ØVKR
Østre Viken kommunerevisjon IKS

OPPFØLGINGSRAPPORT
HALDEN KOMMUNE
01.06.2021

Personvern

Oppfølging av forvaltningsrevisjon for Halden kommune

1 Innhold

2 Innledning

EUs personvernsforordning ble implementert i norsk lov i 2018. Hensikten med denne forordningen er å beskytte personopplysninger, og å gjøre det mulig å oppbevare dataen innenfor samme regler innad i EU og EØS. Forordningen har kommet inn i norsk rett gjennom personopplysningsloven og opphevet loven fra år 2000. Denne loven gir personer rett til innsyn i hvordan ens egne personopplysninger blir behandlet. Informasjonen skal være lettfattelig, informere om typen personopplysninger som blir behandlet, formålet, hvor lenge den skal lagres og hvem som har tilgang til den. I tillegg gir loven nå også hjemmel for å be om at personopplysninger om en selv skal bli slettet[1].

Det var basert på dette nye lovverket at revisjonen gjennomførte forvaltningsrevisjonsprosjektet «Personvern» i Halden kommune i 2020. Rapporten fra revisjonen ble behandlet i kontrollutvalget i sak 19/44 den 26.11.19, og i kommunestyret i sak PS 2020/11 den 16.01.20. Kommunestyret vedtok i saken at vedtaket skulle følges opp med en oppfølgingsrapport levert av revisjonen.

Videre fremkommer det av forskrift om kontrollutvalg og revisjon § 5 at kontrollutvalget skal påse at kommunestyrets vedtak om forvaltningsrevisjoner blir fulgt opp. Kontrollutvalget skal og rapportere til kommunestyret og oppfølgingsrapporten skal behandles av kontrollutvalget og kommunestyret.

Revisjonen ønsker å takke kommuneadministrasjonen for et godt samarbeid i forbindelse med gjennomføringen av oppfølgingsundersøkelsen.

[1] Gisle, J. (2018, 11 30). Store norske leksikon. Hentet fra snl.no.: https://snl.no/Personvernforordningen

3 Gjennomføring av undersøkelsen

3.1 Kommunestyrets vedtak

Formålet med oppfølgingsundersøkelsen er å kontrollere om kommunestyrets vedtak i forbindelse med behandlingen av forvaltningsrevisjonsrapporten er fulgt opp.

Kommunestyret i Halden kommune fattet følgende vedtak i sak PS 2020/11:

1. Kommunestyret tar forvaltningsrevisjonsrapport «Personvern» til orientering, og ber administrasjonen følge opp de 13 anbefalinger som fremkommer av rapporten. Herunder skal kommunen:

- 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

2. Kommunestyret viser til kontrollutvalgets ansvar for å påse at kommunestyrets vedtak i forbindelse med forvaltningsrevisjon blir fulgt opp. Kommunestyret ber kontrollutvalget om å følge opp vedtaket med en oppfølgingsrapport fra revisjonen ett år etter kommunestyrets behandling av saken. Denne oppfølgingsrapporten skal også sendes til kommunestyret.

3.2 Metode og datagrunnlag

Kommunestyret vedtok at administrasjonen skulle følge opp anbefalingene fra forvaltningsrevisjonsrapporten «Personvern». I denne oppfølgingsrapporten vurderer revisjonen kommunens oppfølging av vedtaket.

Revisjonen ba i e-post til kommunedirektøren datert 15.01.2021 om en redegjørelse for hvilke tiltak som er iverksatt som følge av vedtaket. Revisjonen ba også om at eventuelle iverksatte tiltak dokumenteres, for eksempel ved at utarbeidede rutiner, kartlegginger, referater eller lignende dokumentasjon ble lagt ved redegjørelsen.

Kommunen har ved personvernombud Hilde Furuseth redegjort for fremdrift på kommunens oppfølging av de vedtaket. E-posten til revisjonen er datert 12.02.21.

Revisjonen sendte 2 e-poster med oppfølgingsspørsmål. Disse er datert den 26.03.21 og 16.04.21. Her fikk revisjonen oversendt ytterligere dokumenter og redegjørelse fra kommunen. Kommunen sendte over ytterligere informasjon den 09.04.21 og 16.04.21.

På generelt grunnlag informerte kommunen om at alle dokumenter som er oversendt fra kommunen er publisert internt, enten i Risk Manager[2] eller i SharePoint[3].

Revisjonen har gjennomført vurderingene i denne rapporten på bakgrunn av administrasjonens redegjørelse og oversendte dokumenter.

Kommunedirektørens uttalelse til oppfølgingsrapporten fremkommer av kapittel 6.4.

[2] Risk Manger er et kvalitetssystem for å identifisere, evaluere og holde oversikt over områder med høy risiko og rutiner.

[3] SharePoint er en nettbasert samarbeidsplattform for dokumenthåndtering og lagring.

Revisjonens undersøkelser

Denne oppfølgingsrapporten har blitt satt opp tematisk for å gjøre det lettere for leseren å få et overblikk over hvordan Halden kommune har fulgt opp kommunestyrets vedtak. Dette kapittelet består av to deler. Den første delen presenterer og vurderer oppfølgingen av kulepunktene 11, 12, 2, 6, 7, 3, 10, 1, 4 og 8 i vedtaket. Disse kulepunktene er knyttet til informasjonsinnhenting, lagring og sletting av personopplysninger. Den andre delen omhandler kulepunktene 9, 13, 14 og 5. Disse kulepunktene er knyttet til rapportering, internkontroll, videre opplæring i organisasjonen og skole. For mer informasjon om bakgrunnen for vedtaket/anbefalingene, henvises det til forvaltningsrevisjonsrapporten, samt konklusjonen fra rapporten i vedlegg 6.3.

Innhenting, lagring og sletting av informasjon

3.3 Kulepunkt 11 og 12

11: Videreføre arbeidet med behandlingene, slik at alle behandlinger er registrert i protokollen og at det er vurdert om det er høy risiko for personvernkonsekvens.
12. Videreføre arbeidet med å vurdere personvernkonsekvens (DPIA) der risikoen er høy

3.3.1 Administrasjonens redegjørelse for kulepunkt 11 og 12

Kommunen opplyser at de har utarbeidet en behandlingsprotokoll og rutiner for hvordan kommunen skal behandle de ulike kommunikasjonssystemene de bruker. Dette har de lagt på Risk Manger eller SharePoint, og her blir behandlinger oppdatert løpende ifølge kommunen.

Videre har kommunen nylig gått til anskaffelse av programmet «DigiOrden» og har lagt inn alle sine applikasjoner. Kommunen opplyser om at de arbeider med å oppdatere dette systemet slik at det oppfyller personvernsforordningens krav om dokumentasjon.

Kommunen har oversendt dokumentasjon på prosedyrer for behandling av personopplysninger og andre relevante interne dokumenter. Kommunen opplyser at de gjennomfører en vurdering av personvernkonsekvens, der risikoen er høy ved nye behandlinger. Dette er noe kommunen jobber med kontinuerlig og de har sendt over en mal for hvordan dette gjennomføres, og et eksempel på en gjennomført DPIA. Kommunen har også oversendt en oversikt over gjennomførte og ikke gjennomførte vurderinger av om det er behov for å gjennomføre DPIA-er. I tillegg arbeider kommunen med å formalisere en rutine der det blir innarbeidet at det er et lederansvar å vurdere om det er behov for en DPIA.

3.3.2 Revisjonens vurderinger

Denne vurderingen baserer seg på oversendte dokumenter og kommunens redegjørelse. Revisor har ikke gått inn i på Risk Manager, intranettet i kommunen, SharePoint eller sett på programmene DigiOrden eller Nano-Learning. Revisjonen har heller ikke gjennomgått behandlingsprotokollene, eller kontrollert gjennomføringen av DPIAene som er oversendt.

Revisjonen har sett dokumentasjon på behandlingsprotokoll for personopplysninger. Denne dokumentasjonen inneholder både behandlinger kommunen har vurdert og behandlinger der kommunen skal vurdere om det skal gjennomføres en vurdering av personvernskonsekvens. Her kan revisjonen se at det

fortsatt er noen områder der det ikke er vurdert om det er behov med en personvernskonsekvensutredning/DPIA, men at kommunen har vurdert majoriteten av de behandlingen de gjennomfører opp mot det nye regelverket.

Revisjonen har sett kommunens mal for å gjennomføre DPIA-er og et eksempel på gjennomført DPIA på Hospital IT. Her kan revisjonen se at kommunen arbeider med å sikre at alle behandlinger blir registrert i en behandlingsprotokoll. Revisjonen kan også se at kommunen har rutiner for å undersøke personvernskonsekvens ved nye behandlinger, men revisjonen har ikke kontrollert at disse rutinene blir fulgt opp fortløpende.

Når det gjelder overgangen fra et system til et annet skaper dette utfordringer for dokumentasjonskravet i personvernsforordningen. Revisjonen har forståelse for at personvernsarbeid er løpende og at det alltid vil være en periode ved overgangen fra et system til et annet der ikke all dokumentasjon ligger i det nye systemet fra første dag. Det er derimot viktig at all nødvendig dokumentasjon ligger i det gamle systemet, noe det ser ut som det gjør basert på de oversendte dokumentene fra kommunen.

Revisjonen vurderer at kommunen har videreført arbeidet med å vurdere behovet for, dokumentere og gjennomføre DPIA-er. Revisjonen konkluder på bakgrunn av kommunens redegjørelse og oversendt dokumentasjon at kulepunktene 11 og 12 har blitt fulgt opp.

3.4 Kulepunkt 2

2: Behandle de ulike typene kommunikasjonskanaler som ansatte benytter som sms, chat, e-post osv.

3.4.1 Administrasjonens redegjørelse for kulepunkt 2

Til forvaltningsrevisjonsrapporten uttalte kommunedirektøren at de skulle begynne å bruke journalsystemet «Elements» i 2020 og gjennomføre personvernskonsekvensvurderingen for ulike kommunikasjonskanaler.

Kommunen opplyser til revisjonen at de har utarbeidet rutiner og behandling for de ulike typene informasjonskanaler som de har lagt i Risk Manager. Når det kommer til lagringsbegrensning opplyser kommunen om at de bruker HR-Norge sin mal og har beskrevet dette i sikkerhetsrutinene. Videre opplyser kommunen at de har lagt til en henvisning til bevaring- og kassasjonsplanen i sletterutinene.

Kommunen opplyser at de i dag journalfører SMS-er i Elements, eller i fagsystemet Gerica, der man kan dokumentere aktivitet. SMS-er blir lagret som e-post før de overføres til arkivet. Kommunen oppgir at når det kommuniseres utenfor fagsystemer inneholder disse meldingene ikke personopplysninger. Kommunen har og lagt inn en sperre i e-post systemet. Dette gjør at det ikke er mulig å sende kontonummer eller personnummer på e-post.

3.4.2 Revisjonens vurderinger

Revisjonen vurderer basert på kommunens redegjørelse og oversendt dokumentasjon på vurderte behandlinger, at kommunen har vurdert personvernskonsekvensen på de fleste kommunikasjonskanalene. Revisjonen konkluderer med at kommunen har fulgt opp kulepunkt 2.

3.5 Kulepunkt 6, 7 og 3

6. Sikre at personopplysninger ikke lagres lenger enn det som er nødvendig og forsvarlig for den enkelte sak.
7. 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.
3. vurdere lagring og sletting av personopplysninger og personvernkonsekvens.

3.5.1 Administrasjonens redegjørelse for kulepunkt 6, 7 og 3

Kommunen opplyser om at det nå er etablert punkter om lagring, pseudonymisering og sletting av personopplysninger i dokumentet «Sikkerhetspolitikk for behandling av personopplysninger etter GDPR». I tillegg benytter de seg av malen til HR-Norge for GDPR.

Kommunen oppgir at de arbeider med å utarbeide rutiner for sletting og at dette ansvaret ligger på den som «eier» behandlingen. Kommunen opplyser om at tidspunkt for sletting er lagt inn i protokollen.

Videre oppgir kommunen at de ikke lagrer sensitive opplysninger på minnepinner og at minnepinnene de bruker er krypterte. De har heller ikke rutiner for sletting av informasjonen på minnepinnene, siden de oppgir at de ikke inneholder sensitiv informasjon. Kommunen har heller ingen registrerte avvik på tap av minnepinne.

3.5.2 Revisjonens vurderinger

Revisjonen ser i dokumentet «Sikkerhetspolitikk for bruk av IT» at punkt 1.15 omhandler lagring. Her står det at sensitive opplysninger skal lagres på kommunens server. Hvis dette ikke er mulig er det anledning til å legge det over på krypterte minnepinner. Dette kommer også frem i punkt 3.2.17 i dokumentet «Sikkerhetspolitikk for behandling av personopplysninger etter GDPR» der det åpnes for muligheten til å lagre data på krypterte minnepinner. Revisjonen finner at dette ikke er i samsvar med redegjørelsen fra kommunen. Dette kan skyldes at det er avvik mellom det som er fastsatt i dokumentene og hvilken praksis som er vanlig i kommunen. I et slikt tilfelle vil det likevel være uheldig at dokumentene inneholder slike feil, siden det kan føre til at opplysninger lagres i strid med ønsket praksis. Dersom det er ønskelig fra kommunens side å benytte minnepinne til slik lagring, bør kommunen sikre at det er etablert rutiner for å slette potensielt sensitiv data som befinner seg på minnepinner, noe de oppgir å ikke ha etablert per i dag.

I dokumentet «Sikkerhetspolitikk for behandling av personopplysninger etter GDPR» står det at e-post med personopplysninger skal pseudonomyiseres. Videre står det i punkt 3.2.7 at opplysninger som ikke lenger er nødvendig for formålet skal slettes eller sperres. Kommunen arbeider med å utarbeide rutiner på dette området. Her må kommunen ikke bare ta hensyn til kravene fra personvernsforordningen, men også ta stiling til om dataene er arkivverdige. Revisjonen konkluderer med at kommunen har påbegynt arbeidet med kulepunkt 6 og første del av kulepunkt 3 som går ut på å sikre at personopplysninger ikke lagres lenger enn det som er nødvendig og forsvarlig for den enkelte sak.

Andre halvdel av kulepunkt 3 som omhandler personvernskonsekvens, er allerede diskutert under kulepunkt 11 og 12. Her konkluderte revisjonen med at dette var fulgt opp. Når det kommer til den delen av kulepunkt 7 og 3 som omhandler å sikre at opplysninger skal slettes eller pseudonymiseres, og om grunnlaget for behandlingen har endret seg, har kommunen skriftlige føringer på hva som skal lagres og når

det skal slettes. De har derimot ikke ferdigstilt rutiner for dette. I dag ligger ansvaret på den individuelle behandleren, og revisjonen vurderer at dette arbeidet ikke er tilstrekkelig systematisk per i dag. Revisjonen konkluderer dermed med at kulepunkt 7 og 3 er påbegynt.

3.6 Kulepunkt 10

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

3.6.1 Administrasjonens redegjørelse for kulepunkt 10

Kommunen opplyser at det ligger informasjon om kommunens web-kameraer på kommunens intranett og på den gamle hjemmesiden til kommunen. Videre informerer kommunen om at de har gjennomført en behandling av disse kameraene og at disse ikke fanger opp personidentifiserbar data. Kommunen informerer også om at mer informasjon om web-kameraene og personvern skal legges lett synlig på førstesiden til deres nye hjemmeside.

3.6.2 Revisjonens vurderinger

Revisjonen kan se at kommunen har gjennomført en behandling av sine web-kameraer basert på oversendt dokumentasjon, men har ikke kontrollert denne dokumentasjonen i detalj. Revisjonen konkluderer på bakgrunn av kommunens redegjørelse at første del av kulepunkt 10, vedrørende å gjennomføre en behandling av sine webkameraer, er fulgt opp.

Når det kommer til andre del av kulepunkt 10, finner ikke revisjonen informasjon om hensikten til bruken av web-kameraene på kommunens hjemmesider[4]. Revisjonen finner heller ikke informasjon om at kameraene ikke inneholder personidentifiserende data. Kommunen opplyser, som gjengitt over, at dette skal legges ut på den nye hjemmesiden. Arbeidet er dermed ikke ferdigstilt. Etter en helhetsvurdering konkluderer revisjonen med at kulepunkt 10 er delvis fulgt opp.

3.7 Kulepunkt 1

1. 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.

3.7.1 Administrasjonens redegjørelse for kulepunkt 1

Til forvaltningsrevisjonsrapporten uttalte kommunedirektøren at det skulle utarbeides en spesifikk personvernserklæring for barn og unge.

Kommunen har opplyst revisjonen om at informasjon om personvern i dag ligger på hjemmesiden, i søkemotoren og i søk med «Kommune-Kari». Videre opplyser kommunen at de vil legge ut en personvernserklæringen godt synlig på den nye hjemmesiden.

Kommunen informerer også om at de har lagt inn en lenke til hjemmesiden «dubestemmer.no» i deres generelle personvernserklæringen og at innholdet på denne hjemmesiden skal være tilpasset barn og

[4] https://www.halden.kommune.no/tjenester/byen-og-kommunen/informasjon-om-halden/webkamera

unge. Denne siden driftes av Utdanningsdirektoratet. De har lagt ut en generell personvernserklæringen på kommunens hjemmeside og på intranettet. I tillegg skal denne være sendt ut til rektorene i grunnskolen.

3.7.2 Revisjonens vurderinger

På Halden kommunens hjemmeside ligger det i skrivende stund en generell personvernserklæring nederst på forsiden. Denne gjelder kommunen elektroniske løsninger, kommunens fagsystemer og andre henvendelser til kommunen. Her ligger det forklart hvordan Halden kommune behandler personopplysninger, en lenke til gjeldene lov og et skjema for innsyn. Det ligger imidlertid en ødelagt lenke på denne siden, se vedlegg 6.1 til datatilsynet.

Når det gjelder personvernserklæringen for barn og unge har alle kommunens barneskoler og ungdomsskoler generell informasjon på sine hjemmesider om informasjonskapsler/cookies. Denne angår bruk av skolenes nettside spesifikt, og disse er ikke spesifikt rettet mot barn og unge.

Revisjonen finner at den generelle personvernerklæringen på Halden kommune sine nettsider inneholder en lenke til nettsiden «dubestemmer.no» som er laget for barn og unge. Dette er en nettressurs om personvern og nettvett for barn og unge fra 9 til 18 år. Revisjonen får imidlertid ikke åpnet denne lenken på våre pc-er på grunn av at nettsiden har et sikkerhetsproblem. Revisjonen går ut ifra at det er mulig å åpne siden internt i Halden kommune siden kommunen ikke rapporterer om tilsvarende problemer på forespørsel fra revisor.

Videre finner ikke revisjonen en egen personvernserklæring for barn og unge på skolenes åpne nettsider, men ser at 5 av 11 skoler har lagt ut en link til Halden kommune sin generelle personvernerklæring. Dessverre er disse lenkene ofte vanskelige å finne, og lenker noen ganger til gamle versjoner av dokumentet. Den generelle personvernserklæringen er ikke etter revisjonens vurdering tilpasset barn og unge. I tillegg er det kun 1 av 11 skoler som har lagt ut en lenke til nettsiden «dubestemmer.no», som er en side med generell informasjon om personvern for barn og unge.

Revisjonen anbefalte i forvaltningsrevisjonsrapporten å gjøre informasjon om kommunens behandling av personopplysninger forståelig for flere grupper i forskjellige systemer. Revisjonen ser at man blant annet ved å skrive inn personvern i «kommune-Kari» får presis og lett forståelig informasjon om personvern. Her gis det for eksempel god informasjon om hva som skjer med informasjon man oppgir i chatten. Dette gir god informasjon til brukere som ikke har lest hele personvernerklæringen om hva som skjer med deres personlige informasjon i kommunen.

Revisjonen finner at Halden kommune har en generell personverserklæring på sin nettside, og at alle barneskoler og ungdomsskoler har informasjon om bruk av informasjonskapsler på sine hjemmesider. Dette gjelder informasjon som blir samlet inn om dem i skolens systemer og generelt i kommunen. Revisjonen har ikke fått oversendt spesifikk informasjon om hvilken informasjon elever får når de bruker skolenes fagsystemer, og har ikke fått noen indikasjoner på at det er mer alderstilpasset informasjon innad i fagsystemene. Her går revisjonen ut ifra at det er den generelle personvernserklæringen til kommunen som også skal dekke de spesifikke fagprogrammene.

For informasjon tilrettelagt for barn og unge henviser kommunen til en hjemmesiden «dubestemmer.no». Dette er en hjemmeside som driftes av Utdanningsdirektoratet og er derfor ikke tilpasset Halden kommunes fagsystemer. Oppsummert finner revisjonen at kommunen har arbeidet med å gjøre informasjonen om hvordan den behandler personopplysninger mer tilgjengelig for ulike grupper, men at det ikke er utarbeidet en egen personvernserklæring for barn og unge. Revisjonen konkluderer med at kulepunkt 1 er delvis fulgt opp.

3.8 Kulepunkt 4

4. Ha en gjennomgang av hvilke kategoriene personopplysninger som det må innhentes samtykke til på de ulike fagområdene.

3.8.1 Administrasjonens redegjørelse for kulepunkt 4

I forvaltningsrevisjonsrapporten uttalte kommunedirektøren at det skal utarbeides rutiner for når man bruker samtykke som rettsgrunnlag og at dette skulle legges ut på intranettet.

Kommunen opplyser at rutine for hvilke kategorier av personopplysninger kommunen må ha samtykke for å behandle, er utarbeidet. Dette skal være tilgjengeliggjort for barnevernstjenesten, PPT, skole og sykehjem i programmet Smartvakt. Det ligger også på intranettet under IKT, personvern og informasjonsenhet ifølge kommunen.

3.8.2 Revisjonens vurderinger

Kommunen har oversendt dokumentet «Samtykke som behandlingsgrunnlag» som gjør rede for hva slags behandlinger som man kan bruke samtykke til for å gjennomføre. Dette dokumentet skal være tilgjengelig for de ansatte i kommunen. Revisjonen konkluderer på bakgrunn av dette at kulepunkt 4 er fulgt opp.

3.9 Kulepunkt 8

8. Videreføre arbeidet med databehandleravtaler, slik at kommunen har avtale med alle databehandlere

3.9.1 Administrasjonens redegjørelse for kulepunkt 8

Kommunen opplyser at databehandlingsavtaler oppdateres og inngås forløpende. Kommunen har oversendt den siste inngåtte databehandleravtalen fra kommunen og noe dokumentasjon på hvordan de holder oversikt over inngåtte og ikke-inngåtte databehandleravtaler. Videre opplyser de at kommunen arbeider med dette løpende.

3.9.2 Revisjonens vurderinger

Revisjonen har ikke gått inn i oversikten over databehandleravtaler i detalj, men ser at kommunen har en oversikt over inngåtte avtaler og avtaler som skal inngås. Revisjonen kan blant annet se at kommunen har inngått nye avtaler siden revisjonen ble gjennomført, men vi har ikke satt oss inn i hvor mange som er utestående. Revisjonen konkluderer at kommunen har fulgt opp kulepunkt 8.

Kulepunkter knyttet til rapportering, internkontroll, opplæring og skole

3.10 Kulepunkt 9

9: Se til at personvernombudet rapporterer til høyeste ledelsesnivå i kommunen

3.10.1 Administrasjonens redegjørelse for kulepunkt 9

Kommunen uttaler at personvernombudet før rapporterte til kommuneadvokaten, men at personvernombudet nå rapporterer direkte til kommunedirektøren.

3.10.2 Revisjonens vurderinger

I følge kommunen rapporterer nå personvernombudet direkte til kommunedirektøren. Revisjonen konkluderer på bakgrunn av dette at kulepunkt 9 er fulgt opp.

3.11 Kulepunkt 13

13: Etablere og implementere interkontroll på personvernområdet

3.11.1 Administrasjonens redegjørelse for kulepunkt 13

Kommunen opplyser om at internkontroll knyttet til personvernområdet er knyttet opp til resten av internkontrollarbeidet i Risk Manager. I dag opplyser kommunen om at dette arbeidet ligger ute i avdelingene og at de ikke har et godt samlet system for dette.

Kommunen opplyser ytterligere at de holder på å endre systemet for internkontroll. De har også opprettet en egen informasjonssikkerhetsgruppe som skal arbeide med dette. Det nye intranettet skal ifølge kommunen ha et stort fokus på internkontroll. I tillegg opplyser kommunen om at de arbeider med å anskaffe et nytt ledersystem for informasjonssikkerhet.

3.11.2 Revisjonens vurderinger

Revisjonen ser at kommunen arbeider med å etablere og implementere internkontroll på personvernområdet. Revisjonen har ikke sett på hvordan internkontrollen er bygget opp i Risk Manager, og har heller ikke undersøkt hvordan det nye systemet for internkontroll skal se ut. Revisjonen konkluderer med at kulepunkt 13 er påbegynt.

3.12 Kulepunkt 14

14. Sørge for at opplæring blir prioritert nedover i organisasjonen

3.12.1 Administrasjonens redegjørelse for kulepunkt 14

Kommunen uttaler til revisjonen at koronasituasjonen har forsinket arbeidet med opplæring nedover i organisasjonen. Kommunen har arbeidet med personvern ved å gjennomføre fysiske møter, sende ut e-post og ved å gjennomføre Teams-møter. I tillegg har de utarbeidet korte opplæringssekvenser i personvern som blir sendt ut til alle ansatte ukentlig. De dokumenterer hvem som har fullført denne opplæringen, og arbeider med å øke gjennomføringsprosenten blant annet ved at ledere oppfordrer til å gjennomføre

kursene. Kommunen har også oversendt dokumentasjon på gjennomførte sekvenser og et eksempel på en ukentlig e-post.

3.12.2 Revisjonens vurderinger

Revisjonen finner at kommunen har utarbeidet opplæringssekvenser og jobber aktivt med opplæring av sine ansatte på personvernområdet. Kommunen arbeider aktivt med å nå ut til ansatte på alle nivåer i kommunen, og har gjort dette på flere plattformer. Revisjonen har sett dokumentasjon på at ansatte har fullført opplæring og sett et eksempel på en opplæringssekvens fra kommunen. Revisjonen konkluderer basert på oversendt dokumentasjon og kommunens redegjørelse at kommunen har fulgt opp kulepunkt 14.

3.13 Kulepunkt 5

5: Etablere felles rutiner for enhet- skole, når det gjelder tilgangsavgrensing til fysiske arkiv.

3.13.1 Administrasjonens redegjørelse for kulepunkt 5

I forvaltningsrevisjonsrapporten kommenterte kommunedirektøren at skolenes papirarkiv skal digitaliseres og det skal settes opp en løsning slik at skole og PP-tjenesten får tilgang.

Kommunen opplyser at arbeides med å lage enhetlige rutiner for skole arbeides med både på direktoratsnivå og på kommunenivå. I kommunen har de nedsatt en arbeidsgruppe med medlemmer fra undervisning/oppvekst og IT som jobber med et nytt system. Elevarkivet vil, ifølge kommunen, bli tatt inn i dette systemet. Kommunen informerer om at det arbeides med å gjøre skolenes arkiver heldigitale. Videre jobber de med rutiner for det som gjenstår av papirarkivet.

3.13.2 Revisjonens vurderinger

Halden kommune jobber løpende med utfordringer knyttet til elevers personopplysninger og arkiv. Det foregår et arbeid med å digitalisere dagens fysiske løsninger. Dette innebærer en endring i hvordan man får tilgang til arkivet, men det er fortsatt i dag fysiske arkiver uten felles rutiner for tilgangsbegrensning. Revisjonen konkluderer på bakgrunn av dette at arbeidet med kulepunkt 5 er påbegynt.

4 Konklusjon

Revisjonen har i denne rapporten vurdert om og i hvilken grad kommunestyrets vedtak i sak PS 2020/11 den (16.01.20) er fulgt opp. Revisjonen konkluderer at av de 14 kulepunktene er 5 påbegynt og 9 er delvis eller helt fulgt opp.

Revisjonen anbefaler kommunen å videre fokusere på følgende:

Kulepunkt 6. Sikre at personopplysninger ikke lagres lenger enn det som er nødvendig og forsvarlig for den enkelte sak.

Kulepunkt 7. 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.

Kulepunkt 3. Vurdere lagring og sletting av personopplysninger og personvernkonsekvens.

Kulepunkt 10. Informere kommunens innbyggere om hensikten med og bruken av sine webkameraer.

Kulepunkt 1. 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.

Kulepunkt 13. Etablere og implementere interkontroll på personvernområdet

Kulepunkt 5: Etablere felles rutiner for enhet- skole, når det gjelder tilgangsavgrensing til fysiske arkiv.

Østre Viken kommunerevisjon IKS
Rolvsøy, 01.06.2021

Casper Støten (sign.)
oppdragsansvarlig revisor

Kaia Andrea Sølverød (sign.)
forvaltningsrevisor

5 Dokumentliste

- Den registrertes rett til begrensning av behandling av personopplysninger
- Kommunikasjonskanaler
- Personvernerklæring for Halden Kommune
- Prosedyre for behandling av personopplysninger etter GDPR
- Samtykke som behandlingsgrunnlag
- Sikkerhetspolitikk for behandling av personopplysninger etter GDPR
- Sikkerhetspolitikk for bruk av IT
- Behandling webkamera
- Bevaring- og kassasjonsplan Godkjent RLG – personvern PDF
- Databehandleravtale Helseboka
- DPIA Hospital IT 24.01.2020
- GDPR_veiledning_for_HR
- Ikke vurderte behandlinger
- Kopi av Utkast-Handlingsplan 2021 DVØ – Infosik
- MAL DPIA Halden kommune 2020
- Rapport NanoLearning
- VS Databehandleravtaler
- Vurderte behandlinger
- Revisjonsoppfølgingsrapport (ligger i vedlegg 6.2)
- Svarbrev til revisjon (ligger i vedlegg 6.2)

6 Vedlegg

6.1 Skjermdumper fra Halden kommunes hjemmeside

Link går ikke til datatilsynet

https://www.halden.kommune.no/personvernerklaring/

6.2 Administrasjonens redegjørelse

6.2.1 Uttalelsene fra personvernombudet i Halden kommune til revisjonen

Oppfølging av kommunestyrevedtak 16.01.2020, Revisjon, personvern.

Forespørsel om uttalelse til oppfølging av personvernsrapproten ble sendt til Kommunaldirektør og personvernombudet. Personvernombudet har sendt følgende uttalelse på vegne av kommunen:

Oppfølging av kommunestyrevedtak 16.01.2020, Revisjon, personvern.

I 2020 har det blitt jobbet systematisk med å rette opp mangler og avvik i revisjonsrapporten personvern, slik at Halden kommune oppfyller kravene etter GDPR.
De fleste punktene er ferdig utarbeidet og publisert i internkontrollsystemet, Risk Manager. Øvrige punkter er temaer som det jobbes med kontinuerlig i form av opplæring, implementering, problemløsning i oppståtte saker, forbedringsarbeid i eksisterende rutiner og kvalitetssikring.
Implementering av regelverket i arbeidshverdagen ute i avdelingene, er en kontinuerlig prosess.
Skole er en utfordring i forhold til personvern, da det benyttes mange ulike systemer og plattformer på de ulike skolene. Dette er også en kjent utfordring for hele kommune-Norge. Et utvalg i direktoratet jobber med dette på landsbasis, slik at vi får en enhetlig modell i sektoren. Nettverket for Personvernombud i Digi Viken Øst har også dette på agendaen for 2021. Undertegnede er en del av dette nettverket. Parallelt med dette, jobbes det steg for steg for å få gode løsninger i Halden-skolen. Det er nedsatt en arbeidsgruppe i undervisning-oppvekst / IT hvor det jobbes med nytt system. Dette skal resultere i sikrere samhandling mellom skolesystemene og kommunikasjon med foresatte, slik at personvernet ivaretas etter gjeldende lovverk. Elevarkivet vil også inngå her.

Følgende punkter er etablert:

- Det er lagt inn heading «Personvern» på kommunens hjemmeside.
- Personvernerklæring for barn og unge: I eksisterende personvernerklæring er det lagt inn link til "Du bestemmer", som er en nettside tilpasset barn og unge i ulike aldersgrupper. Denne ligger på kommunens hjemmeside, intranett og er sendt ut til rektorene for publisering på skolenes hjemmesider. Ansvarlig for sistnevnte er rektorene på hver enkelt skole. Personvernombudet følger opp.
- Behandle ulike typer kommunikasjonskanaler: rutine er utarbeidet, og behandling skrevet. Er tilgjengeliggjort i Riska Manager.
- Lagringsbegrensning: Her benyttes malen i HR-Norge. Dette er også beskrevet i kommunens sikkerhetspolitikk.
- I sletterutinen er det lagt inn henvisning til bevaring- og kassasjonsplan.
- Lagring og pseudonymisering i fagprogram: Beskrevet i sikkerhetspolitikken.
- Rutine for hvilke kategorier av personopplysninger vi må ha samtykke for, er utarbeidet. Tilgjengeliggjort i Barnevernstjenesten/PPT/skole, samt sykehjem i forbindelse med Smartvakt.
- Databehandleravtaler: Oppdateres fortløpende.
- PVO-rapportering til Kommunedirektøren har vært utsatt pga mye arbeid med Covid-19. Rapporteringen har i denne perioden vært til Kommuneadvokaten. Møteplan for rapportering til Kommunedirektøren er satt fra januar 2021.
- DPIA (personvernkonsekvensvurdering), der risikoen er høy: Vurdering gjøres ved hver ny behandling.
- Web-kamera: Informasjon ligger på kommunens hjemmeside og kommunens intranett. Behandling er utarbeidet.

I januar 2021 etablerte Halden kommune en sikkerhetsgruppe. Gruppa består av IT-sjef, sikkerhetsansvarlig, personvernombud og representanter fra alle kommunalområdene. 2 av medlemmene inngår også i Digi Viken Øst sin gruppe "Informasjonssikkerhet", og er et samarbeid på tvers av kommunene i gamle Østfold. Med felles plattform står vi sterkere i forhold til sikkerhet.

Følgende punkter er en kontinuerlig prosess:

- Felles rutiner, skole: under arbeid i staben, undervisning/oppvekst (beskrevet i innledningen). PVO er rådgivende part.
- Behandlingsprotokollen og rutiner på ulike kommunikasjonssystemer er utarbeidet, og ligger pr i dag i Risk Manager. Her fylles det på med behandlinger fortløpende.
  Kommunen har gått til anskaffelse av DigiOrden, «Orden i eget hus», som fra 01.01.21. ligger under KS. Arbeidet i dette programmet har startet, og alle våre applikasjoner er lagt inn i denne løsningen. Digi Viken Øst har også valgt denne løsningen, og det er inngått et samarbeid for å få alt på plass, slik at det blir i tråd med personvernforordningens krav om dokumentasjon.
- Internkontroll, personvern inngår i kommunens eksisterende internkontrollsystem i Risk Manager. Denne skal videreutvikles når vi i løpet av våren etablerer nytt intranett. Her vil det bli dokumentert (egenkontroll) når ansatte har lest dokumenter, rutiner og prosedyrer, slik at vi sikrer at alle er oppdatert på gjeldende dokumenter. Personvernombudet følger opp dette.
- Databehandleravtaler. Inngås fortløpende
- Opplæring i personvernregelverket: Resterende avdelinger ble våren 2020 satt på vent grunnet koronasituasjonen. Opplæringen pågår kontinuerlig i form av fysiske møter (begrenset pga Covid 19), mail-informasjon og Teams-møter. Det er også tatt i bruk Nano-learning (JungleMap), hvor 2-3minutters opplæringssekvenser i personvern blir publisert ut til alle ansatte ukentlig. Her blir det dokumentert hvem som har fullført opplæringen.
- Tilgangsavgrensning til fysiske arkiv, skole: Staben undervisning/oppvekst har dette under arbeid. (Se beskrivelse tidligere i dokumentet.)

Halden 07.02.21
Hilde Furuseth
Personvernombud

6.2.2 Svar på spørsmål til oppfølgingsrapport om personvern, april 2021

Litt forhåndsinformasjon:
Vi jobber i disse dager med nytt intranett (skal være ferdig i løpet av våren.) Her bygger vi ny struktur, slik at det blir mye mer oversiktlig enn dagens intranett. Siden bygges på temaer slik at det blir lett å finne fram de dokumentene man har behov for, og det blir lagt inn lesebekreftelse på dokumenter hver enkelt ansatt må være kjent med. Her kommer bl.a alt innenfor personvernområdet, og vil inngå som dokumentasjon i internkontrollen. Det er stort fokus på internkontroll i vårt nye intranett.

Svarene som følger, er gitt i samme rekkefølge som i tilsendte dokument fra revisjonen.

Generelle: Alle tidligere innsendte dokumenter ligger i Risk Manager eller i SharePoint.

- **Anbefaling 10 og 11:**

Behandlingsprotokoll for behandlinger av personopplysninger ligger vedlagt. Dersom en behandling avdekker at den har høy personvernkonsekvens for den registrerte, vil dette utløse en DPIA. Mal på DPIA og gjennomført DPIA på "Hospital-IT" (høy personvernkonsekvens) er vedlagt. Det jobbes kontinuerlig med dette.

Rutine: Når ny behandling utarbeides, vil det fremkomme om man også må gjennomføre en DPIA. Det er «eier» av behandlingen (leder) som er ansvarlig for dette. Personvernombudet skal alltid involveres i dette. Rutine blir utarbeidet.

- **Anbefaling 5, 6, 12:**

Sletting av personopplysninger: Behandlingen inneholder et punkt med når opplysningene skal slettes, og blir slettet på det tidspunktet protokollen tilsier det. Tidspunktet avhenger av hvilken lovhjemmel som ligger til grunn. Den som «eier» behandlingen, er ansvarlig for å gjennomgå sine behandlinger etter gitt tidsplan. Rutine vil bli utarbeidet.

Teksten under er hentet fra Sikkerhetspolitikk for bruk av personopplysninger:

3.2.7. Unødvendige opplysninger skal slettes
Du skal slette eller sperre opplysninger som ikke lenger er nødvendige for formålet med registreringen. Dette gjelder selv om opplysningene ikke er mangelfulle.
Dersom dokumentet blir åpenbart misvisende etter sletting, og supplering med korrekte opplysninger ikke er mulig, skal hele dokumentet makuleres.
Dette gjelder ikke dersom opplysningene skal oppbevares i henhold til arkivloven eller annen lovgivning.
Dersom du har registrert opplysninger som er sterkt belastende for den registrerte, kan vedkommende kreve at disse personopplysningene sperres. Vedkommende kan også kreve at opplysningene slettes dersom dette ikke strider mot annen lov, og det er forsvarlig å slette opplysningene etter en samlet vurdering av de motstridende interesser.
Sletting skal erstattes med registrering av korrekte og fullstendige opplysninger dersom det ligger til rette for det.

Personopplysninger kan oppbevares til historiske, vitenskapelige og statistiske formål selv om det ikke er nødvendig lenger etter sitt opprinnelige formål. Forutsetningen er at samfunnets interesse i oppbevaringen klart overstiger den registrertes interesse i personvern.

Minnepinner: Minnepinner som er i bruk (gjelder i hovedsak i skole) er kryptert. Vi har ikke rutine for sletting av personopplysninger på minnepinne, da det ikke skal lagres sensitiv informasjon på minnepinne. Ingen registrerte avvik på tap av minnepinner. Minnepinner ligger i låst arkiv i skolenes administrasjon, og må hentes ut ved behov.

Internkontroll: Egenkontroll skal gjennomføres av hver enkelt ansatt, ledere og systemforvaltere. Dette gjøres ute i avdelingene, og pr i dag har vi ikke et godt system hvor dette samles.

I DigiViken øst (DVØ) skal det anskaffes et ledelsessystem for informasjonssikkerhet, som omfatter kontroll av den enkelte enhet.

Halden kommune har opprettet en egen informasjonssikkerhetsgruppe, som får ansvaret for å etablere nytt internkontrollsystem.

Handlingsplan for DVØ informasjonssikkerhet er vedlagt.

NanoLearning er et godt verktøy for å dokumentere gjennomført opplæring, og denne inngår også i dokumentasjonen for internkontroll. Alle ansatte i kommunen mottar NaniLearning via e-post. Opplæringen er obligatorisk. Deltagelsen var dessverre lav, men økte etter at dette ble lagt fram i Kommunedirektørens utvidede ledermøte hvor lederne ble bedt om å være pådrivere i forhold til egne ansatte. Det er også sendt ut påminnelser på mail.

Rapport for gjennomføring ligger vedlagt.

- **Anbefaling 9:**

Informasjon om personvern og web-kameraer finner man pr i dag på "søk" på hjemmesiden. Vi har nylig fått ny hjemmeside, og disse temaene vil bli lagt godt synlige på førstesiden, slik de gjorde på den gamle hjemmesiden. Webkameraene som finnes i kommunen (Svinesund, Gjestehavna, Fredriksten Festning, taket på Helsehuset) fanger ikke opp personidentifiserbare data, kun oversiktsbilder over byen. Behandlingsprotokoll er vedlagt.

- **Anbefaling 1 og 2:**

Informasjon om personvern finnes pr i dag nederst på hjemmesiden, i søkemotoren og i søk på «KommuneKari». Vi har nylig fått ny hjemmeside, og temaet vil bli lagt godt synlig på førstesiden, slik det gjorde på den gamle hjemmesiden.

https://www.dubestemmer.no/: Det er Utdanningsdirektoratet som er ansvarlig for nettsiden, i samarbeid med Datatilsynet. Halden kommune er ikke kjent med at denne siden ikke er sikker, til tross for nøye gjennomgang. U.t har vært i kontakt med Utdanningsdirektoratet, og de har ingen indikasjoner på at nettsiden ikke er sikker.

Skole og barnehage informerer elever/barn og deres foresatte via skolenes hjemmesider, samt at informasjonen ligger på kommunens hjemmeside og intranett.
Elements er tatt i bruk, og sms'er blir journalført i Elements, evnt annet fagprogram (Gerica) for å dokumentere aktivitet. Dette gjøres ved at SMS'n blir lagret som e-post/fil og overført til Elements via egnet verktøy.

Når det brukes kommunikasjonskanaler utenfor fagsystem, inneholder ikke meldingene personopplysninger (kun f.eks. «husk timen din i morgen»). DPIA på bruk av disse kommunikasjonskanalene er dermed ikke nødvendig.
For å øke sikkerheten, er det satt på en sperre i exchange, som gjør at det ikke går å sende kontonr, personnr etc. via e-post.

HR-Norge sin mal er vedlagt.

Bevarings- og kassasjonsplan ligger vedlagt.

- **Anbefaling 3:**

"Samtykke som behandlingsgrunnlag" ligger på intranettet under IKT, personvern og informasjonssikkerhet.

- **Anbefaling 7:**

Oversikt over inngåtte Databehandleravtaler er vedlagt.
Dokumentasjon på siste inngåtte Databehandleravtale er vedlagt.

Rapportering, opplæring, skole

- **Anbefaling 8:**

Personvernombudet rapporter til Kommunedirektøren.

- **Anbefaling 13:**

Mail med opplæringsvideoer: Sendes som separat mail til revisjonen (videresender en jeg allerede har gjennomgått). På siste side i kurset ser du alle leksjonene som har blitt sendt ut, og tidsbruk på hver enkelt)

Alle ansatte i Halden kommune mottar mailene fra NanoLearning.

Rapport for gjennomføring er vedlagt. Som nevnt tidligere var deltagelsen lav i starten, men dette har bedret seg. Vi har høyt fokus på å få svarprosenten ytterligere opp.

Legger også ved informasjonsmail om nytt NanoLearning-kurs i digital sikkerhet, som er sendt ut til alle ansatte i Halden kommune.

- **Anbefaling 4:**

Felles rutiner for tilgang til skolenes fysiske arkiv: Skoleadministrasjonen, i samarbeid med arkivet, jobber nå med skolenes arkiv (elevmapper), for å kun ha elektronisk arkiv innen kort tid.

Rutine for det som gjenstår av papirarkiv blir utarbeidet.

Halden, 09.04.2021
Hilde Furuseth
Personvernombud

6.3 Konklusjon/ anbefalinger fra forvaltningsrevisjonsrapporten

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

6.4 Kommunedirektørens uttalelse

Kommunedirektørens uttalelse til høringsutkast, «Oppfølgingsrapport i personvern for Halden kommune».

Generelt

Offentlig sektor står foran store utfordringer i årene fremover. Rammebetingelser endres og oppgaver må løses på annen måte og med det må arbeidsprosesser endres. Det er forventninger fra innbyggere som skal møtes; Kommunen skal bl.a. åpne opp, være lettere tilgjengelige og digital selvbetjening skal være et førstevalg. Personvern og informasjonssikkerhet er med det nøkkelord. God håndtering av persondata og sikre løsninger blir med det en grunnpilar i omstillingsarbeidet. Godt system, god kultur og sikre løsninger vil gi oss nødvendig tillit fra brukere, noe som er en forutsetning for kunne nå målsettinger, både lokalt og nasjonalt. Det er derfor viktig at dette arbeidet fortsatt har høy prioritet og blir «allemannseie».

Som nevnt i tidligere innsendt dokumentasjon, er Halden kommune med i en informasjonssikkerhetsgruppe i DigiViken Øst (DVØ). Dette er et svært nyttig samarbeid, hvor vi setter informasjonssikkerhet i fokus, utarbeider felles dokumenter og sikrer framdrift i sikkerhetsarbeidet. Flere av punktene i revisjonens rapport inngår i dette arbeidet, og har et løp med sluttdato.

Som følge av dette arbeidet er det opprettet en informasjonssikkerhetsgruppe internt i Halden kommune. Alle kommunalavdelingene er representert i gruppe for å sikre at arbeidet breddes ut. En videre oppfølging av oppfølgingspunktene i rapporten vil fortsette gjennom denne gruppen.

Kommentarer til punkter

Kommunaldirektøren ønsker å knytte noen kommentarer i til enkelte punkter i revisjonens rapport.

3.5 Kulepunkt 6,7,3 Lagring, sletting, pseudonymisering av personopplysninger.

Det påpekes i revisjonens uttalelse at kommunens opplysninger om lagring på minnepinne og hva som faktisk er beskrevet i «Sikkerhetspolitikk for Halden kommune» ikke stemmer overens. Dette tas til etterretning. Kommunen jobber systematisk med revidering av dokumenter, og dette er ett av de det jobbes med pr i dag. I den nye utgaven vil det ikke være tillatt å lagre personidentifiserbare opplysninger på minnepenn. Dokumentet vil bli publisert i ny versjon om kort tid.

Dette er et av punktene innenfor informasjonssikkerhet, som kommunen samarbeider med DVØ om. Denne informasjonssikkerhetsgruppa utarbeider felles dokumenter for informasjonssikkerhet, og med nødvendige lokale tilpasninger.

3.6 Kulepunkt 10 Webkamera

På kommunens nye hjemmeside er hensikten med webkameraene beskrevet, «Gi innbyggerne oversiktsbilder over byen». Det står også hvor de er plassert. (Festningen, Mølen, Svinesund (for skipstrafikken). Kameraene tar øyeblikksbilder, og det er ikke mulig å identifisere personer.

Vi velger likevel å skrive inn punktet om at det ikke fanges opp personidentifiserende opplysninger.

Det kan være en mulighet for at revisjonen har forvekslet dette punktet med overvåkningskameraer, som også finnes i kommunen. Disse er beskrevet i behandlingsprotokollen, og det er gjort DPIA da det her kan gjenkjennes personer som passerer i kamerasonen. De er satt opp for å forhindre hærverk.

3.7 Kulepunkt 1 Manglende personvernerklæring barn/unge

Dette tas til etterretning, og vil bli prioritert utarbeidet.

Bakgrunnen for å vise til nettsiden «dubestemmer.no» var at den forteller på en alderstilpasset måte hvilke rettigheter vi har som registrerte etter den nye personvernlovgivningen, noe som også forklares i en «ordinær» personvernerklæring. De som leser / får dette gjennomgått, vil få et godt innblikk i hva personvern handler om.
Kommunen har ikke hatt problemer med å åpne siden. Da denne lenken manglet ved mange av skolene, har det nå gått ut ny beskjed til skoleledere om at den skal legges på skolenes hjemmesider.

Den ødelagte lenken til Datatilsynet som ligger på kommunens hjemmeside, er rettet.

3.11 Kulepunkt 13 Internkontroll

Kommunen har materiale på internkontroll, men et mangelfullt samlet system.
Temaet står på agendaen i informasjonssikkerhetsgruppa.
Kommunen har tatt i bruk DigiOrden, hvor behandlingsprotokoller, applikasjoner etc er lagt inn / skal legges inn. Her sjekker vi også muligheten for internkontrollsystem på personvern.
Kommunen tar sikte på å etablere et internkontrollsystem som er enkelt for brukerne, og gir en god samlet informasjon for oppfølging og evaluering.

3.13 Kulepunkt 5 Fysisk arkiv, skole

Kommunen har som mål å digitalisere elevarkivet. Dette er i prosess. Påminnelse om rutine på det gjenstående fysiske elevarkivet ble sendt ut på nytt 26.05.21.

Halden 28.05.21

Roar Vevelstad
kommunedirektør