunen mangler noen databehandleravtaler, men har foreløpig konsentrert seg om de største datasystemene først. Det har vært særlig fokus på å få på plass databehandler avtaler med virksomheter som drifter noe for Halden kommune. Ved inngåelse av avtaler med databehandleren gjør IT-avdelingen en egen vurderinger av hvilke personopplysninger som skal hentes inn, det er ikke databehandlerne som avgjør dette.

Enhet - skole

Intervjuene med ansatte i skole viser at den enkelte skole inngår avtaler med for eksempel fotograf for å ta bilder av klassene/elevene. Avtalene krever personopplysninger for at foreldre eller elever skal få tilgang til bildene og evt. bestille bilder på nettet. Det er skolen selv som inngår databehandler avtale på dette området, uten at personvernombudet er involvert.

Vurderinger

På bakgrunn av det som fremkommer i intervjuene er det vår vurdering at kommunen har etablert en oversikt over databehandlere som kommunen benytter i sine tjenester og til administrasjon og drift.

Det er vår vurdering at kommunen gjør egne vurderinger av hvilke opplysninger som er adekvate, relevante og begrenset for formålet. På bakgrunn av intervjuene er det vår vurdering at kommunen nå har et mer bevisst forhold til hvem i kommunen som kan inngå databehandleravtaler, men at det fortsatt er mulig å avtale direkte, som f.eks. avtaler skolene med direkte med fotograf.

Kommunen har prioritert å få på plass avtaler med de største databehandlerne, og har per i dag ikke alle databehandler avtalene på plass.

5 KONKLUSJONER/ANBEFALINGER

Problemstilling - Har kommunen implementert personvernregelverket?

Det er vår konklusjon at kommunen informerer brukerne av kommunens tjenester om behandlingen og lagring av personopplysninger. Kommunen har imidlertid i for liten grad tilpasset informasjonen til ulike målgrupper, som barn og unge.

Kommunen har en behandlingsprotokoll og er godt i gang med å registrere og behandle de ulike kategoriene personopplysninger til de ulike formål. Det gjenstår imidlertid en del behandlinger før kommunen er i mål med dette arbeidet

Det er vår konklusjon at kommunen har utarbeidet rutiner og retningslinjer som skal ivareta personers integritet og konfidensialitet på de fleste områder. Det er iverksatt tiltak for å sikre at personopplysninger ikke uautorisert blir endret i de ulike systemene for lagring av slike opplysninger. Det er imidlertid noen områder som ikke er synliggjort i kommunens rutiner. En stor del av de ansatte i kommunen kommuniserer med brukerne av kommunens tjenester og pårørende via sms, chat, e-post osv. Kommunen bør se til at denne kommunikasjonen behandles, lagres og slettes i tråd

med personvernregleverket. Kommunen har også fysiske arkiv som ikke har tilstrekkelig avgrensing av tilgangen til personopplysninger.

Det er vår konklusjon at kommunen i for liten grad har ansvarliggjort og involvert de ulike ledernivåene i arbeidet med implementeringen av det nye personvernregelverket. Kommunen har utarbeidet flere rutiner og prosedyrer som er i tråd med den nye personvernlovgivningen. Det er imidlertid vår konklusjon at disse prosedyrene og rutinene ennå ikke er implementert i tilstrekkelig grad.

Kommunen gjør vurderinger av og har en plan for lagring og dataminimering av personopplysninger. Kommunen gjør imidlertid ikke i tilstrekkelig grad, konkrete vurdering på hvor lenge det er nødvendig og forsvarlig å beholde opplysninger, som ikke er arkivpliktige. Vurderingene gjøres på grunnlag av type sak, ikke fra sak til sak.
Kommunen har en innarbeidet praksis for å rette personopplysninger dersom det blir oppdaget feil, mangler eller den registrerte ber om det.

Det er vår konklusjon at kommunen har etablert et system for å melde avvik/brudd på personvernregelverket og at de melder avvik/brudd til Datatilsynet, samt vurderer konsekvensen for den registrerte og varsler denne når det er nødvendig.

Det er vår konklusjon at kommunen har en oversikt over databehandlerne som kommunen benytter. Kommunen sørger for å etablere databehandleravtaler og gjør en egen vurdering av innholdet i avtalene før de godkjennes. Det er per i dag ikke inngått avtaler med alle databehandlerne kommunen benytter.

Kommunen har et personvernombud som har ressurser og rammer som gjør at ombudet kan ivareta sine oppgaver. Personvernombudet rapporter imidlertid ikke til høyeste administrative nivå i kommunen, slik regelverket krever.

Kommunen har igangsatt arbeidet med å gjennomføre risikovurderinger av behandlingskonsekvensene og vurderinger av personvernskonsekvensene (DPIA). Det gjenstår imidlertid mye arbeid på dette området, da kommunen først må ha full oversikt over alle formål det hentes inn personopplysninger til, hvilke personopplysninger dette er, hvordan de lagres osv.

Med bakgrunn i vurderingene i denne revisjonen, er det vår konklusjon at kommunen ikke har en internkontroll som er oppdatert eller implementert på personvernområdet.

Det er vår vurdering at kommunen kom noe sent i gang med å gi opplæring og implementere det nye personvernregelverket. Kommunen har imidlertid i 2019 intensivert arbeidet og jobber nå samtidig på flere områder for å få implementert personvernregelverket. Det jobbes parallelt med å hente inn opplysninger i organisasjonen for å få ferdig en behandlingsprotokoll, utarbeide oversikter over databehandlere og etablere databehandleravtaler, gi opplæring i personvernregelverket, DPIA og implementere et oppdatert internkontrollsystem osv. Det er vår konklusjon at kommunen prioriterer dette arbeidet og tar ansvar på området.

Samlet sett er det revisjonens konklusjon at Halden kommune ikke fullt ut har implementert alle krav og forventninger i personvernregelverket. Kommunen har gitt opplæring til mange av kommunens ledere, men har i liten grad sikret at opplæringen blir videreført ut i enhetene.

Revisjonen anbefaler at kommunen bør:

- sørge for å informere om hvordan de behandler personopplysningene på en måte som gjør informasjonen forståelig for alle målgrupper, som for eksempel for barn og unge.
- behandle de ulike typene kommunikasjonskanaler som ansatte benytter som sms, chat, e-post osv, vurdere lagring og sletting av personopplysninger og personvernkonsekvens
- ha en gjennomgang av hvilke kategoriene personopplysninger som det må innhentes samtykke til på de ulike fagområdene.
- etablere felles rutiner for enhet- skole, når det gjelder tilgangsavgrensing til fysiske arkiv.
- sikre at personopplysninger ikke lagres lenger enn det som er nødvendig og forsvarlig for den enkelte sak.
- se til at det gjøres en vurdering av om opplysninger eller deler av opplysninger skal slettes eller pseudonymiseres ved lagring av ikke arkivverdige personopplysninger, og vurdere om formålet for lagring av opplysningene er et annet enn ved registreringen
- videreføre arbeidet med databehandleravtaler, slik at kommunen har avtale med alle databehandlere
- se til at personvernombudet rapporterer til høyeste ledelsesnivå i kommunen
- gjennomføre en behandling av sine webkameraer og informere kommunens innbyggere om hensikten med og bruken av disse
- videreføre arbeidet med behandlingene, slik at alle behandlinger er registrert i protokollen og at det er vurdert om det er høy risiko for personvernkonsekvens
- videreføre arbeidet med å vurdere personvernkonsekvens (DPIA) der risikoen er høy
- etablere og implementere interkontroll på personvernområdet
- sørge for at opplæring blir prioritert nedover i organisasjonen

Rolvsøy, 18.11.2019

Unn Elisabeth West
prosjektleder

Karianne Åsheim
forvaltningsrevisor

Lene Brudal
oppdragsansvarlig revisor

6 KOMMUNEDIREKTØRENS UTTALELSE

Halden kommune er positive til tilsyn, da det gir oss føringer for å få enda bedre kvalitet på området personvern. Det er vår oppfatning at Halden kommune kom tidlig og godt i gang med arbeidet på dette området, da det ble nedsatt en arbeidsgruppe i 2017. Arbeidsgruppa ble videreført da personvernombudet ble tilsatt våren 2018, og gruppa består fortsatt. Arbeidet er godt i gang. Det er noe variasjon i hvor langt de ulike avdelingene/den enkelte medarbeider har kommet med implementeringen av lovverket.
Kommunalavdeling Helse og omsorg har over lang tid hatt en god praksis innenfor området. Hva gjelder de øvrige kommunalområdene, er det noe mer variasjon i forhold til erfaring med, og praktisering av lovverket. Kommunedirektøren er kjent med denne variasjonen.
Når det gjelder intervjuene som ble foretatt under revisjonsarbeidet, er kommunedirektøren kjent med at det ble foretatt betydelige rettinger under kvalitetssikringen av referatene. Kommunedirektøren legger til grunn at alle intervjuobjekter gjennomførte kvalitetssjekk og eventuelt var i dialog med revisjonen i forhold til dette.

Nedenfor knyttes noen kommentarer til revisjonens anbefalinger.
Kommunen bør:

- **sørge for å informere om hvordan de behandler personopplysningene på en måte som gjør informasjonen forståelig for alle målgrupper, som for eksempel for barn og unge.**

I tillegg til Personvernerklæringen som ligger på intranettet og Halden Kommunes hjemmeside, skal det utarbeides en erklæring som er tilpasset barn/unge.

- **behandle de ulike typene kommunikasjonskanaler som ansatte benytter som sms, chat, e-post osv, vurdere lagring og sletting av personopplysninger og personvernkonsekvens.**

Halden kommune tilstreber i størst mulig grad å kommunisere via de rette kanaler, dvs arkivsystemet og ulike fagprogram. Dette blir det lagt vekt på i opplæringen i personvernlovverket.
Kommunen er kjent med at det også brukes andre ulike kommunikasjonskanaler som sms, mail, messenger (chat), i organisasjonen. Det vil bli utarbeidet retningslinjer for bruken av disse, samt utføres personvernkonsekvensvurdering (DPIA). Nytt arkivsystem, «Elements», er planlagt og tas i bruk i løpet av våren 2020. Her er det mulig å overføre sms til arkivet.

- **ha en gjennomgang av hvilke kategorier personopplysninger som må innhentes samtykke til på de ulike fagområdene.**

Rutiner for når man kan benytte samtykke som rettsgrunnlag, vil bli lagt ut på intranettet.

- **etablere felles rutiner for enhet – skole, når det gjelder tilgangsavgrensning til fysisk arkiv.**

Kommunen har stort fokus på skolenes papirarkiv. Dette skal digitaliseres ved at det tas i bruk en modul for arkiv og kommunikasjon mellom skole og PPT.

- **sikre at personopplysninger ikke lagres lenger enn det som er nødvendig og forsvarlig for den enkelte sak.**

Halden kommune tar dette til etterretning og oppfølging.

- **se til at det gjøres en vurdering av om opplysninger eller deler av opplysninger skal slettes eller pseudonymiseres ved lagring av ikke arkivverdige personopplysninger, og vurdere om formålet for lagring av opplysningene er et annet enn ved registreringen.**

Det skal utarbeides rutine for sletting/pseudonymisering ved lagring av ikke arkivverdige personopplysninger. Denne legges inn i Sikkerhetspolitikken under internkontroll.

- **videreføre arbeidet med databehandleravtaler, slik at kommunen har avtale med alle databehandlere.**

Kommunen har kontinuerlig fokus på databehandleravtaler.

- **Se til at personvernombudet rapporterer til høyeste ledelsesnivå i kommunen.**

Personvernombudets rolle er bl.a å gi råd og veiledning om hvilke forpliktelser virksomheten har etter personvernlovgivningen, og kontrollere overholdelse og etterlevelse av lovverket, (personvernforordningen artikkel 39). Virksomheten (kommunen) skal legge til rette for ombudets uavhengighet for å unngå interessekonflikter og sørge for at ombudet ikke mottar instrukser (personvernforordningen artikkel 38.3) Dette er også vektlagt på Datatilsynets sider.
Det ble i forkant av ansettelse av personvernombud vurdert hvor i organisasjonen ombudet skulle sortere, nettopp for å ivareta dette. Beslutningen falt på Kommuneadvokaten, som også har en uavhengig rolle i kommunen.

- **Gjennomføre en behandling av sine webkameraer og informere kommunens innbyggere om hensikten med og bruken av disse.**

Halden kommune tar dette til etterretning og oppfølging.

- **videreføre arbeidet med behandlingene, slik at alle behandlinger er registrert i protokollen og at det er vurdert om det er høy risiko for personvernkonsekvens.**

Kommunen har fra våren 2019 intensivert arbeidet med å sluttføre behandlingsprotokollen, og å gjennomføre personvernkonsekvensvurdering (DPIA) og risikovurderinger der det er behov for det.

- **etablere og implementere internkontroll på personvernområdet.**

Halden kommune har internkontroll som vil bli utvidet i henhold til kravene i personvernlovverket. Dette ligger i Kommunedirektørens årshjul.

- **sørge for at opplæring blir prioritert nedover i organisasjonen**

Det jobbes parallelt med mange temaer innenfor personvern. Et stort hovedfokus fremover vil være å sørge for at alle ansatte får opplæring. Dette skal hver enkelt ansatt få gjennom elektronisk opplæringsprogram i KS-læring. I tillegg vil personvernombudet være en rådgiver og tilby kurs fortløpende.

7 VEDLEGG

1. Utledning av revisjonskriterier
2. Litteratur- og dokumentliste
3. Definisjoner og begreper
4. Spørsmål i Questback

Vedlegg 1 - Utledning av revisjonskriterier

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

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……..»

Til punkt 5. 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.»* Kommunen har utarbeidet en *Prosedyre for behandling av personopplysninger etter GDPR.* I punkt 6. i denne prosedyren fremkommer det at «*Kommunens personvernerklæring skal være lett tilgjengelig og skrevet på en forståelig måte. All informasjon om hvordan kommunen behandler personopplysninger skal være tilpasset målgruppa, for eksempel barn på ulike alderstrinn*».

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

Kommunen

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

Som grunnlag for implementering av forordningen må kommunen ha vurdert:

1. **Har kommunen vurdert hvilke personopplysninger de har behov for? (art 5, 6, 8, 12, 24, 25**
   Kommunen skal
   - ha en oversikt over de ulike kategoriene personopplysninger som er registrert til ulike formål, jf pvf art. 6.
   - gjøre en vurdering av om de innsamlede opplysningen i hvert tilfelle er adekvate, relevante og begrenset for formålet (dataminimering) jf. pvf art. 5 c)
   - vurdere om personopplysningene er nødvendig for å utøve lovpålagte oppgaver – utøve offentlig myndighet jf. pvf art. 6 e)
   - sikre at personopplysningene er korrekte og om nødvendig oppdatere jf. pvf art. 5 d)
   - gjennomføre egnede tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering jf. pvf art. 25
   - informere den registrerte om kategoriene, formålet, lagringen, viderebehandlingen og –formidlingen av personopplysninger, samt rettigheter, kontaktinformasjon og evt andre forhold, jf pvf art. 12-14
     - ved innsamling av personopplysninger fra den registrerte
     - ved innhenting av personopplysninger fra andre kilder
     Informasjonen skal gis skriftlig eller på annen måte, herunder elektronisk.

2. **Har kommunen vurdert hvorfor de har behov for disse opplysningene?**
   Kommunen skal
   - sikre at personopplysningene kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål og at de ikke viderebehandles utover formålet jf. pvf art. 5 b)
   - ha vurdert til hvilket formål og for hvilke kategorier personopplysninger det er behov for samtykke jf pvf art 8 og 9, og popplyl § 5
   - ha kunnskap om personopplysninger benyttes til andre formål enn det de er samlet inn til, jf pvf art. 5 b) – og hvilke formål det er og om formålet er forenelig med det formålet som personopplysningene opprinnelig ble samlet inn for jf. art 6 pkt 4. a)
   - vurdere når det er behov for behandling av særlige kategorier personopplysninger jf. art 6 og popplyl § 6.
3. **Har kommunen vurdert hvor lenge de har behov for opplysningene**
   Kommunen skal
   - sikre 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. jf. pvf art. 5 e)
   - slette personopplysninger uten ugrunnet opphold dersom personopplysningene ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for, jf pvf art. 17 pkt 1 a)
   - gjennomføre egnede tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering jf. pvf art. 25

4. **Har kommunen vurdert hvordan opplysningene er lagret?**
   Kommunen skal

- sikre at personopplysningene behandles på en måte som gir tilstrekkelig sikkerhet for personopplysningene jf. art 5 f) og art 25
- iverksette 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, jf. pvf art. 25

5. **Har kommunen vurdert hvem som skal ha tilgang til opplysningene?**
   Kommunen skal
   - sikre at personopplysningene behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, jf. pvf art. 5 f)
   - 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, jf. pvf art. 28
   - sikre at eventuelle databehandlere kun behandler personopplysninger etter instruks fra kommunen. Avtale eller annet dokument skal angi innholdet i avtalen med databehandler. Avtalen eller dokumentet skal være skriftlig, jf. pvf art. 28 og 29
   - gjøre en vurdering av hvilke ansatte som skal ha autorisert tilgang til hvilke personopplysninger. Personopplysningene skal være kryptert for ansatte som ikke har autorisert tilgang, jf. pvf art 32.

Har kommunen opprettet et personvernombud?

Kommunen skal
- ha et personvernombud, jf. pvf art. 37
- offentliggjøre kontaktopplysningene til personvernombudet og melde disse til Datatilsynet, jf. pvf art. 37
- på riktig måte og rett tid involvere personvernombudet i alle spørsmål som gjelder vern av personopplysninger, jf. pvf art. 38
- sikre at personvernombudet ikke mottar instruks om utførelsen av oppgavene til personvernombudet, jf. pvf art. 38

Personvernombudet skal
- ha dybdekunnskap om personvernlovgivningen og praksis på området jf. pvf art. 37 pkt. 5
- rapportere direkte til høyeste ledelsesnivå i kommunen, jf. pvf art. 38
- minst ha de oppgaver som fremkommer av pvf. art. 39

Har kommune gjennomført risikovurderinger knyttet til behandlingen av personopplysninger?

Kommunen skal
- ha kunnskap om personopplysninger behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte jf. pvf art. 5 a)
- gjennomføre en vurdering av personvernkonsekvensene (DPIA) i henhold til Datatilsynets liste, jf. pvf art 35 pkt 4. https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/
- iverksette egnede tekniske og organisatoriske tiltak for å oppnå egnet sikkerhetsnivå, jf. pvf art. 32
- sikre at brudd på personopplysningssikkerheten meldes i henhold til pvf art. 33 og 34

Har kommunen sikret at ansatte etterlever regelverket?

Kommunen skal
- iverksette egnede retningslinjer for vern av personopplysninger, jf pvf art. 24 pkt 2
- føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar.
  Protokoll skal inneholde:
  i. navnet på og kontaktopplysningene til den behandlingsansvarlige og personvernombudet
  ii. formålene med behandlingen,

iii. en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger,
iv. kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til
v. dersom det er mulig, planlagte tidsfrister for sletting av de forskjellige kategoriene av opplysninger,
vi. evt generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1……

Protokollene skal være skriftlige, herunder elektroniske. Jf. pvf art. 30

1. **Har kommunen gitt ansatte tilstrekkelig opplæring i regelverket på området? (spørreundersøkelse og intervjuer)**
(For alle virksomheter og underliggende enheter i kommunen?)

Har ansatte fått opplæring i
- behandling av personopplysninger
- vilkår for samtykke til behandling av personopplysninger?
- behandling av avviksmeldinger?
- gjennomføring av risikovurdering?
- ivaretakelse av registrertes rettigheter?
- personvernombudet, kontaktinformasjon og ombudets oppgaver og rolle i kommunen?

Utvalgt virksomhet – skole

Har skolen implementert personvernregelverket?

1) **Har skolen vurdert hvilke personopplysninger de har behov for?**
Skolen skal
- ha oversikt over hvilke kategorier personopplysninger som er registrert til hvilke formål, jf. pvf art. 6
- vurdere om personopplysningene er nødvendige for å utføre lovpålagte oppgaver – utøve offentlig myndighet, jf. pvf art 6 e)
- gjøre en vurdering av om de innsamlede opplysningen i hvert tilfelle er adekvate, relevante og begrenset for formålet (dataminimering) jf. pvf art. 5 c)
- informere den registrerte om kategoriene, formålet, lagringen, viderebehandlingen og –formidlingen av personopplysninger, samt rettigheter, kontaktinformasjon og evt andre forhold, jf pvf art. 12-14.
    - ved innsamling av personopplysninger fra den registrerte
    - ved innhenting av personopplysninger fra andre kilder

  Informasjonen skal gis skriftlig eller på annen måte, herunder elektronisk.
- sikre at personopplysningene er korrekte og om nødvendig oppdatere jf. pvf art. 5 d)
- gjennomføre egnede tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering jf. pvf art. 25

2) **Har skolen vurdert hvorfor de har behov for disse opplysningene?**
Skolen skal
- sikre at personopplysningene kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål og at de ikke viderebehandles utover formålet jf. pvf art. 5 b)
- ha vurdert til hvilket formål og for hvilke kategorier personopplysninger det er behov for samtykke til, jf. pvf art 8 og 9, og popplyl § 5
- ha kunnskap om personopplysninger benyttes til andre formål enn det de er samlet inn til, jf. pvf art. 5 b) – og hvilke formål det er og om formålet er forenelig med det formålet som personopplysningene opprinnelig ble samlet inn for jf. art 6 pkt 4. a)
- vurdere når det er behov for behandling av særlige kategorier personopplysninger jf. art 6 og popplyl § 6.

3) **Har skolen vurdert hvor lenge de har behov for opplysningene**

Skolen skal

- sikre 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. jf. pvf art. 5 e)
- slette personopplysninger uten ugrunnet opphold dersom personopplysningene ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for, jf pvf art. 17 pkt 1 a)
- gjennomføre egnede tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering jf. pvf art. 25

6. **Har skolen vurdert hvordan opplysningene er lagret?**

Skolen skal

- sikre at personopplysningene behandles på en måte som gir tilstrekkelig sikkerhet for personopplysningene jf. art 5 f) og art 25
- iverksette 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, jf. pvf art. 25

7. **Har skolen vurdert hvem som skal ha tilgang til opplysningene?**

Skolen skal

- sikre at personopplysningene behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene jf. pvf art. 5 f)
- gjøre en vurdering av hvilke ansatte som skal ha autorisert tilgang til hvilke personopplysninger. Personopplysningene skal være kryptert for ansatte som ikke har autorisert tilgang, jf. pvf art 32.
- sikre at brudd på personopplysningssikkerheten meldes i henhold til pvf art. 33 og 34

Vedlegg 2 - Litteratur- og dokumentliste

Følgende dokumenter ligger til grunn for faktafremstillingen:
Dokumenter oversendt fra Halden kommune 04.09.2019:

- Organisasjonsplan/-kart Halden kommune
- Oversikt over ansatte i avdeling Kommunikasjon og service med oppgaver
- Oversikt over rutiner og arkiveringsstruktur i Ephorte
- Bevarings- og kassasjonsplan for Halden kommune
- Oversikt over ansatte i avdeling post/arkiv med oppgaver
- Oversikt over arbeidsgruppe GDPR
- Økonomiplan 2018-2021
- Databehandleravtaler i Halden kommune – 26 avtaler
- Oversikt over opplæring i GDPR – enhetsledere og avdelingsledere per 3.09.2019
- Oversikt over personvernombudets oppgaver
- Prosedyre for håndtering av alvorlige sikkerhetsbrudd - GDPR
- Brev med dokumentasjon fra Ljåby skole
    a. oversikt over ansatte med lederfunksjoner
    b. Oversikt over merkantilt ansatte
    c. Oversikt over digital plattformer som skolen bruker
    d. Informasjon om/beskrivelse av rutiner
        i. Personopplysninger
        ii. Fotografering
        iii. Utlevering og/eller digital utsending av elevlister og elevopplysninger
        iv. Arkivering og lagring av personopplysninger
- GDPR – Behandlinger - ansettelser
- GDPR behandling – Kameraovervåking – Wiels plass
- Oversikt over kommunens kameraovervåking og behandling
- Sikkerhetspolitikk for behandling av personopplysninger
    a. Årshjul – personal og organisasjon 2018
- Prosedyre for svar på forespørsel om innsyn i egne personopplysninger (GDPR)
- Prosedyre for behandling av personopplysninger etter GDPR
- Skjema for vurdering av personvernkonsekvens (DPIA) – Halden kommune
- Etiske retningslinjer for Halden kommune – veileder til etikkplakaten
- Etikkplakaten
- Sikkerhetspolitikk for bruk av IT i Halden kommune
- Oversikt over etterspurt dokumentasjon og oversendt dokumentasjon (vedlegg) med kommentarer

- Bruker- og taushetserklæring i Halden kommune, mottatt 04.10.2019
- Rutine – Låby skole Dokumenter som skal inn i Ephorte, mottatt 08.10.2019
- Rutinehefte skolestart, august 2019 – Låby skole, mottatt 08.10.2019

Dokumenter fra kommunens hjemmeside:

- Personvernerklæring Halden kommune
- Innsynsbegjæring
- «Personvern og cookies» fra hjemmesiden til Låby skole
- Personvernerklæring knyttet til digitale søknader, skrevet ut 30.09.2019
- Rettet personvernerklæring knyttet til digitale søknader, skrevet ut 04.10.2019

Systemgjennomsyn:

- Risk Manager

- Meldinger om brudd på personvernregelverket per 08.10.2019
- Protokoll over behandlingsaktiviteter i Halden kommune per 08.10.2019

Vedlegg 3 – 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 4 - Spørsmål i Questback

Personvern - Halden

1) * I hvilken enhet i Halden kommune er du ansatt?

- Rådmannens stab
- Rådmannens støttefunksjoner
- Teknisk
- Undervisning, oppvekst og kultur
- Helse og omsorg
- NAV

2) * Hvilken funksjon har du?

- Kommunalsjef
- Enhetsleder
- Rektor, styrer
- Lærere/pedagoger, avdelingsleder skole e.l

Actions vil skje for følgende alternativer:

- Nei (undersøkelsen avsluttes) : Vis avslutningsmeldingen

3) * Behandler dere personopplysninger i din enhet?

- Ja
- Nei (undersøkelsen avsluttes)
- Vet ikke

4) * Har dere vurdert hvilke personopplysninger dere har behov for i din enhet ?

- Ja
- Nei

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

- Ja

- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

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

6) * Hva tenker du er det rettslige grunnlaget for databehandling i din enhet?

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
- Rektor, styrer
- Enhetsleder
- Kommunalsjef

7) * Informerer dere brukerne i din enhet om at personopplysninger blir lagret?

- Ja
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
- Lærere/pedagoger, avdelingsleder skole e.l

8) * Informerer dere foreldre og elever om hvordan dere lagrer og bruker personopplysninger?

- Ja - elevene
- Ja - foreldrene
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Informerer dere brukerne i din enhet om at personopplysninger blir lagret? inneholder noen av disse alternativene
- Ja
- eller
- Dersom spørsmålet Informerer dere foreldre og elever om hvordan dere lagrer og bruker personopplysninger? inneholder noen av disse alternativene
- Ja - foreldrene
- Ja - elevene

9) * Hva informerer dere om?

- [ ] Hvilke personopplysninger
- [ ] Hva som blir lagret
- [ ] Hva formålet er
- [ ] Personers rettigheter om personvernlovgivningen
- [ ] Annet

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
- Lærere/pedagoger, avdelingsleder skole e.l
- Rektor, styrer

10) * Kontrollerer/loggfører skolen elevenes internettbruk?

- ( ) Ja
- ( ) Nei
- ( ) Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Kontrollerer/loggfører skolen elevenes internettbruk? inneholder noen av disse alternativene
- Ja

11) * Hvem har tilgang til å se loggføringen?

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Kontrollerer/loggfører skolen elevenes internettbruk? inneholder noen av disse alternativene
- Ja

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

- ☐ Ja - foreldrene
- ☐ Ja - elevene
- ☐ Nei
- ☐ Vet ikke

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

- ○ Ja
- ○ Nei
- ○ Vet ikke

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

- ○ Ja
- ○ Nei
- ○ Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- ○ Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
- Rektor, styrer
- Enhetsleder
- Kommunalsjef
- ○ eller
- ○ Dersom spørsmålet Har dere en oversikt over hvilke type formål dere henter personopplysninger til? inneholder noen av disse alternativene
- Ja

15) * Har dere vurdert hvem som skal ha tilgang til personopplysninger?

- ○ Ja
- ○ Nei
- ○ Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- ○ Dersom spørsmålet Har dere vurdert hvem som skal ha tilgang til personopplysninger? inneholder noen av disse alternativene
- Ja

16) * Hvilke vurderinger har dere gjort?

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
  - Lærere/pedagoger, avdelingsleder skole e.l
  - Rektor, styrer

17) * Har lærerne/ansatte tilgang til alle elevmappene/opplysninger om det enkelte barn?

- Ja
- Kun de elevene/barna jeg har fagansvar for
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
  - Lærere/pedagoger, avdelingsleder skole e.l
  - Rektor, styrer

18) * Bruker skolen/barnehagen digitale kartleggingssystem til skolemiljø/barnehagemljø?

- Ja
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Bruker skolen/barnehagen digitale kartleggingssystem til skolemiljø/barnehagemljø? inneholder noen av disse alternativene
  - Ja

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

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Bruker skolen/barnehagen digitale kartleggingssystem til skolemiljø/barnehagemljø? inneholder noen av disse alternativene
  - Ja

20) * På hvilket grunnlag gjør dere vurderinger av hvem som skal ha tilgang til de ulike personopplysningene i skolemiljøsaker?

21) * Vet dere om personopplysningene ikke benyttes til andre formål enn de er samlet inn for?

- Ja
- Nei

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

- Ja
- Nei

23) * Har dere oppgaver som medfører behov for særskilte kategorier personopplysninger (f.eks. informasjon om etnisk opprinnelse, helseinformasjon politisk oppfatning etc.)

- Ja
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Har dere oppgaver som medfører behov for særskilte kategorier personopplysninger (f.eks. informasjon om etnisk opprinnelse, helseinformasjon politisk oppfatning etc.) inneholder noen av disse alternativene
  - Ja

24) * Hvordan er de særskilte kategoriene personopplysningene sikret?

25) * Informerer dere om retten til innsyn, retting og sletting av personopplysninger?

- Ja
- Nei
- Vet ikke

26) * Har noen bedt om innsyn, retting eller sletting av sine personopplysninger i din enhet siste år?

- Ja
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Har noen bedt om innsyn, retting eller sletting av sine personopplysninger i din enhet siste år? inneholder noen av disse alternativene
  - Ja

27) Hvordan har dere behandlet disse kravene?

28) * Hvilke kanaler brukes på ditt fagområde til å kommunisere med brukere og evt. pårørende?

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

29) * Hvordan sørger dere for lagring og sletting av personopplysninger fra disse kanalene?

30) * Har dere vurdert hvor lenge dere har behov for personopplysningene dere har hentet inn?

- Ja
- Nei
- Vet ikke

31) * Finnes det kameraovervåking i din enhet?

- Ja
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
- Rektor, styrer
- Enhetsleder
- Kommunalsjef

32) * Har dere rutiner for å føre protokoll over behandlingsaktivitetene på ditt fagområde?

- Ja
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
- Rektor, styrer
- Enhetsleder
- Kommunalsjef

33) * Har dere utarbeidet en oversikt over databehandlere på ditt fagområde?

- Ja
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Har dere utarbeidet en oversikt over databehandlere på ditt fagområde? inneholder noen av disse alternativene
- Ja

34) * Har dere skriftlige avtaler med alle databehandlerne?

- Ja
- Nei
- Vet ikke

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Har dere utarbeidet en oversikt over databehandlere på ditt fagområde? inneholder noen av disse alternativene
- Ja

35) * Hvem har oversikt over alle databehandlerne på ditt fagområde?

36) * Vet du hvem som er personvernombud i Halden kommune?

- Ja
- Nei

37) * Kjenner du til personvernombudets oppgaver?

- Ja
- Nei

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

- Ja
- Nei
- Vet ikke

39) * Kjenner du til områder der personvernombudet burde vært involvert?

- Ja
- Nei

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Kjenner du til områder der personvernombudet burde vært involvert? inneholder noen av disse alternativene
- Ja

40) * I såfall hvilke?

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Hvilken funksjon har du? inneholder noen av disse alternativene
- Rektor, styrer
- Enhetsleder
- Kommunalsjef

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

- Ja

- Nei
- Vet ikke

42) * Vet du hvordan du går fram for å melde brudd på personvernlovgivningen?

- Ja
- Nei

43) * Har du opplevd brudd på personvernlovgivningen det siste året?

- Ja
- Nei

Følgende betingelser må være oppfylt for at spørsmålet skal vises for respondenten:

- Dersom spørsmålet Har du opplevd brudd på personvernlovgivningen det siste året? inneholder noen av disse alternativene
- Ja

44) * Hvordan gikk du fram da?

45) * Har du fått opplæring i personvernregelverket i Halden kommune?

- Ja
- Nei
- Vet ikke

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

Vedlegg 5 - Prosjektplan