Personvern

Forvaltningsrevisjonsrapport
Karmøy kommune

30. august 2019

www.kpmg.no

Forord

Etter vedtak i kontrollutvalget i Karmøy kommune 28. november 2018, har KPMG gjennomført en forvaltningsrevisjon rettet mot kommunen sin håndtering og behandling av personopplysninger. Denne rapporten er svar på kontrollutvalgets bestilling.

Oppbygging av rapporten

Våre konklusjoner og anbefalinger fremgår av rapportens sammendrag. Kapittel 1 er en innledning til rapporten. Her blir formål, problemstillinger, revisjonskriterier og metode presentert. I kapittel 2-6 besvarer vi problemstillingene i forvaltningsrevisjonen. Her blir revisjonskriteriene konkretisert, i tillegg til at fakta og vurderinger blir presentert. Tekst som gjengis fra dokumentasjon oversendt fra Karmøy kommune er satt i kursiv. I kapittel 7 presenterer vi våre anbefalinger. I kapittel 8 er rådmannens uttalelse til rapporten tatt inn.

Vi vil takke kommunen for et godt samarbeid og god bistand i arbeidet med denne forvaltningsrevisjonen.

Sammendrag

Formålet med forvaltningsrevisjonen har vært å undersøke konkrete temaer innen personvernlovgivningen, nærmere bestemt hvordan Karmøy kommune har innrettet seg for å oppfylle kravene i personopplysningsloven. Med personopplysningsloven mener vi her den nye personopplysningsloven som trådte i kraft 20. juli 2018, og som også gjennomfører forordning EU 2016/679 (Personvernforordningen).

Under følger først våre konklusjoner, deretter våre anbefalinger.

Problemstilling 1 – Har Karmøy kommune etablert et internkontrollsystem for personvern som tilfredsstiller krav i regelverket?
Karmøy kommune har det siste året arbeidet målrettet for å etterleve krav i personopplysningsloven. Det er utarbeidet mye styrende dokumentasjon, rutiner og prosedyrer og de ansatte har blitt bedt om å gjennomføre et e-læringskurs innen personvern.

Kommunikasjon og opplæring er et lederansvar i kommunen. Personvernrelaterte tema har blitt adressert på ledersamlinger, og det er en forventning til at ledere i kommunen skal bringe informasjon de mottar i ledergrupper videre til neste nivå. Dette gir en sårbarhet ved at kommunen blir avhengig av at mange lag med ledere har tilstrekkelig forståelse for informasjonen de får presentert til at de klarer å videreformidle den tydelig ut i virksomheten. Sårbarheten forsterkes i en overgangsfase med implementering av et nytt ledelsessystem, ved at det blir ekstra utfordrende for den enkelte å oppsøke informasjon på eget initiativ. Det er også behov for økt fokus på opplæring av medarbeidere i organisasjonen, og det bør i den forbindelse vurderes hvilke kommunikasjonskanaler som egner seg inn mot ulike grupper medarbeidere. Det er positivt at ledelsen er bevisst på denne utfordringen, og vurderer tiltak for mer effektiv kommunikasjon og opplæring.

Det er positivt at kommunen har en risikobasert tilnærming, og har startet med å kartlegge de behandlingene som innebærer den største risikoen. Kommunen har organisert protokollen basert på ulike system, og ikke per behandling. Hvilket formål som gjelder for behandlinger i systemet er samlet i "en sekkepost". Tilsvarende er gjort for andre parametere, derunder for behandlingsgrunnlaget. Vår vurdering er at kommunens protokoll er mangelfull, fordi formålet med, og behandlingsgrunnlaget for, den enkelte behandling av personopplysninger ikke fremgår tydelig.

Karmøy kommunes personvernerklæring inneholder henvisninger til personopplysningsloven, og kontaktinformasjon til kommunen og kommunens personvernombud, og gir informasjon om ulike parametere vedrørende de registrertes rettigheter. Vår vurdering er at personvernerklæringen, i likhet med kommunens protokoll over behandlinger, særlig er mangelfull når det gjelder beskrivelse av formålet med behandlinger som gjøres. Det mangler således vesentlige opplysninger for at den registrerte skal ha anledning til å tilstrekkelig forstå hvilke typer opplysninger kommunen vil kunne behandle om vedkommende når de er i kontakt med kommunen. En forståelse for hvilke personopplysninger som behandles er en forutsetning for at den registrerte skal kunne ivareta sine rettigheter.

Det gjøres risikovurderinger både sentralt i kommunen og i Helse- og omsorgsetaten. Kommunen har et forbedringspotensial når det gjelder å systematisk gjennomføre og dokumentere risikovurderinger vurdert opp mot kommunens målsettinger, samt når det gjelder å definere og dokumentere kommunens risikoaksept. Som en del av slike risikovurderinger må det vurderes hvilke tiltak det er behov for å gjennomføre, inkl. en tydelig avklaring av ansvarlig for gjennomføring og frist. Aggregeres slike risikovurderinger opp i en helhet og presenteres for ledelsen sentralt gjennom regelmessige ledelsesgjennomganger, vil det legge til rette for at ledelsen på et overordnet nivå kan prioritere ressurser mellom ulike tiltak, vurdere om restrisikoen er akseptabel på ulike områder, og se den opp mot kommunens totale risikoaksept.

Kommunen har etablert en *Prosedyre for vurdering av DPIA*, men ikke en prosedyre eller veiledning for gjennomføring av DPIA. Vi er ikke kjent med at kommunen har gjennomført noen vurderinger av personvernkonsekvenser, såkalte DPIA'er. Det virker å være et behov for at kommunen veileder involverte medarbeidere i praktisk gjennomføring av vurdering av personvernkonsekvenser (DPIA). I tillegg bør kommunen vurdere å etablere en prosedyre for hvordan utføre DPIA for å legge til rette for en betryggende gjennomføring. Det er positivt at kommunen ser behov for å ha økt fokus på DPIA i tiden fremover.

Våre anbefalinger er at Karmøy kommune prioriterer følgende områder:

1. **Kommunikasjon og opplæring**
   Karmøy kommune holder på å implementere et nytt ledelsessystem. Denne prosessen har trolig bidratt til å hemme effektiv kommunikasjon om styrende dokumenter og krav knyttet til bla. personvern. Det anbefales at kommunens sentraladministrasjon vurderer hvordan den effektivt kan kommunisere styrende dokumenter og krav ut i virksomheten, og iverksetter nødvendige tiltak for å gjøre viktig personvernrelatert informasjon kjent.

   Kommunen bør også vurdere å øke omfanget av opplæring i informasjonssikkerhet generelt, og i krav i personopplysningsloven spesielt. Opplæringen bør systematiseres for å sikre at alle medarbeidere får nødvendig opplæring. Det bør blant annet vurderes hvilke kanaler som egner seg for opplæring av ulike typer medarbeidere, eksempelvis ved at medarbeidere som i begrenset grad benytter epost og administrative systemer i hverdagen, tilbys fysisk opplæring i møter eller lignende for å sikre at de får nødvendig informasjon.

2. **Protokoll over behandlinger og personvernerklæring.**
   Karmøy kommunes protokoll over behandlinger er mangelfull når det gjelder å konkretisere formålet med den enkelte behandlingen av personopplysninger. Det er behov for en gjennomgang og oppdatering av innholdet i protokollen.

   Karmøy kommune bør videre gjennomgå personvernerklæringen, og oppdatere den slik at den tilfredsstiller kravene i personopplysningsloven. Det er særlig behov for å utbedre innholdet i personvernerklæringen når det gjelder en tydeliggjøring av formålet med kommunens behandlinger av personopplysninger, slik at den registrerte gis tilstrekkelig informasjon til å forstå hvilke behandlinger kommunen utfører. Å forstå hvilke behandlinger som utføres, er en forutsetning for å kunne ivareta egne personvernrettigheter.

3. **Profesjonalisering av kommunens risikostyring**
   Det er et potensial for å profesjonalisere kommunens risikostyring, både sentralt og i Helse og –omsorgsetaten. Det anbefales at ledelsen legger en plan for å sikre at det er en betryggende risikostyring. Sentrale momenter innen risikostyring omfatter:

   - Avklare ledelsens risikoaksept
   - Gjennomføre en helhetlig risikoanalyse
   - Dokumentere vurderinger
   - Prioritere tiltak, tilordne ansvar og fastsette frist for lukking av det enkelte tiltak
   - Etablere en rutine for å følge opp lukking av prioriterte tiltak
   - Etablere en rutine for å oppdatere risikoanalysen jevnlig, samt ved vesentlige endringer som påvirker gjeldende risikovurderinger

   Planen må videre dokumenteres og innarbeides i virksomhetens årshjul for internkontroll.

Problemstilling 2 – Hvilken rolle og ansvar har personvernombudet i Karmøy kommune?

Karmøy kommune har etablert et personvernombud iht. kravet i personopplysningsloven artikkel 37. Personvernombudet oppfyller lovens kompetansekrav.

Personvernombudets oppgaver er beskrevet på et overordnet nivå i Karmøy kommune. Det vil trolig være hensiktsmessig å utdype enkelte av personvernombudets oppgaver, for å sikre at det er en felles oppfatning av hva som inngår i ombudets mandat. Behovet for dette forsterkes ved at ombudet er leid inn fra en annen kommune, og det i begrenset grad ligger til rette for løpende avklaringer i det daglige.

Det er sannsynligvis begrenset kjennskap blant en del medarbeidere i Karmøy kommune til hvem som er personvernombud og hva som er hans rolle, og det vil trolig være hensiktsmessig å informere mer aktivt om personvernombudet i organisasjonen.

Vår anbefaling er at Karmøy kommune prioriterer følgende område:

4. **Avklaring av personvernombudets rolle og ansvar**
   Det anbefales at Karmøy kommune, i samarbeid med personvernombudet, utdyper ombudets rolle og ansvar, for å sikre at det er en felles oppfatning av hva som inngår i ombudets mandat. I denne forbindelse bør det blant annet klargjøres i hvilket omfang personvernombudet skal utføre kontroller av virksomheten.

Problemstilling 3 – Hvilke rutiner har kommunen for avviksføring knyttet til brudd på personvernregelverket?

Karmøy kommune har nylig implementert et nytt system der avviks- og forbedringsmeldinger skal rapporteres. Det er behov for å gi kommunens ansatte en god innføring i hvordan det nye systemet skal benyttes, derunder tydelig definere hva som utgjør et avvik, og hvordan og hvor avvik skal rapporteres. I Helse- og omsorgsetaten er det behov for å tydeliggjøre forholdet mellom rapportering av avvik i journalsystemet og i det administrative systemet Compilo, for å legge til rette for en enhetlig og forsvarlig praksis. Det er positivt at det er etablert en rutine der personvernombudet varsles umiddelbart om alle avvik vedrørende personvern som rapporteres i Compilo. Det er også positivt at kommunen har vist evne til å mobilisere relevant personell og raskt få oversikt over situasjonen ved personvernrelaterte avvik.

Vår anbefaling er at Karmøy kommune prioriterer følgende område:

5. **Avvikshåndtering**
   Det er behov for å gi medarbeidere i kommunen nødvendig opplæring i rapportering av avvik i Compilo, for å legge til rette for en god rapporteringskultur. Det bør tydelig defineres hva som utgjør et avvik, og hvordan og hvor avvik skal rapporteres. Videre er det behov for å tydeliggjøre rutinen for rapportering av avvik i journalsystemet sett opp mot rutine for rapportering av avvik i det administrative systemet (Compilo), altså hvilke avvik som skal rapporteres hvor, samt om enkelte avvik skal rapporteres begge steder.

Problemstilling 4 – Er det en klar fordeling mellom roller og ansvar i informasjonssikkerhets-arbeidet i kommunen?

Roller og ansvar er relativt tydelig avklart når det gjelder teknisk sikkerhet og personvern. Det er en viss usikkerhet i virksomheten knyttet til ansvar for informasjonssikkerhet utover teknisk sikkerhet og personvern. Det kan være hensiktsmessig at rådmannens ledergruppe drøfter dette temaet, og tydelig kommuniserer ut i hele virksomheten roller og ansvar for informasjonssikkerhet i kommunen, derunder kommunens handlingsplan for å sikre en betryggende praksis på området.

Vår anbefaling er at Karmøy kommune prioriterer følgende område:

6. **Avklaring av roller og ansvar knyttet til informasjonssikkerhet**

   Det anbefales å tydeliggjøre fordeling av roller og ansvar knyttet til informasjonssikkerhet i kommunen, og kommunisere konklusjonen ut i hele virksomheten. Dette kan med fordel gjøres i sammenheng med kommunikasjon av en handlingsplan for å sikre en betryggende praksis på området.

Problemstilling 5 – I hvilken grad har omsorgssektoren i Karmøy kommune innrettet seg etter det nye personvernregelverket?

Helsesektoren er en gjennomregulert sektor med lang erfaring når det gjelder å forholde seg til strenge krav for håndtering av taushetsbelagt informasjon, derunder personopplysninger. Medarbeidere i Helse- og omsorgsetaten har høy bevissthet når det gjelder å sørge for en forsvarlig

behandling av taushetsbelagt informasjon. Det vurderes som sannsynlig at det er et særlig høyt fokus på personvern i Helse- og omsorgsetaten i kommunen.

Krav i styrende dokumentasjon vedrørende personvern er i begrenset grad kommunisert ut i etaten. Det har ikke vært en systematisk opplæring i informasjonssikkerhet generelt, eller i personvern spesielt. Fordi helsesektoren har vært strengt regulert i mange år, vurderes risikoen som begrenset. Opplæring innen informasjonssikkerhet generelt, og personvern spesielt, bør likevel i større grad systematiseres slik at man sikrer at alle får nødvendig informasjon, og at det er en enhetlig tilnærming til kommunikasjon om temaet.

Kommunalsjef helse og omsorg har ansvar for Etatens etterlevelse av personvernkrav. Hun har opprettet et GDPR-utvalg i etaten som ifølge et notat har ansvar for å sørge for at etaten overholder personvernregelverket. Det fremstår som noe uklart hva som er gruppes ansvar for etterlevelse, sett opp mot linjeledelsens ansvar. Det anbefales å tydeliggjøre roller og ansvar for etterlevelse av personvernregelverket i etaten, for å sikre at det er en enhetlig forståelse, og således redusere risikoen for brudd på regelverket.

Helse- og omsorgsetaten har utarbeidet en oversikt over hvilke personopplysninger etaten behandler per fagsystem, og dette er dokumentert i verktøyet Draftit. Etaten har mottatt innsynsbegjæringer, og har i slike tilfeller klart å sammenstille og gjøre tilgjengelig den etterspurte informasjonen. Etaten har imidlertid ikke opplevd en situasjon der et stort antall registrerte ber om innsyn i registrerte personopplysninger samtidig. Det vurderes som sannsynlig at det i en slik situasjon vil bli arbeidskrevende for kommunen å oppfylle forpliktelsen sin til å gi innsyn, fordi det ikke er mulig å automatisere uttrekk av personopplysninger på tvers av ulike systemer.

Etaten har over tid arbeidet med å inngå og kvalitetssikre databehandleravtaler. Det gjenstår imidlertid fortsatt en del arbeid før alle nødvendige, nye avtaler er inngått, og alle gjeldende avtaler er kvalitetssikret og oppdatert.

Etaten gjør løpende risikovurderinger knyttet til personvern der det vurderes som nødvendig, men virker ikke å ha en systematisk tilnærming til gjennomføring og dokumentering av risikovurderinger. Dette gir en risiko for at Etaten ikke blir oppmerksom på viktige risikoer, og som følge av det ikke iverksetter nødvendige risikoreduserende tiltak. Det er således et potensial for å profesjonalisere etatens risikostyring.

Personopplysningsloven artikkel 35 stiller krav til å gjøre personvernkonsekvensvurderinger ved gitte omstendigheter. Representanter for Helse- og omsorgsetaten bekrefter at de er klar over kravet både for pågående og nye behandlinger, men har ikke identifisert behov for å gjennomføre slike vurderinger.

Vår anbefaling er at Helse- og omsorgsetaten prioriterer følgende område:

7. **Opplæring og kommunikasjon i Helse- og omsorgsetaten**
   I Helse- og omsorgsetaten er det, tilsvarende som i kommunen sentralt, et potensial for å systematisere kommunikasjon og opplæring om informasjonssikkerhet og personvern. Dette for å sikre at alle får nødvendig informasjon, og at det er en enhetlig tilnærming til kommunikasjon om temaet. Anbefalingen bør sees i sammenheng med anbefaling 1.

8. **Avklaring av roller og ansvar for etterlevelse av krav i personopplysningsloven i Helse- og omsorgsetaten**
   Det anbefales at roller og ansvar for etterlevelse av personvernregelverket i etaten tydeliggjøres, for å sikre at det er en enhetlig forståelse, og således redusere risikoen for brudd på regelverket. Det er særlig behov for å vurdere ansvarsfordeling mellom linjeledelsen og GDPR-gruppen i Etaten.

9. **Profesjonalisering av Helse- og omsorgsetatens risikostyring**
   Det er et potensial for å profesjonalisere etatens risikostyring. Anbefalingen bør sees i sammenheng med anbefaling 3.

Innhold

1. Innledning

1.1 Bakgrunn og formål

Etter vedtak i kontrollutvalget i Karmøy kommune 28. november 2018, har KPMG gjennomført en forvaltningsrevisjon rettet mot kommunen sin håndtering og behandling av personopplysninger. Denne rapporten er svar på kontrollutvalgets bestilling.

Formålet med forvaltningsrevisjonen har vært å undersøke konkrete tema innen personvernlovgivningen, nærmere bestemt hvordan Karmøy kommune har innrettet seg for å oppfylle kravene i personopplysningsloven. Med personopplysningsloven mener vi her den nye personopplysningsloven som trådte i kraft 20. juli 2018, og som også gjennomfører forordning EU 2016/679 (Personvernforordningen), ofte omtalt som *GDPR*.

Forvaltningsrevisjonen omfatter kommunen sin håndtering og behandling av personopplysninger. Forvaltningsrevisjonen er forbedringsorientert, og har som formål å gi anbefalinger om tiltak der forvaltningsrevisjonen avdekker avvik eller forbedringsområder. Det er imidlertid viktig å bygge videre på god praksis, og forvaltningsrevisjonen vil derfor bestrebe å gi en balansert fremstilling av status, og anerkjenne områder der kommunen har etablert en god praksis.

1.2 Problemstillinger

Forvaltningsrevisjonen gir svar på følgende problemstillinger:

1. Har Karmøy kommune etablert et internkontrollsystem for personvern som tilfredsstiller krav i regelverket?
2. Hvilken rolle og ansvar har personvernombudet i Karmøy kommune?
3. Hvilke rutiner har kommunen for avviksføring knyttet til brudd på personvernregelverket?
4. Er det en klar fordeling mellom roller og ansvar i informasjonssikkerhetsarbeidet i kommunen?
5. I hvilken grad har omsorgssektoren i Karmøy kommune innrettet seg etter det nye personvernregelverket? Herunder:
    a. I hvilken grad har virksomhetene utarbeidet tilstrekkelig internkontroll på området?
    b. Har virksomhetene oversikt over hvilke personopplysninger de behandler?
    c. I hvilken grad er det gjennomført risikovurderinger i virksomhetene?

Nærmere om tilnærming og problemstillinger

I Datatilsynet sine tilsyn overfor kommuner de siste årene er hovedfunnene at norske kommuner mangler oversikt over hvilke personopplysninger kommunen har om innbyggerne, og kommunene har ikke en presis beskrivelse av hva opplysningene brukes til. Videre har norske kommuner generelt

mangelfulle risikovurderinger og mangelfull internkontroll på området. Denne forvaltningsrevisjonen av Karmøy kommune sin innretting etter det nye personvernregelverket har tatt utgangspunkt i Datatilsynets funn i norske kommuner, og nye konkrete krav som følger av den nye personopplysningsloven.

- ✓ Vi har vurdert om Karmøy kommune har tilstrekkelig internkontroll på området. Herunder har vi kartlagt hvilke rutiner kommunen har for behandling av personopplysninger, og om disse er oppdatert i henhold til det nye regelverket. Her har vi også vurdert om kommunen har rutiner for avviksføring, og om det er en tydelig rolle- og ansvarsfordeling når det gjelder å melde eventuelle avvik til Datatilsynet. Vi har også vurdert om det er en tydelig rolle- og ansvarsfordeling generelt i kommunens arbeid for å sikre etterlevelse av personopplysningsloven. Praktisk testing av systemfunksjonalitet har ikke inngått som en del av forvaltningsrevisjonen.

- ✓ En endring i den nye personopplysningsloven er at alle offentlige myndigheter må ha et personvernombud. Her har revisjonen vurdert om Karmøy kommune tilfredsstiller kravet om å ha et personvernombud, samt hvilken rolle og ansvar vedkommende ivaretar i sin ombudsrolle.

- ✓ Som en del av internkontrollen skal kommunen ha en oversikt over hvilke behandlinger av personopplysninger som foretas. Vi har tatt utgangspunkt i omsorgssektoren i Karmøy kommune, og har sett nærmere på om den har oversikt over hvilke personopplysninger den behandler. Omsorgssektoren er valgt fordi den behandler stor grad av personopplysninger generelt, og sensitive personopplysninger spesielt. Alle virksomheter som samler inn eller bruker personopplysninger skal ha oversikt over hvilke personopplysninger de behandler, hvor de kommer fra og hva som er det rettslige grunnlaget for behandlingen. Her har vi undersøkt om virksomhetene innenfor omsorgssektoren har utarbeidet en protokoll over behandlingene i tråd med kravet i personopplysningsloven.

- ✓ Alle kommuner skal gjennomføre en risikovurdering før de iverksetter en ny behandling av personopplysninger, eller tar i bruk et nytt informasjonssystem. Vi har vurdert i hvilken grad kommunen har gjennomført slike risikovurderinger i omsorgssektoren.

1.3 Revisjonskriterier

Revisjonskriterier er de krav og normer som tilstand og/eller praksis i kommunen vurderes opp mot. Revisjonskriterier må være aktuelle, relevante og gyldige for kommunen. Kilder for å utlede revisjonskriterier har vært:

- ✓ Kommunesektorens organisasjon (KS) 2013: Rådmannens internkontroll
- ✓ Lov om behandling av personopplysninger (personopplysningsloven)
- ✓ Datatilsynets veileder om internkontroll og informasjonssikkerhet
- ✓ Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Det er gjort nærmere rede for revisjonskriteriene i vedlegg 2.

1.4 Metode

Forvaltningsrevisjonen er gjennomført i samsvar med kravene i RSK001 Standard for forvaltningsrevisjon[1].

For å svare på problemstillingene i undersøkelsen har vi samlet inn data ved bruk av følgende teknikker:

- ✓ Dokumentgjennomgang og analyse
- ✓ Intervjuer

Det har blitt samlet inn dokumentasjon fra kommunen som har blitt gjennomgått og analysert opp mot revisjonskriteriene; herunder rutinebeskrivelser og øvrig styrende dokumentasjon, risikovurderinger, behandlingsprotokoller, funksjonsbeskrivelser og databehandleravtaler. I tillegg har vi vurdert kommunens personvernerklæring som er tilgjengelig på kommunens internettsider.

Vi har også gjennomført intervjuer med et utvalg ansatte i kommunen, samt med personvernombudet som er innleid fra Haugesund kommune. Vi har intervjuet kvalitetsrådgiver og IKT-sjef i kommunens sentraladministrasjon. I Helse- og omsorgsetaten har vi intervjuet kommunalsjef helse og omsorg, omsorgssjef, avdelingssjef for forvaltning, jurist og IT-medarbeider i forvaltningsenheten, virksomhetsleder for hjemmetjeneste midt, samt en sykepleier i hjemmetjeneste midt.

Hvilke personer som skulle intervjues ble avtalt med administrasjonen i kommunen. I forkant av intervjuene ble det utarbeidet intervjuguider, for å sikre en enhetlig tilnærming og at aktuelle tema ble belyst. Fra hvert intervju ble det skrevet referat som ble sendt til den enkelte respondent for verifisering.

Data fra respondentene ble sammenstilt med analysert dokumentasjon, og dette ble samlet vurdert opp imot revisjonskriteriene, og oppsummert i denne rapporten.

I faktadelene av rapporten oppsummeres relevante deler av Karmøy kommune sin styrende dokumentasjon, kombinert med relevant informasjon fra intervjuene. Informasjon som er gjengitt direkte fra styrende dokumenter i Karmøy kommune er uthevet med kursiv skrift.

Datainnsamlingen ble avsluttet 9. mai 2019.

Rapporten ble sendt rådmannen for uttalelse den 5. august 2019, med høringsfrist 25. august 2019.

[1] Utgitt av Norges Kommunerevisorforbund.

2. Internkontrollsystemet for personvern

2.1 Revisjonskriterier

I kapittel to besvarer vi problemstilling 1:

Har Karmøy kommune etablert et internkontrollsystem for personvern som tilfredsstiller krav i regelverket?

Revisjonskriteriene er nærmere gjort rede for i vedlegg 2.

2.2 Fakta

Flere forteller at de opplever at kommunen har jobbet godt med personvernområdet siste året, at det er en bevissthet rundt sikring av personvernet, og at kommunen begynner å få på plass grunnleggende, viktige ting som styrende dokumenter, krav og rutiner på området. Styrende dokumentasjon knyttet til personvern som gjelder hele kommunen utarbeides sentralt ved kvalitetsrådgiver, og det er en gjennomgående oppfatning blant intervjuobjektene at kommunen har kommet langt i dette arbeidet. Dette underbygges også av oversendt dokumentasjon. Personvern har vært adressert flere ganger i rådmannens ledergruppe og i ledergrupper i Helse- og omsorgsetaten, og det har blant annet vært fokus på å etablere protokoll over behandlingsaktiviteter og å inngå databehandleravtaler iht. lovkrav.

De fleste legger likevel til grunn at kommunen fortsatt har en vei å gå, før den fullt ut etterlever kravene i personopplysningsloven, inklusive det å kommunisere ut informasjon om nye krav, rutiner o.l. i hele organisasjonen. Det at kommunen holder på å gå over til et nytt ledelsessystem (også kalt forbedringssystem), bidrar ifølge flere til at ikke alt har falt på plass enda.

2.2.1 Prosedyre for protokoll over behandlinger

Karmøy kommune har etablert en prosedyre for *Protokoll over behandlinger*. Formålet er å *sikre at det føres protokoll over alle behandlinger av personopplysninger*.

Det skal føres en protokoll over behandlingsaktivitetene som utføres i den enkelte enhet, ved bruk av kartleggingsverktøyet Draftit. *Hensikten er å kartlegge hva slags personopplysninger som behandles, om vi har tilstrekkelig grunnlag for å behandle personopplysningene og hvordan vi behandler personopplysningene i dag. Videre skal det kontrolleres om vi har underleverandører eller samarbeidspartnere som behandler disse personopplysningene og om vi har gyldige databehandleravtaler med disse.*

I følge flere intervjuobjekt, er kommunen godt i gang med dette arbeidet. Det ble gjort en risikobasert tilnærming til arbeidet, der de systemene som ble vurdert til å ha størst risiko, i praksis størst omfang av personopplysninger, ble kartlagt først. Dokumentasjonen sammenstilles og lagres i systemet Draftit. Flere fortalte at det gjenstår å føre protokoll over behandlingsaktiviteter i enkelte systemer, men også at arbeidet skal være fullført for Helse- og omsorgsetaten.

Eksempelvis fremgår det av Draftit for systemet Profil, at formålet med behandlingen er å: *Yte helse- og omsorgstjenester; Saksbehandle søknader om helse- og omsorgstjenester; Lavterskeltilbud; Videre henvisning til spesialisthelsetjenesten; Kommunikasjons mellom 1. og 2. linjetjenesten herunder internt, mot fastleger, andre kommuner, helseforetak og private (støttekontakt, private*

bedrifter som yter helse- og omsorgstjenester (f.eks. transport)) og ideelle organisasjoner; Rapportere til statlige organ.

Når det gjelder hvilke type sensitive opplysninger som behandles, nevnes følgende: *Rase eller etnisk opprinnelse; Religiøs/filosofisk overbevisning; Helseforhold; seksuelle forhold*.

Som behandlingsgrunnlag nevnes: *Avtale; Samtykke; Myndighetsutøvelse; Spesiallovgivning; Rettslig forpliktelse; Samfunnssikkerhet; Beskytte registrertes vitale interesser.*

Det fremgår ikke til hvilke formål de ulike personopplysningene behandles, eller hva som er behandlingsgrunnlaget for den enkelte behandling.

2.2.2 Personvernerklæring

På kommunens hjemmeside ligger det en personvernerklæring som gir informasjon om kommunens innsamling og bruk av personopplysninger. Erklæringen inneholder blant annet henvisninger til personopplysningsloven, og kontaktinformasjon til kommunen og kommunens personvernombud.

Personvernerklæringen viser til *Lov om behandling av personopplysninger av 20.07.2018*, og det fremgår at den sist ble oppdatert 31.01.19. Det fremgår ikke hvordan det informeres til de registrerte om endringer / oppdateringer av personvernerklæringen.

Når det gjelder formålet med behandling av personopplysninger, fremgår følgende av personvernerklæringen: *Karmøy kommune behandler personopplysninger for å kunne yte tjenester til innbyggerne i kommunen. Karmøy kommune innhenter bare opplysninger som er nødvendige for å kunne yte tjenester til innbyggerne. Opplysningene som samles inn, behandles i henhold til de regler og forskrifter som gjelder for de aktuelle tjenestene*. Det fremgår ikke av noen punkter hva som menes med *nødvendige for å kunne yte tjenester*.

Når det gjelder sletting av personopplysninger, fremgår det at den registrerte kan be om at personopplysninger blir rettet eller slettet dersom de er uriktige, samt at *Personopplysninger vil bli slettet når formålet med behandlingen er oppfylt, med mindre annet lovverk sier at de skal oppbevares.* Retten til å protestere på behandlinger av personopplysninger fremgår av avsnitt 5.5. i personvernerklæringen.

2.2.3 Reglement for informasjonssikkerhet og personvern

Karmøy kommune har etablert et *Reglement Informasjonssikkerhet og personvern. Formålet med reglementet er å sikre tilstrekkelig styring og kontroll (internkontroll) innen informasjonssikkerhets- og personvernområdet.* Reglementet poengterer at informasjonsbehandling skal være lovlig og pålitelig.

Reglementet viser til at GDPR setter krav til vern av fysiske personer ved behandling av personopplysninger, inneholder regler for fri utveksling av personopplysninger m.v.

Reglementet fastsetter at Karmøy kommune er behandlingsansvarlig for personopplysninger, *og har ansvar for å etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av overnevnte lover*.

Når det gjelder roller og ansvar, fastslår reglementet at *ansvar og myndighet (…) skal følge det ordinære linjeansvaret. Ledere (virksomhetsledere) som har ansvar for mål, arbeidsoppgaver og tjenester skal også ha ansvaret for tilhørende informasjonsbehandling (herunder også behandling av personopplysninger), IKT-system og informasjonssikkerhet.* Av intervju fremgår det at roller og ansvar oppleves å være relativt tydelig avklart både internt i helse- og omsorgsetaten, mellom etaten og kommunens sentraladministrasjon, samt mellom kommunen og personvernombudet som er innleid fra Haugesund kommune. Et område som ikke oppleves å være like tydelig, er avklaring av roller og ansvar knyttet til informasjonssikkerhet generelt, jf. kapittel 5 for mer om dette.

Reglementet viser til at arbeidet med informasjonssikkerhet skal baseres på *Difis veileder «Internkontroll i praksis – informasjonssikkerhet» og Normen (Norm for informasjonssikkerhet, helse og omsorgstjenesten)*.

Sentrale begreper relatert til personvern som informasjonssikkerhet, personopplysninger, sensitive personopplysninger, behandlingsansvarlig m.v. defineres i reglementet. Det var gjennomgående en god kjennskap til betydningen av disse begrepene blant intervjukandidatene.

Det fremgår at *Informasjonssikkerhets- og personvernstrategien skal ligge til grunn for all behandling av informasjon og personopplysninger i kommunen*, og at oppfølging skal skje gjennom kommunens fremtidige ledelsessystem. I følge kvalitetsrådgiver holder kommunen på å implementere et nytt ledelsessystem. Deler av funksjonaliteten i systemet er tatt i bruk, derunder rapportering av avvik og forbedringsforslag, men det gjenstår en god del arbeid før implementeringen av systemet er fullført:

> *Gjennom forankring, forpliktelse og forståelse vil Karmøy kommune oppnå effektiv sikkerhetsstyring. Kommunen har følgende prioriteringer for å oppnå dette:*
> - *Etablering av et helhetlig styringssystem*
> - *Tydelig ledelsesforankring og styrking av sikkerhetskulturen (bevisstgjøring)*

Reglementet presiserer hva kommunen mener med begrepene tilgjengelighet, integritet og konfidensialitet knyttet til personopplysninger. Videre viser det til at internkontroll bidrar til å redusere risiko for uønskede hendelser på personvernområdet, og mulige konsekvenser (for kommunen) av slike hendelser. Reglementet stiller krav til at kommunen skal ha oversikt over behandlinger av personopplysninger som foretas, og at den skal brukes som underlag ved risikovurderinger:

> *Det er ikke tillatt å behandle personopplysninger uten at det er definert et formål med behandlingen (…) Kort oppsummert kreves det at*
> - *Den registrerte har gitt samtykke til behandlingen*
> - *Behandlingen er nødvendig for å oppfylle en avtale*
> - *Behandlingen er hjemlet i lov*

Det fremgår også at den enkelte etat / virksomhet må *identifisere plikter og tilpasse internkontroll og informasjonssikkerhetstiltak til sin organisasjon*.

Det stilles krav til at kommunen må etablere personvernerklæringer, og at det skal gis *nødvendig informasjon for å sikre en rettferdig og gjennomsiktig behandling*.

Når det gjelder risikovurderinger, presiserer reglementet at det må utarbeides en oversikt over hvilke personopplysninger kommunen behandler, og at det må utarbeides en risikoanalyse basert på den. Dette skal igjen danne grunnlaget for iverksettelse av nødvendige risikoreduserende tiltak, og *inngår i underlag for ledelsens gjennomgang av styringssystemet.* Reglementet viser videre til kommunens *prosedyre for risikohåndtering for mer informasjon*, og sier følgende om kommunens risikoaksept: *For å kunne fastsette hva akseptabelt risikonivå er, skal behov for konfidensialitet, tilgjengelighet og integritet vurderes. I noen situasjoner kan disse tre komme i konflikt med hverandre (…) Det er viktig at kryssende hensyn identifiseres, og at prioritering mellom forskjellige behov fremgår i beskrivelsen av akseptabelt risikonivå.*

Reglementet fastslår videre at *gjennomførte vurderinger og tiltak skal dokumenteres,* samt hvem denne dokumentasjonen skal være tilgjengelig for. Det vises til *Arkivplanen* for oversikt over elektroniske systemer som behandler data.

I følge flere av intervjukandidatene, gjøres det risikovurderinger i kommunen generelt, og i Helse- og omsorgsetaten spesielt. Slike vurderinger dokumenteres imidlertid i begrenset grad. Manglende dokumentasjon understøttes av tilsendt dokumentasjon som ikke inneholder noen risikovurderinger,

samt av dokumentasjon i systemet Draftit, der kolonnen "Risiko" står tom for de ulike programmene som er kartlagt.

Reglementet presiserer behovet for å etablere og forankre en betryggende internkontroll, og viser til ledelsens årlige gjennomgang av *mål, strategi og organisering av styringssystemet.* Videre presiseres det at brukere av IKT-systemer må få nødvendig opplæring i riktig bruk, krav til internkontroll og informasjonssikkerhet, sikkerhetstiltak m.v.

Når det gjelder opplæring innen personvern (som inngår som en del av kommunens informasjonssikkerhet), har kommunens sentraladministrasjon tatt initiativ til at alle ansatte skal gjennomføre e-læringskurs innenfor personvern per epost. Kurset ble distribuert som 15 korte moduler innen ulike personvernrelaterte tema, inklusive en GDPR-quiz. Alle intervjuobjektene bekreftet at de hadde gjennomført disse kursene, og flere la til grunn at de hadde vært nyttige og bidratt til at de hadde reflektert rundt viktige problemstillinger. Alle kommunens medarbeidere har imidlertid ikke gjennomført kursene. I følge flere intervjuobjekter, er det en betydelig andel medarbeidere som ikke har aktivert epost-kontoen sin, eller som bare i begrenset grad forholder seg til epost. I følge statistikk tilsendt fra kommunen, varierte andelen som startet på de ulike leksjonene fra 17% til 39%, med størst oppslutning på de innledende leksjonene. Det var også en andel som ikke fullførte kursene de startet på. På noen ledersamlinger har slike e-læringskurs også blitt gjennomgått, for å nå ut til flere av kommunens ansatte.

Kommunikasjon og opplæring er et lederansvar i kommunen, og personvernrelaterte tema adresseres ifølge intervjuobjektene på ledersamlinger, med en forventning om at lederne skal ta informasjonen videre i sine ledergrupper. Av intervju fremgikk det at dette i varierende grad var blitt gjort innen personvern. Det fremgikk blant annet at det høsten 2018 hadde blitt informert på ledermøter sentralt i kommunen, samt i Helse- og omsorgsetaten, om at kommunen hadde fått et nytt personvernombud. Flere fortalte at denne informasjonen ikke var presentert for operative ledere og medarbeidere ute i Helse- og omsorgsetaten.

2.2.4 Retting og sletting av personopplysninger

Karmøy kommune har en prosedyre for *Retting og sletting av personopplysninger*, som har til formål å sikre at kommunen utøver *de registrertes rettigheter ved henvendelse om retting og sletting av personopplysninger i henhold til personopplysningsloven*. Av prosedyren fremgår det at kommunen ikke skal *behandle opplysninger som er uriktige, ufullstendige eller som det ikke er lov til å behandle*, og at den ikke skal lagre opplysninger lenger enn nødvendig ihht. Personopplysningsloven eller annen lovgivning.

Opplysninger som er feil skal slettes, er de ufullstendige skal de rettes, og ved sletting skal nye korrekte opplysninger legges til. *Dersom uriktige eller ufullstendige opplysninger kan ha betydning som dokumentasjon, skal opplysninger om rettinger/slettinger gjøres ved at de uriktige/ufullstendige opplysningene blir markert, og riktige/fullstendige opplysninger tilført*. *Dersom vedkommende opplysningen gjelder ønsker å slette opplysningene helt, eller at de blir sperret, kan en avgjørelse om retting/tilføyelse klages inn for Datatilsynet.* De fleste som ble intervjuet kjente til at rutinen fantes, og hadde også et forhold til innholdet i rutinen.

2.2.5 Prosedyre for kontroll og revisjon av databehandlere

Karmøy kommune har etablert en prosedyre for *Kontroll og revisjon av* databehandlere. *Forholdet mellom Karmøy kommune (KK) og databehandleren skal være regulert i en databehandleravtale.* Prosedyren regulerer videre krav til innhold i en slik avtale.

I følge prosedyren har KK som behandlingsansvarlig en *plikt til å undersøke om databehandleren er kompetent til å behandle de aktuelle personopplysningene i tråd med pliktene som følger av*

personvernlovgivningen. *Den behandlingsansvarlige skal ta hensyn til databehandleroppdragets karakter og omfang, samt hvilken risiko behandlingen kan få for de registrerte det gjelder*.

Kommunen forplikter seg til å ivareta sine lovpålagte oppgaver/plikter når behandling av personopplysninger settes ut til en ekstern tjenesteleverandør. Vi kan bare benytte databehandlere og underleverandører som kan dokumentere tilstrekkelige garantier for at kravene i personopplysningloven blir ivaretatt, samt at personopplysningene som behandles er tilstrekkelig sikret. Dette betyr blant annet at databehandleren må kunne vise at man har gode nok tekniske og organisatoriske tiltak som sikrer at loven følges i praksis.

Prosedyren inneholder videre en rekke krav til hva den enkelte databehandleravtale skal inneholde. Den poengterer at hvor detaljert avtalen skal beskrives, avhenger av hvor kompleks behandlingen er.

Det fremgår blant annet at det tydelig skal defineres hva *KK sine personopplysninger kan brukes til,* og at databehandleren trenger tillatelse til det dersom opplysningene skal benyttes til annet enn det som opprinnelig var avtalt. Under følger utdrag av annen informasjon slike avtaler skal omfatte.

D*atabehandleravtalen skal beskrive pliktene og rettighetene til Karmøy kommune*, og må bla. regulere at kommunen er behandlingsansvarlig, at den skal bestemme formål for behandlingen, at den skal gi databehandler dokumenterte instrukser om hvordan personopplysningene skal behandles, at kommunen kan si opp avtalen ved lovbrudd, og at avtalen skal regulere databehandlerens plikter.

Prosedyren påpeker behovet for en betryggende tilgangsstyring til personopplysningene som behandles. Prosedyren pålegger Helse- og omsorgsetaten å sikre at det kommer inn i databehandleravtalene at databehandler må autorisere alle som skal ha tilgang. Det stilles også krav om tiltak for å unngå at personer som ikke har et tjenstlig behov for opplysningene får tilgang.

Prosedyren spesifiserer at databehandler må ha tilfredsstillende sikkerhetstiltak:

> *Databehandleren forplikter seg til å iverksette alle nødvendige organisatoriske og tekniske tiltak for å unngå at personopplysninger som kommunen er ansvarlig for utsettes for uautorisert tilgang, spredning, endring, skade, ødeleggelse eller utilgjengelighet (informasjonssikkerhet). Kravet er at informasjonssikkerheten hos leverandøren skal være tilfredsstillende. Tiltak for a oppnå tilfredsstillende informasjonssikkerhet kan blant annet omfatte pseudonymisering eller kryptering av personopplysninger*.

Det fremgår videre at databehandleren skal bistå kommunen i risikovurderinger av tjenester eller teknologier som *representerer en særlig høy risiko for personvernet*, og også ved dialog med Datatilsynet i tilfeller der *personvernrisikoen (avdekket gjennom konsekvensutredningen) vanskelig lar seg håndtere på en hensiktsmessig måte*.

Prosedyren stiller videre særlige krav dersom databehandleren ønsker å bruke en underleverandør for å oppfylle forpliktelsene som følger av avtalen. Blant annet stilles det krav om at kommunen må godkjenne slike underleverandører.

Det fremgår at det er kommunen som plikter å legge til rette slik at den registrerte får oppfylt sine rettigheter, mens databehandler skal hjelpe kommunen å oppfylle denne plikten. Det følger også at avtalen må regulere at databehandleren plikter å bistå kommunen for å kunne oppfylle sine plikter ihht. *Artikkel 32-36: Sikkerhet ved behandlingen, melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten, underretning av den registrerte om brudd på personopplysningssikkerheten, vurdering av personvernkonsekvenser og forhåndsdrøftinger*.

Databehandleravtalen må inneholde krav om at *Databehandleren må gjøre tilgjengelig all informasjon som er nødvendig for å påvise at forpliktelsene er oppfylt, for KK*, og om at *Databehandleren må muliggjøre og bidra til revisjoner (slik som inspeksjoner) som gjennomføres av kommunen eller en annen inspektør, på fullmakt fra KK*.

Prosedyren presiserer at databehandleren skal varsle behandlingsansvarlig dersom *personopplysninger som KK er ansvarlig for utsettes for sikkerhetsbrudd (uautorisert tilgang,*

spredning, endring, skade, ødeleggelse eller utilgjengelighet). Sikkerhetsbrudd skal dokumenteres, og varsling skje så snart som mulig på en slik måte at kommunen er i stand til å oppfylle sine forpliktelser.

2.2.6 Tekniske tilpasninger og sikkerhet

Kommunen har startet et arbeid for å ta i bruk MinID for å sikre at det er rett person som ber om innsyn ved innsynsforespørsler. Ved slike forespørsler om innsyn i hvilke personopplysninger som er lagret om en person, må opplysningene hentes ut manuelt fra hvert enkelt system og sammenstilles.

Det er ifølge IKT-sjef gjort tilpasninger for å innfri kravet om innebygget personvern der det er mulig gjennom å begrense tilganger så langt det lar seg praktisk gjøre. Ved anskaffelse av nye IT-systemer har kommunen fokus på at personopplysninger skal beskyttes, og at systemene skal ha innebygget personvern slik at brukerne ikke får tilgang til flere personopplysninger enn de har tjenstlig behov for. Flere forteller at det er et høyt fokus på tilgangsstyring, særlig i Helse- og omsorgsetaten, men også at det er en problemstilling at en del medarbeidere har bredere tilganger enn deres tjenstlige behov.

I følge IKT-sjef tester kommunen konfigurasjoner på det som går fra kommunen til leverandør, og ber om revisjonsbevis på at kravene i databehandleravtaler etterleves. Det er ikke gjennomført revisjon eller test av hvordan databehandler i praksis følger opp kravene i databehandleravtaler, men det vurderes som aktuelt i fremtiden.

2.2.7 Prosedyre for informasjon til den registrerte

Karmøy kommune har etablert en Prosedyre for *Informasjon til den registrerte,* som regulerer kommunens plikter på dette området. Av prosedyren fremgår det at kommunen alltid er behandlingsansvarlig for personopplysninger som kommunen selv samler inn og håndterer, og at kommunen har en plikt til å gi informasjon til de registrerte, både på eget initiativ og på forespørsel. Videre fremgår det at:

> *Alle har rett til informasjon om hvilke personopplysninger som er registrert om dem, hvorfor opplysningene er registrert og hva de brukes til*.
>
> *Ved innsamling av personopplysninger skal KK på eget initiativ informere den som registreres om:*
>
> - *Navn og adresse på den behandlingsansvarlige, og eventuelt dennes representant*
> - *Formålet med behandlingen*
> - *Om opplysningene vil bli utlevert, og eventuelt til hvem*
> - *At det er frivillig å gi fra seg opplysningene*
> - *Annet som hjelper den registrerte til å bruke sine rettigheter etter loven her på best mulig måte, f.eks. informasjon om retten til å kreve innsyn og retten til å kreve retting.*

Den registrerte skal også informeres når opplysninger samles inn fra andre enn den registrerte selv, men ikke dersom *behandlingen er fastsatt i lov, varsling er urimelig vanskelig eller den behandlingsansvarlige er sikker på at du allerede kjenner informasjonen*. Samtykkeerklæringer skal være tilgjengelig på kommunens internettsider og i det administrative systemet Compilo, og det skal være henvist til den i e-læringskurset innen personvern. Helse- og omsorgsetaten har egne samtykkeskjemaer, der bruker signerer på samtykke til bruk av personopplysninger. Dersom en person motsetter seg at helse- og omsorgsetaten skal kunne bruke personopplysninger om vedkommende, forteller flere intervjuobjekt at kommunen kan se bort fra det dersom det er nødvendig for å sikre liv og helse.

Det fremgår videre at forespørsler om innsyn skal være skriftlige og sendes lokal behandlingsansvarlig, alternativt til personvernombudet. *KK skal på eget initiativ rette eller slette personopplysninger som er uriktige, ufullstendige, som det ikke er adgang til å behandle, eller når opplysningene ikke lenger er nødvendige for formålet med behandlingen. Den registrerte kan også*

kreve manuell behandling i stedet for automatiserte avgjørelser der hvor det utføres. Det samme gjelder etter begjæring fra den registrerte.

2.2.8 Reglement - internkontroll og kontinuerlig forbedring

Karmøy kommune har et *Reglement – internkontroll og kontinuerlig forbedring,* som har til formål å forbedre *internkontroll og kvalitet gjennom utvikling av effektive arbeidsprosesser og riktige tjenestetilbud,* og legge til rette for *læring i organisasjonen gjennom erfaringsutveksling, refleksjon, læring og kompetanseutvikling på tvers av enheter og etater.*

Forbedringsarbeidet baserer seg på modellen Deming-sirkel som inneholder elementene planlegge, utføre, vurdere og iverksette. Den enkelte leder har ansvar for at det gjennomføres en årlig gjennomgang av internkontrollen på sitt ansvarsområde og i grensesnitt mot andre enheter, og basert på det identifisere forbedringsområder.

Alle ledere som har internkontrollansvar, skal i samarbeid med medarbeiderne utvikle og vedlikeholde en forbedringsplan – eller del av en helhetlig forbedringsplan - som gir et bilde av det systematiske arbeidet med forbedringsområdene. Planen skal angi mål, tiltak, ansvar, fremdrift/status – og ha høy oppmerksomhet tilknyttet implementering, oppfølging og evaluering av tiltak. Karmøy kommune benytter et årshjul for oppfølging av internkontroll og kontinuerlig forbedring.

Vi har ikke fått forelagt en helhetlig plan over hvilke tiltak som gjenstår og plan for å lukke disse tiltakene på personvernområdet, verken per leder eller på overordnet nivå. Ved spørsmål om dette i intervju, peker flere på at nødvendig informasjon er sammenstilt i systemet Draftit, som benyttes for kartlegge behandlinger av personopplysninger i ulike systemer. I Draftit opplyses det innledningsvis om risikoen i det enkelte systemet er vurdert som lav, middels eller høy. Kolonnen kalt risiko i selve beskrivelsen av systemet er tom for alle systemene som er kartlagt. Systemet inneholder også et punkt kalt videre behov, der det er oppført hvilke punkter som må sjekkes nærmere opp. Det er ikke oppført ansvarlig for gjennomføring eller frist for de tiltakene som er listet opp som oppfølgingspunkter.

Kommunen etablerte i 2016 et system for *intern revisjon av internkontroll/kvalitet*. Internrevisjonene gjennomføres med interne ressurser i kommunen, og rådmannen beslutter revisjonsprogram, revisjonskriterier med videre. Når det gjelder rapportering, viser prosedyren til kommunens *fremtidige styrings- og rapporteringssystem*.

2.2.9 Prinsipper for internkontroll og forbedringsarbeid

Kommunen har et dokument kalt *Hensikt, prinsipper og praktiske retningslinjer.* Dokumentet vektlegger *kompetente, engasjerte, ansvarsbevisste og deltagende medarbeiderne* som kommunens viktigste ressurs for å utvikle en velfungerende internkontroll.

Vi forutsetter at gjeldende lover og regler etterleves, politiske vedtak følges opp og brukernes behov og forventninger oppfylles etter beste evne innen gitte rammer. Vårt arbeid med å styrke internkontrollen skal baseres på fastsatte og omforente mål som er målbare og kan etterprøves. Risikoanalyser og erfaringer fra avvikshåndtering skal danne grunnlaget for utforming og gjennomføring av tiltak. Gjennom oppfølging, overvåking og målinger skal vi følge opp etterlevelsen og effekten av iverksatte tiltak - og om nødvendig foreta løpende justeringer/vedlikehold. Melding og håndtering av avvik trekkes frem som viktig for å legge til rette for organisatorisk læring og forbedring. *Aktiviteter og resultater i arbeidet med internkontroll skal styres og synliggjøres gjennom bruk av årshjul og systematisk rapportering,* og inngå som en *integrert del av kommunens rapporteringssystem*.

God og helhetlig informasjonsflyt i internkontrollarbeidet vektlegges. Forbedringsarbeidet skal bidra til å *redusere kritiske risikoer og faren for uønskede hendelser, samt bedre kvaliteten på tjenestene og øke brukertilfredsheten*. Flere ledere uttrykte at det er et forbedringspotensial i kommunen når det gjelder å sikre at viktig informasjon når ut i hele organisasjonen, og at det i forbindelse med implementering av et nytt forbedringssystem pågår drøftelser om hvordan dette kan gjøres mer effektivt.

2.2.10 Prosedyre for risikohåndtering

Karmøy kommune har en prosedyre kalt *Prosedyre – risikohåndtering.* Av denne fremgår det at:

> *Risikohåndtering fungerer best når den gjennomføres med de som utfører oppgaven/er deltager i prosessene. Det blir derfor viktig med bred medarbeiderdeltagelse. Sentrale roller i dette arbeidet er prosessleder (…) og referent. Leder må også vurdere om det er behov for å utpeke en medarbeider som skal bistå leder i internkontrollarbeidet (…) Vedkommende kan ha oppgaver/ansvar under kartleggingsarbeidet (…) og i forbindelse med utarbeidelse av tiltak og implementering (…) av disse.*
>
> *Ved vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal prosedyre «Vurdering om behov for DPIA» følges.*
>
> *Risikohåndtering forutsetter at de sentrale prosessene innen enheten og i grensesnittet til andre enheter er identifiserte, og at en har prioritert og beskrevet de prosessene som er mest kritiske og risikoutsatte. Risikohåndtering tar utgangspunkt i beskrivelsen av en slik prosess.*

Hoveddelen av prosedyren handler om risikohåndtering. Her fremgår det at følgende aktiviteter skal gjennomføres:

- Risikokartlegging – "Hva kan gå galt?"
- Risikovurdering – "Hvor galt kan det gå?"
- Vurdere potensielle årsaker – "Hvorfor kan det gå galt?"
- Vurdere behovet for tiltak – "Hva er gjort – er det nok?"
- Etablere systematisk oppfølging – og kontinuerlig forbedring
- Registreringer / dokumentasjon

I tillegg følger en utdypning av hvordan de ulike aktivitetene skal gjennomføres, samt hvilken funksjon som har ansvar for gjennomføring av de ulike aktivitetene.

Intervjuobjektene forteller gjennomgående at det gjøres risikovurderinger både i kommunens sentraladministrasjon, og i Helse- og omsorgsetaten. Flere forteller at kommunen har et forbedringspotensial når det gjelder å gjøre systematisk risikovurderinger og dokumentere disse i en helhet, inklusive tiltak som skal følges opp, derunder ansvar og frist for gjennomføring. Ledelsen skal ha drøftet akseptkriterier for personvernrisiko, men ikke konkludert.

2.2.11 Prosedyre for vurdering av DPIA

Karmøy kommune har etablert en prosedyre for *Vurdering om behov for DPIA.* DPIA står for Data Protection Impact Assessment og er en vurdering av personvernkonsekvenser, som ifølge Datatilsynet skal sikre at personvernet til de som er registrert i løsningen ivaretas[2]. DPIA skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter, ved å vurdere dem og fastlegge risikoreduserende tiltak. Formålet med prosedyren er å *avklare om det er behov for å gjennomføre en utredning av personvernkonsekvenser (DPIA).* Videre:

> *Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og i det 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 vernet av personopplysninger.*

Prosedyren inneholder videre en opplisting av kriterier for når DPIA kan bli et krav, og spørsmål som må vurderes ved vurdering av om det er nødvendig å gjøre en DPIA. Prosedyren viser til *Prosedyre*

[2] Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og i det det tas hensyn til behandlingens art, omfang, format og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, så skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet.

for gjennomføring av DPIA. Kvalitetsrådgiver har opplyst at det ikke finnes en prosedyre for gjennomføring av DPIA, at DPIA skal gjennomføres i systemet DraftIt, og at det er utarbeidet et eksempel for hvordan en slik konsekvensvurdering kan se ut. Vi er ikke kjent med at det er utført DPIA sentralt i kommunen eller i Helse- og omsorgsetaten. DPIA trekkes frem som et område kommunen vil ha økt fokus på i tiden fremover.

2.3 Vurdering

Karmøy kommune har det siste året arbeidet målrettet for å etterleve krav i personopplysningsloven. Det er utarbeidet styrende dokumentasjon, rutiner og prosedyrer og de ansatte har blitt bedt om å gjennomføre et e-læringskurs innen personvern. Kvalitetsrådgiver har bygget kompetanse på personvernområdet, og har bidratt i intern opplæring av ledere i kommunen. Hun har også vært en pådriver for å legge til rette for, og gjennomføre kartlegging av behandlinger av personopplysninger i kommunen.

Det er relativt kort tid siden en rekke nye krav ble implementert i Personopplysningsloven. Kommunen arbeider for å etterleve nye krav, samtidig som det er områder hvor det gjenstår arbeid. Dette omtales nedenfor.

2.3.1 Kommunikasjon og opplæring

Kommunikasjon og opplæring er et lederansvar i kommunen. Personvernrelaterte tema har blitt adressert på ledersamlinger, hvor det også har blitt gitt litt grunnleggende opplæring i intern regi, og det har vært mye snakk om personvern i kommunikasjonen i forbindelse med at den nye personopplysningsloven trådte i kraft i juli 2018. Det er en forventning til at ledere i kommunen skal bringe informasjon de mottar i ledergrupper videre i sine respektive ledergrupper, som igjen skal bringe den videre ut i organisasjonen. Dette gir en sårbarhet ved at kommunen blir avhengig av at mange lag med ledere har tilstrekkelig forståelse for informasjonen de får presentert til at de klarer å videreformidle den tydelig ut i virksomheten, og at de husker og prioriterer å bringe den videre. Informasjon ut i organisasjonen om kommunens personvernombud illustrerer denne problemstillingen. Enhetslederen i hjemmetjenesten som ble intervjuet fortalte at han hadde fått informasjon om personvernombudet på en ledersamling, men at han ikke hadde informert de tre avdelingslederne han hadde ansvar for, og følgelig heller ikke hadde bedt dem informere videre ut til de mer enn hundre medarbeiderne som var ansatt i deres enheter.

Medarbeidere kan også aktivt oppsøke styrende dokumentasjon på intranett, i kommunens ledelsessystem m.v. Det at kommunen holder på å implementere et nytt ledelsessystem, har bidratt til å øke utfordringen med å implementere og kommunisere nye eller endrede prosesser, rutiner og krav ut til hele organisasjonen. Det er imidlertid positivt at ledelsen er bevisst på denne utfordringen, og drøfter hvordan kommunen mer effektivt kan legge til rette for at viktig informasjon når ut til hele organisasjonen.

Alle ansatte i kommunen skal gjennomføre et e-læringskurs i personvern som er distribuert på epost. Mange ansatte har imidlertid enten ikke aktivert epostkontoen sin, eller bruker den i begrenset omfang. Blant annet har Helse- og omsorgsetaten mange medarbeidere i felt som trolig i begrenset grad forholder seg til administrative systemer og epost som informasjonskanal. Statistikk viser at under en tredjedel av de ansatte i snitt har gjennomført de ulike leksjonene i e-læringskurset, hvilket bidrar til redusert effektivitet av opplæringen. Slike kurs har blitt gjennomgått i noen ledergrupper, hvilket trolig har bidratt til å nå ut med informasjonen til noen flere ansatte.

2.3.2 Protokoll over behandlinger

Karmøy kommune har etablert en prosedyre for *Protokoll over behandlinger*, med formål om å *sikre at det føres protokoll over alle behandlinger av personopplysninger*.

Artikkel 30 i Personopplysningsloven stiller krav til at hver behandlingsansvarlig skal føre en protokoll over behandlingsaktiviteter. Protokollen skal blant annet inneholde *formålene med behandlingene.* I følge artikkel 5 (*prinsipper for behandling av personopplysninger)*, skal personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenelig med disse formålene (…). Datatilsynet sier videre at: *Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist. Alle formål skal være forklart på en måte som gjør at alle berørte har samme forståelse av hva personopplysningene skal brukes til (...).*

Vi har ikke grunnlag for å vurdere hvorvidt protokollen over behandlinger inneholder informasjon om alle systemer som behandler personopplysninger i Karmøy kommune. Det er positivt at kommunen har en risikobasert tilnærming, og har startet med å kartlegge de behandlingene som innebærer den største risikoen først.

Kommunen har organisert protokollen basert på ulike system, og ikke per behandling som kommunen utfører. Hvilket formål som gjelder for behandlinger i systemet er samlet i "en sekkepost". Tilsvarende er gjort for andre parametere, derunder for behandlingsgrunnlaget. Dette bidrar til at det ikke fremgår tydelig hva som er behandlingsgrunnlaget for, eller formålet med, den enkelte behandlingsaktivitet.

Vår vurdering er at kommunens protokoll er mangelfull ifht. kravene i Personopplysningsloven artikkel 30, fordi formålet med, og behandlingsgrunnlaget for, den enkelte behandlingen av personopplysninger ikke fremgår tydelig. En protokoll som tilfredsstiller kravene i personopplysningsloven er en forutsetning for at en virksomhet skal kunne etterleve personvernregelverket generelt, og for å etablere en tilfredsstillende personvernerklæring spesielt.

2.3.3 Personvernerklæring

Karmøy kommunes personvernerklæring inneholder henvisninger til personopplysningsloven, og kontaktinformasjon til kommunen og kommunens personvernombud, og gir informasjon om ulike parametere vedrørende de registrertes rettigheter. Det fremgår ikke hvordan det informeres til de registrerte om endringer / oppdateringer av personvernerklæringen.

Personvernopplysningsloven artikkel 6 stiller krav til at personvernerklæringen skal inneholde informasjon om:

i. hvilke kategorier av personopplysninger virksomheten behandler
ii. hva kilden for de ulike opplysningene er og
iii. om de kom fra en offentlig tilgjengelig kilde,
iv. hvilke formål hver av de ulike personopplysningene behandles for
v. hvilket behandlingsgrunnlag de ulike behandlingene av personopplysninger har

Karmøy kommunes personvernerklæring inneholder ikke tilstrekkelig informasjon om punktene i-v til at den registrerte kan forstå hvilke personopplysninger som behandles om vedkommende. Av personvernerklæringen skal det blant annet fremgå en beskrivelse av hver enkelt behandling som kommunen faktisk utfører. For å unngå at personvernerklæringen blir for omfattende, kan kommunen eksempelvis velge å beskrive de ulike behandlingene av personopplysninger i protokoll over behandlinger, og lenke erklæringen opp til denne. Vår vurdering er at personvernerklæringen er svært mangelfull når det gjelder beskrivelse av formålet med behandlinger som gjøres. Uten dette mangler det vesentlige opplysninger for at den registrerte i tilstrekkelig grad skal forstå hvilke personopplysninger som behandles, og basert på det kunne utøve sine rettigheter.

Når det gjelder sletting av personopplysninger, fremgår det at den registrerte kan be om at personopplysninger blir rettet eller slettet dersom de er uriktige, samt at *Personopplysninger vil bli slettet når formålet med behandlingen er oppfylt, med mindre annet lovverk sier at de skal oppbevares.* I og med at formålet med den enkelte behandlingen av personopplysninger ikke fremgår tydelig av personvernerklæringen, vil det ikke være mulig for den registrerte å forstå når ulike

personopplysninger slettes om vedkommende, og dette vanskeliggjør den registrertes utøvelse av retten til sletting.

Det er et krav at den registrerte skal gjøres uttrykkelig oppmerksom på retten til å protestere senest den første gangen virksomheten kommuniserer med vedkommende. Informasjon om rettigheten skal fremlegges på en klar måte og adskilt fra annen informasjon. Retten til å protestere på behandlinger av personopplysninger fremgår av underpunkt 5.5. i personvernerklæringen. Vår vurdering er at det kan stilles spørsmål ved hvorvidt retten til å protestere fremgår tydelig nok, og i tilstrekkelig grad er adskilt fra annen informasjon.

En personvernerklæring skal ifølge Datatilsynet være *Kortfattet, (…) og forståelig (…)*. Språket i Karmøy kommune sin personvernerklæring er etter vår vurdering tidvis litt tungt med tanke på at den skal kunne leses av alle den påvirker. Likevel er det lett å finne frem ved hjelp av gode overordnede overskrifter med lenker og henvisninger til Datatilsynet sine sider.

2.3.4 Styrende dokumentasjon og risikovurderinger

Styrende dokumentasjon er i betydelig grad utarbeidet eller oppdatert i forbindelse med at den nye personopplysningsloven trådte i kraft. Det gjenstår imidlertid en del arbeid for å sikre at organisasjonen er tilstrekkelig bevisst på nye og endrede krav (jf. avsnitt 2.3.1).

Det anbefales å oppdatere *Reglement for informasjonssikkerhet og personvern*, slik at det ikke viser til *GDPR* som en frittstående forordning, men til *Personopplysningsloven* som Personvernforordningen / GDPR ble innlemmet i 20. juli 2018.

Prosedyre for kontroll og revisjon av databehandlere gir en relativt detaljert beskrivelse av krav til databehandlere og databehandleravtaler i Karmøy kommune. Prosedyren har blant annet fokus på at databehandler må iverksette tilstrekkelige sikkerhetstiltak, og bistå kommunen ved behov for å etterleve kravene i personopplysningsloven. Kommunen tester ikke at den enkelte databehandler faktisk etterlever krav i databehandleravtalen.

I følge *Reglement – internkontroll og kontinuerlig forbedring*, har alle ledere med et internkontrollansvar, ansvar for å utvikle og vedlikeholde en forbedringsplan, eller en del av en helhetlig forbedringsplan. Det fremgår også at planen skal inneholde *mål, tiltak, ansvar, fremdrift / status*, samt at det skal være et høyt fokus på *implementering, oppfølging og evaluering av tiltak*. De lederne vi intervjuet hadde ikke etablert en egen plan, eller en del av en helhetlig plan, som inkluderte gjennomføring av tiltak innen personvern.

Det gjøres risikovurderinger både sentralt i kommunen og i Helse- og omsorgsetaten. Basert på informasjon fremkommet i intervju og oversendt dokumentasjon, er vår vurdering at kommunen har et forbedringspotensial når det gjelder å systematisk gjennomføre og dokumentere risikovurderinger vurdert opp mot kommunens målsettinger, samt når det gjelder å definere og dokumentere kommunens risikoaksept. Som en del av slike risikovurderinger må det vurderes hvilke tiltak det er behov for å gjennomføre, inkl. en tydelig avklaring av ansvarlig for gjennomføring og frist. Aggregeres slike risikovurderinger opp i en helhet og presenteres for ledelsen sentralt, vil det legge til rette for at ledelsen på et overordnet nivå kan prioritere ressurser mellom ulike tiltak. Basert på en slik prioritering kan ledelsen vurdere om restrisikoen er akseptabel på ulike områder, og se den opp mot kommunens totale risikoaksept.

Kommunen har etablert en *Prosedyre for vurdering av DPIA*, men ikke en *Prosedyre for gjennomføring av DPIA* (selv om det vises til denne i førstnevnte prosedyre). Iflg. kvalitetsrådgiver skjer veiledning for gjennomføring av DPIA i Draftit. Kommunen har ikke gjennomført noen vurderinger av personvernkonsekvenser, såkalte DPIA'er, og det virker basert på intervju, å være en viss terskel for å gjennomføre slike vurderinger. Det virker å være behov for at kommunen veileder involverte medarbeidere i praktisk gjennomføring av DPIA. Dette kan eksempelvis gjøres gjennom en workshop der relevante medarbeidere inviteres til å delta i en slik vurdering, fasilitert av en person med tilstrekkelig kompetanse om temaet. I tillegg bør kommunen vurdere å etablere en prosedyre for hvordan utføre DPIA, for å legge til rette for en betryggende gjennomføring. Det er positivt at både

kommunen sentralt, og Helse- og omsorgsetaten, legger til grunn at det er behov for å ha økt fokus på DPIA i tiden fremover.

3. Personvernombudets rolle og ansvar

3.1 Revisjonskriterier

I kapittel tre besvarer vi problemstilling 2:

Hvilken rolle og ansvar har personvernombudet i Karmøy kommune?

Revisjonskriteriene er nærmere gjort rede for i vedlegg 2.

3.2 Fakta

3.2.1 Prosedyre for etablering av personvernombud

Formålet med prosedyren er *å klargjøre hvilke kvalifikasjoner og oppgaver personvernombudet i kommunen skal ha*.

Prosedyren påpeker plikten alle kommuner har til å utpeke et personvernombud med nødvendige faglige kvalifikasjoner, og at vedkommende skal *involveres i alle spørsmål som gjelder behandling av personopplysninger*.

Karmøy kommune har spesifisert personvernombudet sine oppgaver som følger:

- *Informere den behandlingsansvarlige og databehandler om plikter de har etter regelverket om personopplysninger*
- *Kontrollere overholdelse av regelverket, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som utfører behandlingsaktivitetene.*
- *På anmodning, gi råd om vurdering av personvernkonsekvenser der dette er påkrevd*
- *Foreta forhåndsdrøftinger der dette er påkrevd*
- *Samarbeide med og være kontaktpunktet for Datatilsynet*
- *Være kontaktpunktet for de registrerte angående alle spørsmål som omhandler behandling av deres personopplysninger*
- *Personvernombudet skal være bundet av taushetsplikt ved utførelse av sine oppgaver*
- *Personvernombudet kan i tillegg til dette ha andre oppgaver, sa lenge det ikke fører til interessekonflikter*

Det fremgår at personvernombudet må ha nødvendige faglige kvalifikasjoner, tilstrekkelig kompetanse *om personvernlovgivning og praksis på området, …* og *evne til å utføre oppgavene sine* både med hensyn til personlige kvaliteter og kunnskap, og ombudets posisjon i virksomheten.

Kontaktopplysningene til PVO skal offentliggjøres, for å *sikre at de registrerte … enkelt kan kontakte ombudet uten å må ta kontakt med en annen del av organisasjonen først.* Kontaktopplysningene til PVO skal også registreres hos Datatilsynet og *på de valgte mediene i kommunen*.

Ved søk på "Personvernombud" på Karmøy kommunes internettside kommer det (per juni 2019) opp tre treff, hvorav to med tittelen "Personvernombud" og et med tittelen "Personvernerklæring". Det ene treffet leder til en side med kortfattet informasjon om personvernombudets rolle, samt navn og kontaktinformasjon på kommunens personvernombud. Her er det oppgitt ombudets epostadresse i

Haugesund kommune. Det andre treffet leder til en side som gir noe mer informasjon om personvernombudets oppgaver og som gir noe veiledning om hvilke spørsmål som kan rettes til Personvernombudet. Denne siden inneholder lenker til Datatilsynets sider om personvernombudet, til Personvernforordningen og til Personopplysningsloven, men inneholder ikke informasjon om ombudets navn eller kontaktinformasjon.

3.2.2 Samarbeidsavtale mellom Haugesund kommune og Karmøy kommune om personvernombudtjeneste

I september 2018 inngikk Haugesund kommune og Karmøy kommune en samarbeidsavtale om et felles personvernombud i kommunene. Personvernombudet skal *påse at virksomheten/behandlingsansvarlig, på en uavhengig måte, overholder kravene i personopplysningsloven*. Under personvernombudets ansvarsområder, er følgende punkter listet opp:

- *Påse at behandlinger av personopplysninger blir meldt til ombudet, og at meldingene inneholder korrekte og tilstrekkelige opplysninger.*
- *Føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene*
- *Påse at behandlingsansvarlig har et system for internkontroll*
- *Bistå de registrerte med å ivareta deres rettigheter etter kravene om behandling av personopplysninger*
- *Påpeke brudd på personopplysningsloven overfor behandlingsansvarlig*
- *Gi Datatilsynet opplysninger dersom tilsynet ber om det, herunder foreta undersøkelser i konkrete saker*
- *Holde seg orientert om utviklingen innen personvern*
- *Gi råd og veiledning til behandlingsansvarlig og den registrerte om behandling av personopplysninger og kravene for dette*
- *Melde avvik som angår informasjonssikkerhet og personvern til Datatilsynet*
- *På anmodning, gi råd om vurdering av personvernkonsekvenser der dette er påkrevd*
- *Personvernombudet skal være bundet av taushetsplikt ved utførelse av sine oppgaver*

Da den nye personopplysningsloven trådte i kraft, hadde Karmøy kommune i en mellomperiode et internt personvernombud ved kvalitetsrådgiver sentralt i kommunen. Kommunen inngikk høsten 2018 en avtale med Haugesund kommune om å leie inn Haugesund kommune sitt personvernombud i en deltidsstilling. Dette ble gjort for å legge til rette for erfaringsutveksling mellom kommunene, og for å få et ombud som reelt sett var uavhengig av Karmøy kommunes administrasjon og ledelse.

Alle som ble intervjuet var klar over at kommunen hadde et personvernombud. Enhetslederen som ble intervjuet fortalte at han ikke hadde informert om personvernombudet i sin ledergruppe, og at han var usikker på om sykepleieren som skulle intervjues kjente til ham. Sykepleieren som ble intervjuet var blitt oppmerksom på ombudet gjennom e-læringskurset om personvern. Flere uttrykte at de opplevde ordningen med felles personvernombud med Haugesund kommune som positiv, ved at det legger til rette for økt grad av erfaringsdeling og læring på tvers av kommunene, og at Karmøy kommune på den måten også fikk et godt kvalifisert personvernombud.

Flere fortalte at de har brukt personvernombudet som sparringspartner og rådgiver i ulike situasjoner. Ombudet har også blitt involvert i kommunens arbeid med databehandleravtaler. Ombudet har ikke vært involvert i kommunens kartlegging av personopplysninger, men det skal ha skjedd før han ble innleid. Personvernombudet beskriver en tett dialog med kvalitetsrådgiver om hvordan ting skal gjøres, og om hvordan kravene i personopplysningsloven skal gjøres håndgripelige for kommunen. Flere fortalte at de hadde en høyere terskel for å kontakte personvernombudet enn kommunens egne ansatte dersom de trengte råd om personvern, og begrunnet det med at han var ansatt i en annen kommune.

Av intervju fremgikk det at personvernombudet oppleves å både ha en rolle for å påse at kommunen forholder seg til Personopplysningsloven, og skal være en diskusjonspartner og rådgiver ved behov, eksempelvis ved brudd på personvernreglene. Dette fremgår også av både *Prosedyre for etablering av personvernombud* og av *Samarbeidsavtale mellom Haugesund kommune og Karmøy kommune om personvernombudtjeneste,* som begge definerer personvernombudets oppgaver, men med noe ulik ordlyd. Personvernombudet uttalte selv at hva som inngår i rollen hans ikke hadde blitt diskutert i detalj, og at det nok kunne vært nyttig om personvernombud og dets rolle hadde blitt presentert for hele organisasjonen.

Personvernombudet fortalte at han har tilgang til styrende dokumentasjon i Compilo, men at han ikke har sett på den. Ombudet har også tilgang til Draftit, og mener han bør foreta noen stikkprøvebaserte kontroller der av og til, og stille spørsmål ved praksisen, men at han ikke hadde gjort det så langt. Han la til grunn at kontroller vil bli utført på bakgrunn av identifisert risiko.

3.3 Vurdering

Karmøy kommune har etablert et personvernombud iht. kravet i personopplysningsloven artikkel 37. Personvernombudet har relevant kompetanse og erfaring fra arbeid med personvern.

Kommunen har gått fra en midlertidig løsning med et personvernombud i kommunens sentraladministrasjon, til innleie av et eksternt personvernombud fra Haugesund kommune. Selv om kommunen har anledning til å ha et internt personvernombud, bidrar ordningen med et eksternt ombud til å styrke ombudets uavhengighet, samtidig som kommunen fortsatt har et ombud med god forståelse for kommunal virksomhet, og sentrale personvernrelaterte problemstillinger en kommune typisk står overfor. I tillegg bidrar løsningen til at vedkommende som ivaretar ombudsfunksjonen totalt sett får mer tid til å spesialisere seg på personvernrelaterte tema, og det legger til rette for erfaringsutveksling og kompetansedeling mellom kommunene.

Når det gjelder personvernombudets rolle og ansvar, fremgår dette av *Prosedyre for etablering av personvernombud* og av *Samarbeidsavtale mellom Haugesund kommune og Karmøy kommune om personvernombudtjeneste* som begge beskriver at ombudet både har en rådgivende og en kontrollerende rolle. Det er også noe informasjon om ombudets oppgaver på Karmøy kommune sine hjemmesider, som også inneholder en henvisning til Datatilsynet sine sider. Det benyttes ulik ordlyd for å beskrive ombudets oppgaver i de ulike kildene, men det er ikke motstrid mellom innholdet i de ulike dokumentene. Det er heller ikke motstrid mellom dokumentene som beskriver personvernombudets rolle, og kravene i personopplysningsloven 39 bokstav a til e, som beskriver hvilke roller Personvernombudet som et minimum skal ha (jf. vedlegg 2, avsnitt 10.2).

Personvernombudets oppgaver er beskrevet på et overordnet nivå i Karmøy kommune. Det kan etter vårt skjønn være hensiktsmessig å utdype enkelte av personvernombudets oppgaver, for å sikre at det er en felles oppfatning av ombudets mandat. Behovet for dette forsterkes ved at ombudet er leid inn eksternt, og det i begrenset grad ligger til rette for løpende avklaringer i det daglige. Personvernombudet uttalte selv at *hva som inngår i rollen hans ikke hadde blitt diskutert i detalj.* Eksempelvis kan det være hensiktsmessig å tydeliggjøre hva som menes med kravet i samarbeidsavtalen om å *Påse at behandlingsansvarlig har et system for internkontroll.* Enhver kommune vil typisk ha et system for interkontroll, det som menes kan være et *betryggende system for internkontroll*, og det bør i så fall presiseres. I tillegg kan det med fordel tydeliggjøres hvilke forventninger kommunen har til at personvernombudet skal kontrollere deres system for internkontroll. Selv har ombudet uttalt at *han* trolig bør ta noen stikkprøvebaserte kontroller av og til, og at det bør gjøres på bakgrunn av identifisert risiko. Det er et krav i personopplysningsloven at personvernombudet skal kontrollere virksomhetenes etterlevelse av personvernregelverket. Videre fremgår det av avtalen at personvernombudet skal *Føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene*. Dette tolkes som å føre en protokoll over kommunens behandlinger av personopplysninger. Kommunen har iverksatt et arbeid for å etablere en protokoll over behandlinger, men etter vår forståelse har personvernombudet så langt i begrenset grad vært involvert i dette arbeidet. Det bør derfor trolig presiseres hvilket ansvar ombudet eventuelt har for at det gjøres.

Personvernombudet har blitt invitert inn i noen ledergrupper i kommunen for å presentere seg, og det har blitt nevnt på kommunens intranettsider og i et e-læringskurs, men utover det har det vært lite kommunikasjon om temaet. Det er sannsynligvis begrenset kjennskap i organisasjon om hvem ombudet er og hva som er hans rolle. Eksempelvis fortalte enhetslederen som ble intervjuet, og som har ansvar for i overkant av 100 medarbeidere, at han ikke hadde informert om personvernombudet i sin ledergruppe, og at han tvilte på om sykepleierne ute i hjemmetjenesten kjente til ombudet. Dette indikerer at det er behov for å informere mer aktivt om personvernombudet i organisasjonen. Behovet forsterkes ved at ombudet er leid inn i en lav stillingsbrøk fra en ekstern kommune, og således er lite fysisk til stede hos kommunen.

Karmøy kommune bør for øvrig oppdatere internettsidene sine slik at alle sider som refererer til personvernombudet inneholder navn på vedkommende som innehar rollen, samt kontaktinformasjon.

4. Håndtering av avvik

4.1 Revisjonskriterier

I kapittel 4 besvarer vi problemstilling 3:

Hvilke rutiner har kommunen for avviksføring knyttet til brudd på personvernregelverket?

Revisjonskriteriene er nærmere gjort rede for i vedlegg 2.

4.2 Fakta

4.2.1 Reglement Informasjonssikkerhet og personvern

Av prosedyren fremgår det at:

> *ved brudd på personopplysningssikkerheten skal det innen 72 timer etter å ha fått kjennskap til avviket, melde bruddet til Datatilsynet (…). Det er kun ved hendelser hvor det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter at Datatilsynet ikke skal varsles. Ved usikkerhet rundt varslingsplikten til Datatilsynet, vil personvernombudet kunne hjelpe.*
>
> *Hendelser som kan påvirke målene for informasjonssikkerhet negativt, skal meldes og følges opp på en systematisk måte. Videre skal prosedyre for melding og håndtering av avvik følges for intern melding og håndtering av hendelsen.*

4.2.2 Prosedyre for melding og håndtering av avvik

Karmøy kommune har etablert en prosedyre for *Melding og håndtering av avvik.* Av denne fremgår det at:

> *Et avvikssystem skal sikre at avvik eller andre uønskede hendelser meldes og håndteres på en enhetlig og systematisk måte. Riktig avvikshåndtering vil kunne bidra til løpende læring og forbedring, positive konsekvenser for den enkeltes arbeidshverdag og bedret kvalitet på tjenestene.*

Avvik defineres i prosedyren som *mangel på oppfyllelse av et krav, og oppstår når det ikke er samsvar mellom den praksisen som blir utøvd – og de krav som følger av lover, forskrifter, regelverk eller av interne reglementer og prosedyrer. En annen uønsket hendelse er en situasjon som har forårsaket eller kunne ha forårsaket personskade, sykdom og/eller skade på/tap av eiendom, skade på miljøet eller tredjepart.*

Systematisk oppfølging av avvik beskrives som viktig både for å korrigere det aktuelle avviket, og for å kunne iverksette tiltak for å forebygge tilsvarende hendelser i fremtiden:

> *Alle ansatte i kommunen er ansvarlige for å melde avvik eller annen uønsket hendelse i henhold til denne prosedyren. Nærmeste leder har ansvar for å håndtere avvik/utforme og iverksette tiltak slik at avviket blir lukket innen fastsatt tidsfrist*.
>
> Avvik skal *meldes i kommunens digitale avvikssystem, og meldte avvik eller andre uønskede hendelser vil deretter bli styrt/håndtert som beskrevet i følgende prosess*:
>
> 1. *Ved oppdaget avvik skal det vurderes om det er behov for å iverksette strakstiltak for å stoppe avviket og/eller begrense skadeomfanget.*
>   *Oppdaget avvik meldes i forbedringssystemet. En beskrivelse av avviket med*

tilhørende informasjon legges inn i meldingen.
Avviksmelder kan følge behandlingen av avviket ved å se på sine innsendte avvik.

2. *Avviket mottas av nærmeste leder.*
3. *Vurdere om andre instanser/myndigheter skal varsles om avviket. Dette kan være Personvernombud, fylkesmannen, politi.*
4. *Avviket håndteres (se bruksanvisning). Avviket er ikke lukket før alle tiltak er gjennomført og ny praksis er etablert. Ved opprettelse av tiltak utvides "behandlingsfristen" med 30 dager (…).*
5. *Dersom det ikke gjøres en aktiv handling med avviket innen fastsatt tidsfrist (14 dager), sendes avviket videre i linjen*.

Prosedyren inneholder også informasjon om hvem som er ansvarlig for de ulike aktivitetene.

I følge kvalitetsrådgiver i kommunens sentraladministrasjon, gjenstår det et arbeid for å detaljere prosedyren for melding og håndtering av avvik mht. brudd på personopplysningsloven. Dette planlegges gjort når organisasjonen har fått mer erfaring med håndtering av avvik.

I Karmøy kommune skal avvik og forbedringsmeldinger rapporteres i et administrativt system kalt Compilo. Systemet er nylig implementert i kommunen, og flere forteller at kommunen har en kommunikasjons- og forankringsjobb foran seg for å bygge en god rapporteringskultur, og at det pt. er en betydelig underrapportering. En leder uttalte i intervju at vedkommende var usikker på om det er en rutine for varsling av brudd på personopplysningsloven, men at det naturlige ville være å varsle ledervei dersom det oppstod avvik.

Det er etablert en rutine der personvernombudet automatisk får en kopi på mail av alle avvik som omhandler personvern som meldes i Compilo. Denne rutine skal bidra til å gjøre kommunen i stand til å overholde fristen om å melde avvik til Datatilsynet innen 72 timer, samt til raskt å kunne underrette registrerte i de tilfeller der det er sannsynlig at bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter. Når avvik er meldt elektronisk, kan den som har meldt avviket følge saksbehandlingen i systemet, og se hvilke vurderinger som blir gjort og eventuelt hvilke tiltak som blir iverksatt. Det er ikke etablert en tilsvarende automatisk varslingsrutine av personvernombudet ved personvernrelaterte avvik i kommunens journalsystem.

Personvernombudet fortalte at han var positivt overrasket over hvor effektivt kommunen klarte å fremhente nødvendig dokumentasjon i forbindelse med en henvendelse fra Datatilsynet.

I Helse- og omsorgsetaten opererer man med to avvikssystemer. Compilo skal benyttes for rapportering av "generelle" avvik, mens avvik knyttet til den enkelte pasient rapporteres i journalsystemet. Flere forteller i intervju at det er en relativt god rapporteringskultur for pasientrelaterte avvik, enten ved at avvik rapporteres til nærmeste leder, eller ved at de registreres elektronisk. Flere forteller at det er større grad av underrapportering når det gjelder "generelle" avvik som skal rapporteres i Compilo. En leder forteller at avvik som registreres i journalsystemet også skal registreres i Compilo, og at det er en tungvint prosess å skulle rapportere avvik to ganger. Andre ledere forteller at avvik enten skal rapporteres i journalsystemet eller i Compilo, avhengig av avvikets karakter.

Kommunen har oppdaget avvik fra kravene i personopplysningsloven, men ikke noe så alvorlig at det har blitt vurdert som nødvendig å varsle Datatilsynet eller registrerte. Da avviket ble oppdaget mobiliserte ledelsen raskt ledere på ulike nivå, etatens jurist, kvalitetsrådgiver i kommunens sentraladministrasjon og kommunens personvernombud, og gjorde i samarbeid en vurdering av alvorligheten av avviket, og av hvorvidt det var behov for å melde avviket til Datatilsynet og registrerte.

4.3 Vurderinger

Karmøy kommune har nylig implementert et nytt system der avviks- og forbedringsmeldinger skal rapporteres, og det er således naturlig at det i en tidlig fase er en viss underrapportering av avvik som følge av begrenset kjennskap til systemet. Det er imidlertid behov for å gi kommunens ansatte en god innføring i hvordan det nye systemet skal benyttes, derunder tydelig definere hva som utgjør et avvik, og hvordan og hvor avvik skal rapporteres. Dette gjelder både generelt for avvik sett under ett, og spesielt for personvernrelaterte avvik. For personvernrelaterte avvik er det i tillegg behov for å tydeliggjøre krav til rapportering i styrende dokumentasjon, for å gi nødvendig veiledning til organisasjonen om hvordan slike avvik skal følges opp. Tilstrekkelig og tydelig kommunikasjon om dette vil bidra til å muliggjøre en god rapporteringskultur.

Det er positivt at det er etablert en rutine der personvernombudet varsles umiddelbart om alle avvik vedrørende personvern som rapporteres i Compilo. Det kunne med fordel vært etablert en tilsvarende automatisk varslingsrutine ved personvernrelaterte brudd i kommunens journalsystem.

Det er også positivt at kommunen har vist evne til å mobilisere relevant personell og raskt få oversikt over situasjonen ved personvernrelaterte avvik, og til å fremskaffe nødvendig dokumentasjon ved forespørsel fra Datatilsynet.

I Helse- og omsorgsetaten opplever enkelte respondenter usikkerhet rundt hvilke avvik som skal rapporteres hvor, samt om det er tilstrekkelig å rapportere pasientrelaterte avvik i journalsystemet, eller om det også skal rapporteres i Compilo. Det er således behov for å tydeliggjøre forholdet mellom rapportering av avvik i journalsystemet og i Compilo, for å legge til rette for en enhetlig og forsvarlig praksis.

5. Fordeling av roller og ansvar innen informasjonssikkerhet

5.1 Revisjonskriterier

I kapittel 5 besvarer vi problemstilling 4:

Er det en klar fordeling mellom roller og ansvar i informasjonssikkerhetsarbeidet i kommunen?

Revisjonskriteriene er nærmere gjort rede for i vedlegg 2.

5.2 Fakta

De fleste respondenter beskriver i intervju at roller og ansvar generelt, og i forhold til personvern spesielt, oppleves å være relativt tydelig avklart både internt i helse- og omsorgsetaten, mellom etaten og kommunens sentraladministrasjon, samt mellom kommunens sentraladministrasjon og personvern-ombudet. Flere fortalte at de opplevde at fordeling av roller og ansvar også fungerte greit i praksis.

Kvalitetsrådgiver i kommunens sentraladministrasjon forteller at hun har ansvar for at det etableres et rammeverk på personvernområdet, og for at det kommuniseres ut i organisasjonen. Øvrige intervjuobjekter delte denne oppfatningen. Rådmannen er behandlingsansvarlig for personopplysninger i kommunen, og har således ansvar for at kommunen etterlever krav i Personopplysningsloven. Rådmannen har imidlertid delegert ansvar og myndighet til Kommunalsjefene for de ulike etatene for å sørge for at etatene drives i samsvar med lover, forskrifter og overordnede instrukser, og at de er gjenstand for betryggende kontroll. Denne delegeringen omfatter også at kommunalsjefene har ansvar for etterlevelse av kravene i personopplysningsloven i sine respektive etater, inklusive inngåelse og kvalitetssikring av databehandleravtaler. Denne delegeringen av ansvar og myndighet fremgår av styrende dokumentasjon. Tilsvarende har rådmannen delegert myndighet og ansvar for etterlevelse av krav i personvernlovgivningen i kommunens sentraladministrasjon til stabssjef.

IKT-sjef fortalte at han har ansvar for *den tekniske sikkerheten i kommunen*. Det er ikke etablert en Informasjonssikkerhetsansvarlig (ofte kalt en CISO). Informasjonssikkerhet dreier seg ifølge Datatilsynet om å *håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger.* Arbeid med informasjonssikkerhet er således viktig for å sikre personopplysninger i samsvar med personopplysningsloven artikkel 32. I følge artikkel 32 (1) *skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen* (…). Artikkel 32 (2) presiserer videre at *Ved vurdering av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen (…)*. Denne plikten til å sørge for sikkerhet ved behandlingen omhandler ikke bare teknisk sikkerhet, men informasjonssikkerhet som helhet. Norm for informasjonssikkerhet i helsesektoren stiller videre konkrete og strenge krav til arbeidet med informasjonssikkerhet innen helse og omsorg. Vi anbefaler å knytte arbeidet med å etablere en betryggende informasjonssikkerhet opp mot anerkjente standarder som f. eks. ISO 27001. Et rammeverk for informasjonssikkerhet bør blant annet inneholde informasjon om, og et tydelig ansvar for å følge opp følgende områder:

- **Etterlevelse**, derunder utvikle oversikt over interessenter relatert til informasjonssikkerhet, sammenstille krav fra interessenter, følge opp myndigheter og spesielle interessegrupper og koordinere all innsats knyttet til personvern.

- **Dokumentasjon**, derunder foreslå et utkast til et rammeverk for informasjonssikkerhet, og være ansvarlig for å revidere og oppdatere hoveddokumentene.

- **Risikostyring**, derunder lære opp medarbeidere i risikovurderinger, koordinere utarbeidelse og sammenstilling av risikovurderinger, foreslå tiltak og frister for implementering.

- **HR oppgaver**, derunder utføre bakgrunnssjekker av jobbsøkere, forberede og gjennomføre opplæring og andre aktiviteter for å heve bevissthetsnivået mv.

- **Samhandling med toppledelsen**, derunder kommunisere behovet for informasjonssikkerhet, foreslå mål, rapportere status, foreslå tiltak, budsjett og andre nødvendige ressurser mv.

- **Forbedringer**, derunder følge opp at alle besluttede tiltak iverksettes, og verifisere at de korrigerende handlingene har eliminert risiko iht. forutsetningen.

- **Håndtering av aktiva**, derunder ha oversikt over alle viktige informasjonsaktivum, slette filer som ikke lenger er nødvendige og sørge for sikker avhending av overflødige medium og tilbehør.

- **Tredjeparter**, derunder gjøre risikovurdering av aktiviteter som planlegges outsourcet, utføre bakgrunnssjekk av involverte parter og definere sikkerhetsklausuler i avtaler.

- **Kommunikasjon**, derunder definere hvilke kommunikasjonskanaler som det er tillatt å benytte, og forberede utstyr til kommunikasjon i en beredskapssituasjon.

- **Håndtering av hendelser,** derunder motta informasjon om hendelser, koordinere respons på hendelser, sikre bevis i etterkant av en hendelse og analysere hendelser for å forhindre tilsvarende hendelser i fremtiden.

- **Forretningskontinuitet**, derunder koordinere prosessen for å gjøre en konsekvensanalyse (Business Impact Analysis) og responsplaner, koordinere øvelser og testing, samt revidere gjenopprettingsplaner i etterkant av hendelser.

- **Teknisk sikkerhet**, derunder metoder for å besørge virksomhetens tekniske sikkerhet, eksempelvis policy for å beskytte mobiltelefoner, policy for passord, bruk av kryptering mv.

Det er ikke et eksplisitt krav at kommunen skal etterleve ISO 27001. Kommuneloven stiller imidlertid krav til at kommunen skal ha en betryggende internkontroll. I dette inngår en betryggende oppfølging av ulike aspekter ved informasjonssikkerhet. I tillegg stiller som nevnt både Personopplysningsloven og Norm for informasjonssikkerhet i helsesektoren krav til kommunens arbeid med informasjonssikkerhet. Ansvaret for informasjonssikkerhet som helhet påhviler rådmannen. Ansvaret kan delegeres, og det er gjort på enkelte områder, derunder for teknisk sikkerhet og etterlevelse av personvernkrav. Vi finner imidlertid ikke dokumentasjon som tilsier at ansvaret for alle aspekter ved informasjonssikkerhet er delegert ut i kommunen, utover en generell formulering i delegasjoner om at stabssjef / Kommunalsjef skal sikre etterlevelse av eksterne og interne krav, og at det er en betryggende kontroll. Flere respondenter uttrykte at de var usikker på hvem som hadde ansvaret for å følge opp ulike aspekter ved informasjonssikkerhet, derunder for arbeidet med å forestå nødvendig opplæring innen informasjonssikkerhet som helhet.

5.3 Vurdering

Roller og ansvar virker å være tydelig avklart når det gjelder teknisk sikkerhet og personvern. Informasjonssikkerhet er imidlertid et bredt begrep som både dekker den tekniske sikkerheten, og mer "myke" tema som også omhandler den menneskelige faktor og arbeid for å styrke sikkerhetskulturen og –bevisstheten i en virksomhet, derunder opplæring.

Det virker å være en viss usikkerhet i virksomheten knyttet til ansvar for informasjonssikkerhet utover teknisk sikkerhet og personvern (jf. veiledning i avsnitt 5.2 om tema som inngår i informasjonssikkerhetsdimensjonen). Det kan være hensiktsmessig at rådmannens ledergruppe drøfter dette temaet, og tydelig kommuniserer ut i hele virksomheten roller og ansvar for ulike aspekter ved informasjonssikkerhet, derunder kommunens handlingsplan for å sikre en betryggende praksis på området. Dersom dette ansvaret er delegert til den enkelte kommunalsjef og til stabssjef, bør det tydeliggjøres i rådmannens delegasjoner.

6. Omsorgssektorens håndtering av personopplysninger

6.1 Revisjonskriterier

I kapittel 6 besvarer vi problemstilling 5:

I hvilken grad har omsorgssektoren i Karmøy kommune innrettet seg etter det nye personvernregelverket? Herunder:

a. I hvilken grad har virksomhetene utarbeidet tilstrekkelig internkontroll på området?

b. Har virksomhetene oversikt over hvilke personopplysninger de behandler?

c. I hvilken grad er det gjennomført risikovurderinger i virksomhetene?

Revisjonskriteriene er nærmere gjort rede for i vedlegg 2.

6.2 Fakta

6.2.1 I hvilken grad har virksomhetene utarbeidet tilstrekkelig internkontroll på området?

Helse- og omsorgsetaten er underlagt *Norm for informasjonssikkerhet, helse og omsorgstjenesten (heretter "Helsenormen")*. Normen trådte opprinnelig i kraft i 2006, og har blitt oppdatert en rekke ganger siden det, blant annet for å ta høyde for nye krav på personvernområdet. Normen adresserer tydelig taushetsplikt for helsepersonell, og flere forteller at endringene i personopplysningsloven ikke innebærer så store endringer for Helse- og omsorgsetaten, fordi etaten i lang tid har vært underlagt streng lovgivning på området. Innføring av nye personvernkrav fikk begrensede konsekvenser for Etaten.

Samtidig forteller flere om et økt fokus på personvern det siste året, og om et høyt bevissthetsnivå ute i Helse- og omsorgsetatens virksomhetsområder. Enkelte beskriver også et økt fokus på å ivareta personvernet til de ansatte med den nye personopplysningsloven. Intervjuobjektene hadde gjennomgående en god forståelse for grunnleggende krav i personopplysningsloven, derunder for hva som kjennetegner en personopplysning, ulike kategorier personopplysninger, og for hvordan slike opplysninger skal håndteres.

6.2.2 Roller og ansvar i Helse- og omsorgsetaten ift. Personvern

Som en forberedelse til forvaltningsrevisjonen av Karmøy kommune sin etterlevelse av personvernregelverket, utarbeidet jurist i Helse- og omsorgsetaten notatet *Roller og ansvar i Helse- og omsorgsetaten ift. personvern.* Under følger en oppsummering av innholdet i notatet.

Rådmannen har delegert følgende myndighet til kommunalsjef helse og omsorg:

Av delegasjonsreglementet fremgår det at

- *"Kommunalsjef helse og omsorg skal sørge for at helse- og omsorgsetaten drives i samsvar med lover, forskrifter og overordnede instrukser, og at helse- og omsorgsetaten er gjenstand for betryggende kontroll (…).*

- *"Kommunalsjef helse og omsorg gis innenfor sitt ansvarsområde fullmakt til å avgjøre alle saker som må regnes som ikke av prinsipiell betydning, så langt som rådmannens myndighet på området rekker (…).*

Det ovenfor nevnte omfatter blant annet at kommunalsjef i helse og omsorg skal sørge for at etaten oppfyller personvernlovgivningen. Det fremgår også at kommunalsjef har anledning til å videredelegere fullmakter. *Det er utarbeidet delegasjonsreglement fra kommunalsjef helse og omsorg til avdelingssjefer. Disse er under omarbeidelse.*

Kommunalsjef helse og omsorg har opprettet et GDPR-utvalg i Helse- og omsorgsetaten bestående av IT-koordinator (…) (utvalgets leder), forvaltningssjef (…), helsesjef (…), omsorgssjef (…) og jurist (…). Gruppen har ansvar for å sørge for at kommunen overholder personvernregelverket.

Internt har arbeidet i GDPR-gruppen blitt fordelt slik blant medlemmene:

- *Alle gruppens medlemmer har kartlagt databehandlingen i Profil*
- *Jurist (…) har ansvaret for at databehandleravtaler inngås.*
- *IT-koordinator (…) har sammen med hver sektors sjef foretatt kartlegging av databehandling innen den aktuelle sektor.*

Alle nyansatte må signere en taushetserklæring, og ledere er forpliktet til å ta opp taushetsplikt og journalføring med de ansatte i den utførende virksomheten, bla. gjennom opplæring:

> *Sektor forvaltning (…) sørger i anskaffelsesprosesser for at leverandører gjennom* krav i *avtalene … må forholde seg til taushetsplikt- og personvernreglene i lovgivningen (…)* Enheten følger opp *kontrakter på personvern*, og har bla. fått gjennomslag for krav om *2-faktor-pålogging* til *Telenor* for trygghetsalarmtjenesten.

Helse og omsorgsetaten gjør ifølge notatet fortløpende vurderinger av personvern. Dette underbygges gjennom intervju. Slike vurderinger dokumenteres ikke systematisk.

Det fremgår av notatet at *I Helse- og omsorgsetaten, som i kommunen for øvrig, er det linjeansvar, dvs. at overordnede har ansvar for at underordnede følger lover og forskrifter i sin utførelse av sine arbeidsoppgaver. Oppgaver blir gitt i henhold til kompetanse. Blant annet har IT-koordinator hovedarbeidsoppgaver i tilknytning til* Helsenormen, og etaten har også fått bistand fra IT-avdelingen for å sikre etterlevelse av Normen.

I tillegg gjelder personvernlovgivningen og taushetspliktreglene i forvaltningsloven og særlovgivningen i helse- og omsorgssektoren for alle ansatte i Helse- og omsorgsetaten.

I intervju beskrives en situasjon med høyt fokus på lederes kompetanse om personvernrelaterte krav. Kvalitetsrådgiver i kommunens sentraladministrasjon og Forvaltningssjef i Helse- og omsorgsetaten har gjennomgått ulike personvernrelaterte krav og problemstillinger i ledermøter i Etaten. Flere ledere forteller også at de har sett på innholdet i personvernforordningen på eget initiativ, for å skaffe seg nødvendig oversikt over de nye kravene. Alle medarbeidere har fått tilsendt et e-læringskurs innen personvern, men kun en andel har gjennomført dem (jf. avsnitt 2.2.3). IT-medarbeider i Etaten inviteres av og til inn i enhetsmøter, der hun bidrar med opplæring knyttet til informasjonssikkerhet generelt, og personvern spesielt. I følge intervju er det ikke distribuert noe informasjon om informasjonssikkerhet generelt, eller om personvern spesielt i Etaten, og det er eksempelvis ikke gitt informasjon om kryptering av epost for å unngå at sensitiv informasjon kommer på avveie. Flere forteller at mange lave stillingsbrøker og høy turnover gjør det utfordrende å sørge for at alle får tilstrekkelig opplæring.

Det er utarbeidet rutiner, prosedyrer, skjema osv. for Helse- og omsorgsetaten, for å sikre en enhetlig praksis, derunder skjema der bruker signerer på samtykke til bruk av personopplysninger, rutine for behandling av forespørsler fra pårørende m.v. I tillegg forholder Etaten seg til sentralt utarbeidede rutiner og krav knyttet til personvern. Det er etablert et eget avvikssystem for pasientrelaterte avvik, i tillegg til at Etaten forholder seg til kommunens avvikssystem for generelle avvik. Det er også etablert ulike møteplasser som avdelingsmøter og pasientsikkerhetsvisitter, der medarbeidere kan ta opp ulike tema de er usikre på for å få nødvendige avklaringer.

Ute i hjemmetjenesten beskriver flere en årvåkenhet for å sikre fortrolig informasjon, inklusive personopplysninger. Nytilsatte får opplæring i håndtering av fortrolig informasjon, og må signere en taushetserklæring. Risiko diskuteres, og det iverksettes praktiske risikoreduserende tiltak, eksempelvis stille rapport der den enkelte medarbeider leser seg opp på viktig pasientrelatert informasjon i stedet for at det gjennomgås i dialog, låsing av dører, tildekking av dokumenter i bil med videre. Flere forteller at det tidligere var vanlig å dele passord med nytilsatte og vikarer av effektivitets-hensyn, men at Etaten nå har gått bort fra denne praksisen. Det føres logg over oppslag og endring i pasientsystemet, og det er etablert en rutine for å forebygge og avdekke såkalt journalsnoking, altså at medarbeidere leser informasjon i pasientjournaler som de ikke har et tjenstlig behov for.

Forvaltningssjef forteller at han har ansvar for å initiere aktiviteter på et overordnet nivå innen personvern som å sette i gang opplæring, kartlegging, lage plan for hva som skal gjøres, prioritering av tiltak osv. Informasjon følger i høy grad lederrekken utover i organisasjonen.

6.2.3 Oversikt – databehandleravtaler – Helse- og omsorgsetaten

Karmøy kommune har oversendt en oversikt over status for inngåelse av databehandleravtaler for Helse- og omsorgsetaten, derunder oversikt over 17 inngåtte databehandleravtaler og syv som etaten vurderer det som sannsynlig at snart er på plass. Etaten har lang erfaring med databehandleravtaler, men legger til grunn at eksisterende avtaler må gjennomgås på nytt for å sikre at innholdet tilfredsstiller nye krav i personopplysningsloven.

I følge flere intervjuobjekt, har Helse- og omsorgsetaten fokus på innebygd personvern ved innkjøp av nye IT-systemer. Flere intervjuobjekt fortalte at Etaten arbeider godt med å få på plass nødvendige databehandleravtaler, inklusive en kvalitetssikring av innholdet. Det er også etablert en egen prosedyre for kontroll og revisjon av databehandlere (jf. avsnitt 2.2.5).

6.2.4 Har virksomhetene oversikt over hvilke personopplysninger de behandler?

I regi av GDPR-gruppen (jf. avsnitt 6.2.2), har det vært gjennomført en kartlegging av behandlinger, behandlingsgrunnlag og formål for data som finnes i alle Helse- og omsorgsetaten sine fagsystemer. Denne kartleggingen har blitt dokumentert i et system kalt Draftit. Arbeidet har hatt en risikobasert tilnærming, der man startet med å kartlegge de systemene som inneholdt flest personopplysninger. Under hvilke personopplysninger som behandles, fremgår informasjon om ulike opplysninger, derunder om hvilke identitetsopplysinger, kontaktopplysninger og sensitive personopplysninger som behandles. Etaten har organisert protokollen basert på ulike system, og ikke per behandling som utføres. Hvilket formål som gjelder for behandlingene i systemet er samlet i "en sekkepost". Tilsvarende er gjort for andre parametere, derunder for behandlingsgrunnlaget. Jf. avsnitt 2.2.1 for mer informasjon om hvilken informasjon som fremgår av systemet.

Helse- og omsorgsetaten har mottatt og behandlet enkelte krav om innsyn i personopplysninger. Dersom slike krav leveres til operativt personell, vil de bli løftet til nærmeste leder som enten fatter en beslutning eller løfter beslutningen til neste ledernivå dersom vedkommende er usikker på hvordan det bør håndteres. Det er ikke mulig å søke opp personopplysninger for en registrert på tvers av ulike datasystemer, og informasjon vil således måtte hentes ut manuelt fra det enkelte system og sammenstilles. I intervju legger intervjuobjektene til grunn at Helse- og omsorgsetaten bør være i stand til å gi innsyn i personopplysninger på forespørsel, også dersom antall slike innsynsbegjæringer øker.

6.2.5 I hvilken grad er det gjennomført risikovurderinger i virksomhetene?

I følge intervju og notatet om roller og ansvar i Helse- og omsorgsetaten, gjør Etaten løpende risikovurderinger knyttet til personvern. Aktuelle tema som nevnes omfatter bla:

- Tilgangsstyring for å sikre at medarbeidere kun har tilgang til informasjon de har tjenstlig behov for
- Avklaring av hvilke opplysninger som bør, og ikke bør, fremgå av en journal
- Tiltak for å beskytte fysiske dokumenter med sensitiv informasjon
- Tiltak for å unngå at uvedkommende overhører samtaler
- Etablering av et responssenter som tar imot alarmer for å unngå at man må ta potensielt sensitive telefonsamtaler ute hos brukerne
- Nye rutiner for utskrift som krever pålogging

Flere beskriver en høy årvåkenhet ifht. systemteknisk risiko, og da særlig ved innføring av nye løsninger innen velferdsteknologi, og at det følges opp i databehandleravtaler.

I følge intervju og tilsendt dokumentasjon, er det ikke gjort en helhetlig risikoanalyse for Etaten sett under ett og / eller per tjenesteområde, og risikovurderinger er ikke systematisk dokumentert. Det er ikke gjennomført noen personvernkonsekvensvurderinger (DPIA) i Etaten. Flere la til grunn at det er et forbedringspotensial knyttet til systematisk gjennomføring og dokumentasjon av risikovurderinger generelt, og til personvernkonsekvensvurderinger spesielt.

6.3 Vurdering

I hvilken grad har virksomhetene utarbeidet tilstrekkelig internkontroll på området?

Helsesektoren er en gjennomregulert sektor med lang erfaring når det gjelder å forholde seg til strenge krav til håndtering av taushetsbelagt informasjon, derunder personopplysninger. Medarbeidere i Helse- og omsorgsetaten har en høy bevissthet når det gjelder å sørge for en forsvarlig behandling av taushetsbelagt informasjon. Det vurderes som sannsynlig at det er et særlig høyt fokus på personvern i Helse- og omsorgsetaten i Karmøy kommune.

Med den nye personopplysningsloven har det likevel kommet noen nye krav som Etatens ledere og medarbeidere må forholde seg til. Det er etablert flere rutiner og prosedyrer for å sikre forsvarlig håndtering av personopplysninger i Etaten, i tillegg til at styrende dokumentasjon vedrørende personvern som er utarbeidet sentralt i kommunen også gjelder for Etaten. Det er imidlertid begrenset grad av kommunikasjon av krav i styrende dokumentasjon ut i virksomheten.

Nye personvernkrav har vært tema i en del møter, det har vært sendt ut e-læringskurs på epost, og nytilsatte må signere taushetserklæringer. Utover det har det ikke vært en systematisk opplæring i informasjonssikkerhet generelt, eller i personvern spesielt. Den opplæringen som foregår er ikke basert på en tydelig "bestilling" eller på annen måte systematisert, og den er personavhengig i den forstand at Forvaltningssjef eller IT-medarbeider inviteres inn i henholdsvis ledergrupper og avdelingsmøter for å informere om temaet. Fordi helsesektoren har vært strengt regulert i mange år vurderes risikoen som begrenset. Likevel bør opplæring innen informasjonssikkerhet generelt, og personvern spesielt, i større grad systematiseres slik at man sikrer at alle får nødvendig informasjon, og at det er en enhetlig tilnærming til kommunikasjon om temaet.

Kommunalsjef helse og omsorg har ansvar for Etatens etterlevelse av personvernkrav. Hun har opprettet et GDPR-utvalg i etaten som ifølge et notat etatens jurist har utarbeidet *har ansvar for å sørge for at kommunen overholder personvernregelverket.* Kommunen tolkes her som Helse- og omsorgsetaten, hvilket en representant for etaten har bekreftet at er korrekt. Det fremstår som noe uklart hvorvidt dette i praksis betyr at GDPR-gruppen har fått ansvar for å sikre etterlevelse av

personvernkrav i etaten, og hva som er gruppens ansvar for etterlevelse, sett opp mot linjeledelsens ansvar for etterlevelse. Notatet er imidlertid ikke et formelt dokument, og vi tolker gruppens mandat dit hen at de er etablert for å gi ledelsen nødvendig støtte i arbeidet med å sikre etterlevelse av regelverket. Helse- og omsorgsetaten har bekreftet at kommunalsjef helse og omsorg fortsatt har et overordnet ansvar for overholdelse av personvernlovgivningen, selv om hun har delegert et ansvar til GDPR-gruppen. Det anbefales å tydeliggjøre roller og ansvar for etterlevelse av personvernregelverket i etaten, for å sikre at det er en enhetlig forståelse, og således redusere risikoen for brudd på regelverket.

Helse- og omsorgsetaten har utarbeidet en relativt detaljert prosedyre for kontroll og revisjon av databehandlere, som gir nyttig veiledning ved inngåelse og kvalitetssikring av databehandleravtaler. Etaten har over tid arbeidet med å inngå og kvalitetssikre databehandleravtaler. Det gjenstår imidlertid fortsatt en del arbeid før alle nødvendige, nye avtaler er inngått, og alle gjeldende avtaler er kvalitetssikret og oppdatert.

Har virksomhetene oversikt over hvilke personopplysninger de behandler?

Helse- og omsorgsetaten har utarbeidet en oversikt over hvilke personopplysninger etaten behandler per fagsystem, og dette er dokumentert i verktøyet Draftit. Vår vurdering er imidlertid at kommunens protokoll er mangelfull, fordi formålet med den enkelte behandlingen av personopplysninger ikke fremgår tydelig.

Etaten har mottatt innsynsbegjæringer, og har i slike tilfeller klart å sammenstille og gjøre tilgjengelig den etterspurte informasjonen. Etaten har imidlertid ikke opplevd en situasjon der et stort antall registrerte ber om innsyn i registrerte personopplysninger samtidig. Dette kan typisk skje i kjølvannet av et kritisk medieoppslag om kommunens håndtering av personopplysninger. Det vurderes som sannsynlig at det i en slik situasjon vil bli arbeidskrevende for kommunen å oppfylle forpliktelsen sin til å gi innsyn, fordi det ikke er mulig å automatisere uttrekk av personopplysninger på tvers av ulike systemer. Manuelle uttrekk av informasjon, og sammenstilling av opplysningene, er arbeidskrevende og gir normalt en økt risiko for feil relativt til automatiserte prosesser.

I hvilken grad er det gjennomført risikovurderinger i virksomhetene?

Etaten gjør løpende risikovurderinger knyttet til personvern der det vurderes som nødvendig, men virker ikke å ha en systematisk tilnærming til gjennomføring og dokumentering av risikovurderinger. Dette gir en risiko for at Etaten ikke blir oppmerksom på viktige risikoer, hvilket igjen kan føre til at den ikke iverksetter nødvendige risikoreduserende tiltak. Det er således et potensial for å profesjonalisere etatens risikostyring.

Det er et høyt fokus på fysisk sikring av personopplysninger, derunder på oppbevaring av dokumenter som inneholder personopplysninger, risiko for at noen overhører fortrolige samtaler osv. Det virker i mindre grad å være fokus på IKT-relatert risiko, derunder på risiko for feilsending av epost, at kriminelle skaffer seg tilgang til sensitiv informasjon i elektroniske kanaler gjennom medarbeidere m.v. Det virker således å være behov for at etaten øker fokuset på IKT-relaterte risikoer.

Personopplysningsloven artikkel 35 stiller krav om å gjøre personvernkonsekvensvurderinger ved gitte omstendigheter. Representanter for Helse- og omsorgsetaten er klar over dette kravet, både for pågående og nye behandlinger, men har så langt ikke gjort noen slike vurderinger. Vi har ikke grunnlag for å vurdere hvorvidt det så langt har vært behov for at etaten skulle ha gjort en eller flere personvernkonsekvensvurderinger, for å etterleve krav i personopplysningsloven.

7. Anbefalinger

KPMG vil her komme med anbefalinger på områdene der det i forvaltningsrevisjonen er funnet regel/rutinebrudd eller forbedringspotensial.

Anbefalingene er formulert på bakgrunn av vurderingene, og peker på områder hvor kommunen etter vår vurdering i første omgang bør prioritere å gjøre tiltak for å legge til rette for en tryggere praksis for behandling av personopplysninger.

Vår anbefaling er at Karmøy kommunes sentraladministrasjon prioriterer følgende områder:

1. Kommunikasjon og opplæring

Karmøy kommune holder på å implementere et nytt ledelsessystem. Denne prosessen har trolig bidratt til å hemme effektiv kommunikasjon om styrende dokumenter og krav knyttet til blant annet personvern. Det anbefales at kommunens sentraladministrasjon vurderer hvordan den effektivt kan kommunisere styrende dokumenter og krav ut i virksomheten, og iverksetter nødvendige tiltak for å gjøre viktig personvernrelatert informasjon kjent.

Kommunen bør også vurdere å øke omfanget av opplæring i informasjonssikkerhet generelt, og i krav i personopplysningsloven spesielt. Opplæringen bør systematiseres for å sikre at alle medarbeidere får nødvendig opplæring. Det bør blant annet vurderes hvilke kanaler som egner seg for opplæring av ulike typer medarbeidere, eksempelvis ved at medarbeidere som i begrenset grad benytter epost og administrative systemer i hverdagen, tilbys fysisk opplæring i møter eller lignende for å sikre at de får nødvendig informasjon.

2. **Protokoll over behandlinger og personvernerklæring.**
Karmøy kommunes protokoll over behandlinger er mangelfull når det gjelder å konkretisere formålet med den enkelte behandlingen av personopplysninger. Det er behov for en gjennomgang og oppdatering av innholdet i protokollen.

Karmøy kommune bør videre gjennomgå personvernerklæringen, og oppdatere den slik at den tilfredsstiller kravene i personopplysningsloven. Det er særlig behov for å utbedre innholdet i personvernerklæringen når det gjelder en tydeliggjøring av formålet med kommunens behandlinger av personopplysninger, slik at den registrerte gis tilstrekkelig informasjon til å forstå hvilke behandlinger kommunen utfører. Å forstå hvilke behandlinger som utføres, er en forutsetning for å kunne ivareta egne personvernrettigheter. .

3. Profesjonalisering av kommunens risikostyring

Det er et potensial for å profesjonalisere kommunens risikostyring, både sentralt og i Helse og –omsorgsetaten. Det anbefales at ledelsen legger en plan for å sikre at det er en betryggende risikostyring. Sentrale momenter innen risikostyring omfatter:

- Avklare ledelsens risikoaksept
- Gjennomføre en helhetlig risikoanalyse
- Dokumentere vurderinger
- Prioritere tiltak, tilordne ansvar og fastsette frist for lukking av det enkelte tiltak
- Etablere en rutine for å følge opp lukking av prioriterte tiltak
- Etablere en rutine for å oppdatere risikoanalysen jevnlig, samt ved vesentlige endringer som påvirker gjeldende risikovurderinger

Planen må videre dokumenteres og innarbeides i virksomhetens årshjul for internkontroll.

4. Avklaring av personvernombudets rolle og ansvar

Det anbefales at Karmøy kommune, i samarbeidet med personvernombudet, utdyper ombudets rolle og ansvar, for å sikre at det er en felles oppfatning av hva som inngår i ombudets mandat. I denne forbindelse bør det blant annet klargjøres i hvilket omfang personvernombudet skal utføre kontroller av virksomheten.

5. Avvikshåndtering

Det er behov for å gi medarbeidere i kommunen nødvendig opplæring i rapportering av avvik i Compilo, for å legge til rette for en god rapporteringskultur. Det bør tydelig defineres hva som utgjør et avvik, og hvordan og hvor avvik skal rapporteres. Videre er det behov for å tydeliggjøre rutinen for rapportering av avvik i journalsystemet sett opp mot rutine for rapportering av avvik i det administrative systemet (Compilo), altså hvilke avvik som skal rapporteres hvor, samt om enkelte avvik skal rapporteres begge steder.

6. Avklaring av roller og ansvar knyttet til informasjonssikkerhet

Det anbefales å tydeliggjøre fordeling av roller og ansvar knyttet til informasjonssikkerhet i kommunen, og kommunisere konklusjonen ut i hele virksomheten. Dette kan med fordel gjøres i sammenheng med kommunikasjon av en handlingsplan for å sikre en betryggende praksis på området.

Vår anbefaling er at Helse- og omsorgsetaten i Karmøy kommune prioriterer følgende områder:

7. Opplæring og kommunikasjon i Helse- og omsorgsetaten

I Helse- og omsorgsetaten er det, tilsvarende som i kommunen sentralt, et potensial for å systematisere kommunikasjon og opplæringen om informasjonssikkerhet og personvern. Dette for å sikre at alle får nødvendig informasjon, og at det er en enhetlig tilnærming til kommunikasjon om temaet. Anbefalingen bør sees i sammenheng med anbefaling 1.

8. Avklaring av roller og ansvar for etterlevelse av krav i personopplysningsloven i Helse- og omsorgsetaten

Det anbefales at roller og ansvar for etterlevelse av personvernregelverket i etaten tydeliggjøres, for å sikre at det er en enhetlig forståelse, og således redusere risikoen for brudd på regelverket. Det er særlig behov for å vurdere ansvarsfordeling mellom linjeledelsen og GDPR-gruppen i Etaten.

9. Profesjonalisering av Helse- og omsorgsetatens risikostyring

Det er et potensial for å profesjonalisere etatens risikostyring. Anbefalingen bør sees i sammenheng med anbefaling 3.

8. Uttalelse fra rådmannen

Anbefalingene som er kommet frem i rapporten var kjent i kommunen i forkant av forvaltningsrevisjonen, og rådmannen ser seg positiv til at administrasjonen og revisjonen kommer med sammenfallende vurderinger her.

Etter at det kom nye krav i personopplysningsloven er det blitt jobbet systematisk med å sikre at de formelle kravene blir oppfylt. Dette kommer også til uttrykk i forvaltningsrevisjonen. Arbeidet med å implementere ny praksis er et omfattende arbeid som krever systematikk og langsiktighet.

Rapporten viser at Karmøy kommune har forbedringsområder. Som forventet er det ikke funnet vesentlige mangler ved dagens praksis for hvordan kommunen har innrettet seg for å oppfylle kravene i den nye personopplysningsloven. Rådmannen opplever at sektor omsorg jobber systematisk med personvern. Dette bekreftes også av forvaltningsrevisjonens vurderinger.

Rådmannen takker for framlagt rapport og merker seg revisjonens vurdering av kommunens etterlevelse av personopplysningsloven. Rådmannen vil legge vekt på rapportens anbefalinger, og vil ha økt fokus på tre sentrale prinsipper som trekkes frem i rapporten:

- Kommunikasjon og opplæring
- Protokoll over behandlinger
- Risikostyring

Rapporten fremhever behovet for bedre kommunikasjon i kommunen. Dette er en kjent utfordring som det jobbes kontinuerlig med, og opprettelse av kommunikasjonsavdeling vil støtte opp om dette arbeidet. I forhold til rapportens resterende anbefalinger har administrasjonen allerede påbegynt et arbeid.

9. Vedlegg 1 Dokumentliste

- ✓ Reglement Informasjonssikkerhet og personvern
- ✓ Prosedyre for melding og håndtering av avvik
- ✓ Retting og sletting av personvernopplysninger
- ✓ Prosedyre for kontroll og revisjon av databehandlere
- ✓ Prosedyre for informasjon til den registrerte
- ✓ Prosedyre for protokoll over behandlinger
- ✓ Reglement – internkontroll og kontinuerlig forbedring
- ✓ Internkontroll og kontinuerlig forbedring
- ✓ Prosedyre for ledelsens gjennomgang og forbedringsplan
- ✓ Prinsipper for internkontroll og forbedringsarbeid
- ✓ Prosedyre for vurdering av DPIA
- ✓ Prosedyre for risikohåndtering
- ✓ Eksempel for gjennomføring av DPIA / personvernkonsekvensvurdering
- ✓ Oversikt over nano-kurs innen personvern
- ✓ Oversikt over andel som har gjennomført nano-kurs innen personvern

10. Vedlegg 2 Revisjonskriterier

10.1 Kommunesektorens organisasjon (KS) 2013: Rådmannens internkontroll

Kommuner og fylkeskommuner har et selvstendig ansvar for å føre kontroll med egen virksomhet.

De tre viktigste rådene til kommuner som vil forbedre sin internkontroll:

1. Internkontroll og kontrollaktiviteter må være basert på risikoanalyser
2. Internkontrollen må i større grad være en del av ordinær ledelse og virksomhetsstyring
3. Det er nødvendig med mer formalisering av internkontrollen

Den administrative ledelsen skal sikre at internkontroll er etablert og etterleves.

Ved styrking av internkontrollen er det viktig at medarbeidere på ulike nivåer forstår sin rolle, og at deres innsats er en del av et helhetlig arbeid. Både ledere og medarbeidere må være kjent med og forstå hvilket ansvar de har og hva de skal gjøre.

Gitt at målet er å integrere internkontrollens aktiviteter (risikovurderinger, kontrolltiltak, avvikshåndtering mv) i helheten, så bør også kommunikasjon og en del dokumentasjon av internkontroll gjøres innenfor samme helhet – f.eks. i årshjul, planlegging og rapporteringer. Dette gjelder selvsagt bare så langt det er hensiktsmessig, fortrinnsvis på overordnet/aggregert nivå, og detaljerte kartlegginger, prosedyrer, rapporter mv skal selvsagt ikke inngå i styringsdokumentene.

Dokumentasjon av internkontroll bør struktureres og helst samles på ett sted (felles).

For at internkontrollen skal være enhetlig bør man etablere felles metoder, maler og rapporteringer for hele kommunen.

10.2 Lov om behandling av personopplysninger (personopplysningsloven)

Kapittel 1. Personvernforordningen

§ 1.Gjennomføring av personvernforordningen

EØS-avtalen vedlegg XI nr. 5e (forordning (EU) 2016/679) 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) gjelder som lov med de tilpasningene som følger av vedlegg XI, protokoll 1 og avtalen for øvrig.

§ 4.Geografisk virkeområde

Loven og personvernforordningen gjelder for behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler i Norge, uavhengig av om behandlingen finner sted i EØS eller ikke.

Loven og personvernforordningen gjelder for behandling av personopplysninger om registrerte som befinner seg i Norge, og som utføres av en behandlingsansvarlig eller databehandler som ikke er etablert i EØS, dersom behandlingen er knyttet til

a) tilbud av varer eller tjenester til slike registrerte i Norge, uavhengig av om det kreves betaling fra den registrerte eller ikke, eller
b) monitorering av deres atferd, i den grad deres atferd finner sted i Norge.

§ 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.

§ 9.Behandling av særlige kategorier av personopplysninger uten samtykke for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål

Personopplysninger som nevnt i personvernforordningen artikkel 9 nr. 1 kan behandles uten samtykke fra den registrerte dersom behandlingen er nødvendig for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål og samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene for den enkelte. Behandlingen skal være omfattet av nødvendige garantier i samsvar med personvernforordningen artikkel 89 nr. 1.

Før det foretas behandling på grunnlag av første ledd, skal den behandlingsansvarlige rådføre seg med personvernombudet etter personvernforordningen artikkel 37 eller en annen som oppfyller vilkårene i personvernforordningen artikkel 37 nr. 5 og 6 og artikkel 38 nr. 3 første og annet punktum. Ved rådføringen skal det vurderes om behandlingen vil oppfylle kravene i personvernforordningen og øvrige bestemmelser fastsatt i eller med hjemmel i loven her. Rådføringsplikten gjelder likevel ikke dersom det er utført en vurdering av personvernkonsekvenser etter personvernforordningen artikkel 35.

§ 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.

Kapittel 5. Personvernombud

§ 18.Personvernombudets taushetsplikt

Personvernombud plikter å hindre at andre får adgang eller kjennskap til det de i forbindelse med utførelsen av sine oppgaver får vite om

a) noens personlige forhold
b) tekniske innretninger, produksjonsmetoder, forretningsmessige analyser og beregninger og forretningshemmeligheter ellers når opplysningene er av en slik art at andre kan utnytte dem i sin egen næringsvirksomhet
c) sikkerhetstiltak etter personvernforordningen artikkel 32
d) enkeltpersoners varsling om overtredelser av loven her.

Taushetsplikten gjelder ikke dersom personvernombudet får samtykke fra den opplysningene gjelder, til å legge dem frem, eller dette er nødvendig for gjennomføring av personvernombudets lovpålagte oppgaver.

Taushetsplikten gjelder også etter at personvernombudet har avsluttet tjenesten eller arbeidet. Opplysninger som nevnt i denne paragraf kan heller ikke utnyttes i egen virksomhet eller i tjeneste eller arbeid for andre.

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) (GDPR).

GDPR er innlemmet i personopplysningsloven. Avsnitt som har særlig relevans for forvaltningsrevisjon av etterlevelse av personvernregelverket i Karmøy kommune fremgår av teksten under.

Kapittel I Alminnelige bestemmelser

Artikkel 1.Formål og mål

1. Denne forordning fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger.
2. Denne forordning sikrer vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger.
3. Fri utveksling av personopplysninger i Unionen skal verken begrenses eller forbys av årsaker knyttet til vern av fysiske personer i forbindelse med behandling av personopplysninger.

Artikkel 2.Saklig virkeområde

1. Denne forordning får anvendelse på helt eller delvis automatisert behandling av personopplysninger og på ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register.

Kapittel II Prinsipper

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»).

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,

f. behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

Nr. 1 bokstav f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver.

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 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. Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art, som ledd i organets berettigede aktiviteter og med nødvendige garantier, forutsatt at behandlingen bare gjelder organets medlemmer eller tidligere medlemmer eller personer som på grunn av organets mål har regelmessig kontakt med det, og at personopplysningene ikke utleveres til andre enn nevnte organ uten de registrertes samtykke.
   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.

KAPITTEL III Den registrertes rettigheter

Avsnitt 1 Åpenhet og vilkår

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.

Avsnitt 2 Informasjon og innsyn i personopplysninger

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,
f. dersom det er relevant, det faktum at den behandlingsansvarlige akter å overføre personopplysninger til en tredjestat eller en internasjonal organisasjon og om hvorvidt Kommisjonen har truffet en beslutning om tilstrekkelig beskyttelsesnivå eller ikke, eller når det gjelder overføringene nevnt i artikkel 46 eller 47 eller artikkel 49 nr. 1 annet ledd, en henvisning til nødvendige eller passende garantier, hvordan man får tak i et eksemplar av dem, eller hvor de er gjort tilgjengelig.

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.

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.

Avsnitt 3 Retting og sletting

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.

Avsnitt 4 Rett til å protestere og automatiserte individuelle avgjørelser

Artikkel 22.*Automatiserte individuelle avgjørelser, herunder profilering*

Den registrerte skal ha rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende.

KAPITTEL IV Behandlingsansvarlig og databehandler

Avsnitt 1 Generelle forpliktelser

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.

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. …
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.

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.

2. Hver databehandler og, dersom det er relevant, databehandlerens representant skal føre en protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av en behandlingsansvarlig, og som skal inneholde:
    a. navnet på og kontaktopplysningene til databehandleren eller databehandlerne og til hver behandlingsansvarlig som databehandleren opptrer på vegne av, samt, dersom det er relevant, den behandlingsansvarliges eller databehandlerens representant og personvernombudet,
    b. kategoriene av behandling utført på vegne av hver behandlingsansvarlig,
    c. 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,
    d. 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.

Avsnitt 2 Personopplysningssikkerhet

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. …
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.
3. Meldingen nevnt i nr. 1 skal minst
    a. 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,
    b. inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes,
    c. beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
    d. 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:
    a. 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,
    b. 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,
    c. 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.

Avsnitt 3 Vurdering av personvernkonsekvenser og forhåndsdrøftinger

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.

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.

Avsnitt 4 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,
    b. den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandlingsaktiviteter som på grunn av sin art, sitt omfang og/eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte, eller
    c. den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandling i stor skala av særlige kategorier av opplysninger i henhold til artikkel 9 eller personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10.

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.

10.3 Datatilsynets Veileder - Internkontroll og informasjonssikkerhet

Ansvarlighet, internkontroll og informasjonssikkerhet

Personvernforordningen stiller krav til den behandlingsansvarliges ansvar. Det innebærer å sette i verk egnede tiltak, både tekniske og organisatoriske, for å sikre og påvise at personopplysninger behandles i samsvar med regelverket.

Dersom det blir behov for det, skal de tiltakene man har valgt endres og oppdateres. Dette kan oppsummeres som rutiner for oppfyllelse av virksomhetens plikter og de registrertes rettigheter, og rutiner og tekniske tiltak for informasjonssikkerhet.

Hva er internkontroll?

En virksomhet må forholde seg til og etterleve flere ulike regelverk. Disse kan for eksempel omhandle helse, miljø, sikkerhet, regnskap eller avgifter. Tilsvarende finnes det regelverk for hvordan personopplysninger skal behandles. De som fastsetter regelverk, forventer at virksomhetene har en systematisk tilnærming i etterlevelsen.

Først og fremst må man sette seg inn i de ulike bestemmelsene for å avgjøre hvilke som er relevante i egen virksomhet. Noen bestemmelser har spesiell relevans for ledelsen i virksomhetene, mens andre er ment å påvirke hvordan de ansatte kan utføre sitt arbeid. Det kan også være bestemmelser som gir andre personer eller grupper rettigheter og som virksomheten har plikt til å oppfylle.

For å ivareta krav om en systematisk tilnærming oppretter virksomhetene en internkontroll. Denne består gjerne av tre hovedelementer:

1. **Styrende elementer**, som i hovedsak retter seg mot ledelsen, herunder hvilke beslutninger og føringer de legger for internkontroll.
2. **Gjennomførende elementer**, som i hovedsak retter seg mot ansatte. Her finner man beskrivelse av rutiner som er tilpasset den enkeltes arbeidssituasjon.

3. **Kontrollerende elementer**, som bidrar til å fange opp avvik fra systemet og til at det gjennomføres periodiske gjennomganger.

Internkontroll kalles i ulike sammenhenger et kvalitetssystem, styringssystem eller ledelsessystem for etterlevelse av regelverk.

Hva er internkontroll etter personvernregelverket

Virksomheten må sikre en forsvarlig behandling av personopplysninger ved at man ivaretar den registrertes rettigheter og friheter, samtidig som man ivaretar virksomhetens mål ved behandlingen. Etter personvernforordningen (artikkel 24) innebærer det en forholdsmessighet hvor man ser på behandlingens art, omfang, formål og sammenheng, samt risikoene for fysiske personers rettigheter og friheter, og ut fra det gjennomfører egnede tekniske og organisatoriske tiltak. Internkontroll skal være ledelsens verktøy for å ivareta sitt ansvar og demonstrere etterlevelse etter personvernregelverket, og de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte. Tiltakene skal dokumenteres og oppdateres ved behov.

Det er ikke nødvendig eller hensiktsmessig å etablere en egen internkontroll for personvernregelverket dersom dere allerede har en internkontroll for andre regelverk eller for andre formål. Dere bør heller sørge for å utvide det eksisterende systemet med det som er påkrevd etter personvernregelverket.

Om informasjonssikkerhet

Personvernregelverket krever at personopplysninger skal beskyttes tilfredsstillende mot uberettiget innsyn og endringer. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene, når de har behov for dem.

Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har. Deretter gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende.

Dersom risikovurderingen avdekker manglende tiltak må det vurderes om nye tiltak skal iverksettes for å oppnå tilfredsstillende sikkerhetsnivå for personopplysningene. Kontrollrutiner må utarbeides og jevnlig følges, for å kontrollere at tiltakene blir fulgt opp og virker etter hensikten.

En slik fremgangsmåte som skissert ovenfor vil sammen med tilhørende rutiner kunne utgjøre virksomhetens styringssystem for informasjonssikkerhet. Dette systemet for informasjonssikkerhet vil være en sentral del av virksomhetens internkontroll. Det er utviklet standarder som beskriver hvordan styringssystem for informasjonssikkerhet skal etableres.

Hvordan gjennomføre internkontroll i praksis

Denne delen beskriver prosessen for å etablere internkontroll. Den beskriver hvilke oppgaver som må løses, hvilke plikter en virksomhet har, hvilke rutiner som må dokumenteres og aktiviteter som må gjennomføres.

- **Dette kapittelet inneholder følgende:**
- Skaff kunnskap
- Ledelsen har ansvaret
- Formålet med internkontrollen
- Få oversikt og vurder lovlighet, nødvendighet og proporsjonalitet
- Beskrive overordnede rammer
- Identifisere plikter
- Utarbeide rutiner

Skaff kunnskap

Virksomheten må selv ha et minimum av kunnskap, og sørge for å ha tilgang til nødvendig kunnskap om personopplysningsloven og personvernforordningen. Slik kunnskap er nødvendig for å kunne starte arbeidet med å etablere en internkontroll og tilfredsstillende informasjonssikkerhet. Virksomheten må videre identifisere de lovpålagte pliktene den skal overholde.

På våre nettsider finner du oppdatert og relevant informasjon som kan benyttes i arbeidet med internkontroll og informasjonssikkerhet.

Ledelsen har ansvaret

Ledelsen er ansvarlig for at det settes i gang aktiviteter for å etablere internkontroll i virksomheten. Den har et spesielt ansvar for å utarbeide policy, målsetning, identifisere forpliktelser, klarlegge intern organisering og ikke minst tydelig identifisere ansvar og myndighet.

Ledelsen har også ansvar for at det etableres rutiner og instrukser basert på vurderinger for risiko for rettigheter og friheter. Det må tas stilling til hvilke rutiner som er påkrevd for å sikre samsvar mellom den etablerte systematikken og aktivitetene som faktisk utføres i virksomheten.

Dokumentasjon over systemet for internkontroll skal være tilgjengelig for de ansatte i virksomheten og for Datatilsynet ved eventuell kontroll.

Formålet med internkontrollen

Ved å etablere internkontroll bør virksomheten oppnå:

1. bedre ivaretakelse av de registrertes rettigheter
2. bedre informasjonssikkerhet, informasjonskvalitet og effektiviseringsgevinst
3. system for kvalitetssikring av at offentlig regelverk følges
4. forsvarlig drift innenfor lovverket
5. fastsatte rutiner og instrukser som bidrar til at ledelsen sikrer at de ansatte arbeider i samsvar med virksomhetens mål og policy
6. at avvik blir oppdaget og håndtert
7. reduksjon i sjansen for alvorlige feil som skyldes manglende oppfølging av lovverket

Få oversikt, og vurder lovlighet, nødvendighet og proporsjonalitet

Virksomheten skal etablere og vedlikeholde en oversikt over alle behandlingene av personopplysninger. For å få en fullstendig oversikt, må man se på karakteristikker ved behandlingen og gjøre en vurdering proporsjonalitet og nødvendighet for å sikre at behandlingen er lovlig og at man ivaretar de registrertes rettigheter.

Internkontrollens struktur

Det er nyttig å etablere en struktur for internkontrollsystemet. I kapittelet "Internkontrollens struktur" finner dere forslag til struktur og dokumenter som kan opprettes i de ulike fasene - styrende dokumentasjon, gjennomførende dokumentasjon og kontrollerende dokumentasjon - og som vi vil vise til i den påfølgende teksten.

Beskrivelser, vurderinger og valg kan føres inn i styringsdokument for internkontroll. Disse beskrivelsene vil videre være grunnlag for å føre protokoll over behandlinger. Protokollen inkluderer blant annet oversikt over type behandlingsaktiviteter, kategorier av personopplysninger og registrerte, rettslig grunnlag og formål med behandlingene. Protokollen kan også inngå i styringsdokument for internkontroll. Dokumentasjonen bør oppdateres og gjennomgås jevnlig.

Oversikt over behandlingen er nødvendig for at virksomheten skal kunne ivareta pliktene sine. Oversikten danner også grunnlag for utarbeidelse av virksomhetens sikkerhetsmål og sikkerhetsstrategi, og vil være underlag ved risikovurderinger.
For å få en fullstendig oversikt over behandlingen, vurdere lovlighet, nødvendighet og proporsjonalitet, må man gå systematisk til verks og sørge for at beskrivelsene er tydelige:

Behandlingens art, omfang, formål og sammenheng

Beskriv behandlingens art, det vil si behandlingens iboende karakteristikk. Dette kan innebære beskrivelser av hva dere gjør eller planlegger å gjøre med personopplysningene, for eksempel hvordan personopplysningene skal samles inn, lagres og brukes, og hvem det skal behandles personopplysninger om.

Beskriv behandlingens omfang. Det omfatter blant annet kategorier av personopplysninger, antall registrerte involvert, volum av data, hvor hyppig er behandlingen, lagringstid og geografisk omfang.

Beskriv behandlingens formål, det vil si å beskrive tydelig hva personopplysningene skal brukes til.

Beskriv hvilken sammenheng eller kontekst behandlingen utføres i. Dette innebærer å se behandlingen i et større bilde, og beskrive alle interne og eksterne faktorer som kan påvirke forventninger eller konsekvenser. Beskriv for eksempel hvilke kilder som brukes for innhenting av personopplysninger, hvilken relasjon virksomheten har til de registrerte, hvilke forventninger de registrerte har til behandlingen og i hvilken grad de registrerte har kontroll over sine personopplysninger.

Kilder, mottakere og ansvarsforhold

Identifiser, avklar og dokumenter ansvarsforhold. Dette innebærer blant annet å klargjøre egen virksomhets rolle og ansvar knyttet til verdikjedene for behandling av personopplysninger i virksomheten. Dokumenter når virksomheten er behandlingsansvarlig eller databehandler.

Identifiser og dokumenter alle mottakere av personopplysninger. Dette omfatter deling internt i virksomheten, databehandlere, tredjeparter, eksterne virksomheter (private og offentlige myndigheter) og så videre. Gjennomgå formål, rettslig grunnlag og hvilke forhåndsregler som tas for å beskytte personopplysningene (taushetserklæringer, databehandleravtale, atferdsnormer, sikkerhetstiltak og så videre). Dersom personopplysninger overføres eller lagres i land utenfor EU/EØS, må det sikres at det foreligger mekanismer som tillater slik overføring (se artikkel 44-49 i personvernforordningen).

Dersom det tas i bruk tjenesteutsetting eller skytjenester, bør man se på Nasjonal sikkerhetsmyndighets temahefte «Sikkerhetsfaglige anbefalinger ved tjenesteutsetting» (pdf).

Vurdering av lovlighet, nødvendighet og proporsjonalitet

Virksomheten må undersøke om behandlingene er lovlige, at de valgene man tar er nødvendige og står i et rimelig forhold til formålene. Dere må ta utgangspunkt i prinsippene for behandling av personopplysninger. Beskrivelser, vurderinger og valg kan føres i styringsdokumentet for internkontroll.

Fastsette behandlingsgrunnlag: Det er ikke tillatt å behandle personopplysninger uten et rettslig grunnlag. Behandlingen skal være basert på lovlighet, rettferdighet og åpenhet (artikkel 5.1 bokstav a og artikkel 6 og 9).

Et rettslig grunnlag/behandlingsgrunnlag kan være samtykke, at det er nødvendig for avtale/kontrakt, en rettslig forpliktelse, vitale interesser, utøvelse av myndighet eller en berettiget interesse. Undersøk om det rettslige grunnlaget omfatter både egne formål og utlevering.

Vurder og kontroller behandlingsgrunnlagets gyldighet og rimelighet. Er det et tydelig skille mellom hvilke personopplysninger som er nødvendig for avtale og hva som skal baseres på samtykke? Hva er de forventede fordelene ved behandlingen for virksomheten, den registrerte og samfunnet for øvrig?

Vurder hvordan åpenhet ivaretas i behandlingen.

Identifiser formål: Det er ikke tillatt å behandle personopplysninger uten at det er definert et formål med behandlingen. Formål(ene) skal være spesifikt, uttrykkelig angitt og berettiget (artikkel 5.1 bokstav b). Det innebærer at formålet skal være klart definert og i samsvar med forventningene til de registrerte. Kan formålet oppnås med en mindre inngripende behandling og med anonyme eller pseudonyme alternativer?

Dataminimering: Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene (artikkel 5.1 bokstav c). Identifiser og vurder personopplysningene som skal behandles. Kan formålet oppnås ved å begrense innsamlingen av personopplysninger, med mindre detaljerte personopplysninger, uten fortrolige eller sensitive personopplysninger, med aggregerte eller pseudonyme personopplysninger?

Riktighet: Personopplysninger skal være korrekte og oppdaterte (artikkel 5.1 bokstav d). Vurder hvordan personopplysninger skal holdes korrekte og oppdaterte, med og uten den registrertes involvering. Har dere nødvendig funksjonalitet for å rette og slette uriktige personopplysninger? Har dere rutiner for å oppdage feil ved personopplysninger? Har dere rutiner for hvordan registrertes anmodning om retting og sletting av personopplysninger skal håndteres?

Lagringsbegrensning: Personopplysninger skal slettes eller anonymiseres når formålet er oppnådd (artikkel 5.1 bokstav e). Avklar lovlig oppbevaringstid og slettefrister for alle typer personopplysninger som virksomheten behandler. Det innebærer å ta stilling til avveiinger som omfatter formålet med behandlingen, virksomhetens behov og andre rettslige krav som regulerer oppbevaringsrett og oppbevaringsplikt. Utarbeid nødvendige rutiner og tekniske løsninger for nødvendig sletting, anonymisering eller pseudonymisering.

Integritet og konfidensialitet: Virksomheten skal sørge for tilstrekkelig sikkerhet for personopplysningene ved bruk av tekniske og organisatoriske tiltak (artikkel 5.1 bokstav f). Det innebærer å sikre opplysningene mot uautorisert eller ulovlig behandling, og mot utilsiktet tap, ødeleggelse eller skade.

Ansvar: Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at prinsippene overholdes (artikkel 5.2).

Beskrive overordnede rammer

Denne delen omfatter ledelsens begrunnelse for behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi i virksomheten. Begrunnelsen og de overordnede føringene kan beskrives i styringsdokumentet for internkontroll. Begrunnelsene omhandler virksomhetens behov for å behandle personopplysningene slik at den kan ivareta sine forpliktelser, herunder levere sine tjenester eller følge opp sine ansatte. De overordnede føringene er krav og plikter som virksomheten blir underlagt fordi den behandler personopplysninger. Slike krav og plikter kan blant annet følge av personvernlovgivningen, av pålegg fra Datatilsynet eller av annen lovgivning.

Andre føringer er sikkerhetsmål og sikkerhetsstrategier. Disse legger begrensninger på bruken av IKT for å sikre tilfredsstillende sikkerhet for personopplysningene. Samme dokument kan også inneholde føringer som krav til hendelseshåndtering, egenkontroll, avviksbehandling og ledelsens gjennomgang.

Identifisere plikter

Behandling av personopplysninger medfører plikter for virksomheten. Ulike opplysninger og ulike formål gjør at ingen virksomheter er like. Hver virksomhet må derfor identifisere plikter og tilpasse internkontroll og informasjonssikkerhetstiltak til sin organisasjon. Dette gjøres med utgangspunkt i behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoen for de registrertes rettigheter og friheter.

Prinsippene for behandling av personopplysninger legger føringer for hvordan personopplysninger skal behandles. Virksomheten må identifisere hvilke plikter den har og gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen (artikkel 24).

De ulike pliktene for behandlingsansvarlig og databehandlere er beskrevet i kapittel IV i personvernforordningen. Nedenfor nevner vi noen av disse pliktene med lenker til mer informasjon.

1. Innebygd personvern og personvern som standardinnstilling (artikkel 25) – Veileder om programvareutvikling med innebygd personvern
2. Databehandler (artikkel 28) – Veileder om databehandleravtaler
3. Protokoller over behandlingsaktiviteter (artikkel 30) – Veiledning og mal for protokoll
4. Sikkerhet ved behandlingen (artikkel 32)
5. Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten (artikkel 33) og informasjon til den registrerte om brudd på personopplysningssikkerheten (artikkel 34) – Avvikshåndtering
6. Vurdering av personvernkonsekvenser (DPIA) (artikkel 35) – Veileder om vurdering av personvernkonsekvenser
7. Forhåndsdrøftinger (artikkel 36)
8. Personvernombud (artikkel 37-39)

9. Atferdsnormer/bransjenormer (artikkel 40)
10. Sertifisering (artikkel 42)
11. Overføringer av personopplysninger til tredjestater og internasjonale organisasjoner (artiklene 44-49)

Virksomheten må identifisere hvilke rettigheter og friheter for de registrerte som gjør seg gjeldende på grunn av virksomhetens behandling av personopplysninger. Virksomheten har plikt til å oppfylle disse rettighetene (beskrevet i artiklene 12-22) Vi har laget en samleside med oversikt over rettighetene. Med de registrertes friheter mener vi blant annet friheter etter Den europeiske menneskerettskonvensjonen (EMK), slik som retten til privatliv og kommunikasjonsvern, retten til ikke å bli diskriminert, tanke-, tros- og religionsfrihet, ytrings- og informasjonsfrihet. Vurder hvordan de registrertes rettigheter og friheter skal ivaretas.

Det finnes også nasjonale bestemmelser i personopplysningsloven som er presiseringer og unntak fra hovedregler i personvernforordningen.

Utarbeide rutiner

Personvernforordningen stiller krav til internkontroll i form av egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen. Tiltakene skal gjennomgås på nytt og skal oppdateres ved behov.

Utarbeid rutiner som er nødvendige for oppfyllelse av virksomhetens plikter og de registrertes rettigheter. Her nevnes noen nødvendige rutiner, samt hvordan rutinene kan utformes. Alle rutiner vil imidlertid ikke være relevante for alle virksomheter. En risikovurdering kan dessuten vise at virksomheten har behov for andre rutiner enn dem som er listet opp.

Eksempler på rutiner for håndtering av personopplysninger:

- Iverksettelse og opphør av behandling
- Informasjon (rettferdig og gjennomsiktig behandling, artikkel 12, 13 og 14)
- Innhenting og kontroll av samtykke (artikkel 7 og 8)
- Innsyn (artikkel 15)
- Dataportabilitet (artikkel 20)
- Retting og sletting (artikkel 16, 17 og 19)
- Begrensning (artikkel 18 og 19)
- Protestere (artikkel 21)
- Særskilte regler for automatiserte avgjørelser (artikkel 22)
- Utlevering av personopplysninger til andre
- Overføring til tredjestater (artikkel 44-49)

Rutinene bør utformes etter en felles mal. Rutinene blir da enklere å bruke, og det blir lettere å vurdere om de er fullstendige.

Følgende mal kan benyttes for utforming av rutiner:

- Hvorfor skal rutinen utarbeides, hva er hensikten med den?
- Hvem er ansvarlig for å utføre de ulike aktivitetene?
- Hva skal utføres av de ulike ansvarlige?
- Hvordan skal aktivitetene utføres?
- Når skal de ulike aktivitetene utføres, eller under hvilke betingelser?
- Hva er forventet resultat ved utførelse av rutinen?

Iverksette styringssystem for informasjonssikkerhet

Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. Personopplysninger kommer i mange former. De kan trykkes eller skrives på papir, lagres elektronisk, overføres via post eller elektroniske media, eller formidles muntlig. Uansett hvordan informasjonen formidles og lagres, skal den alltid beskyttes på en tilfredsstillende måte.

Informasjonssikkerhet omfatter her beskyttelse av:

- Konfidensialitet – at informasjonen ikke blir kjent for uvedkommende
- Integritet – at informasjonen ikke blir endret utilsiktet eller av uvedkommende
- Tilgjengelighet – at informasjonen er tilgjengelig for autoriserte ved behov
- Robusthet – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser

Organisasjoner og deres informasjonssystemer står overfor en stadig lengre rekke av sikkerhetstrusler, for eksempel datasvindel, spionasje, sabotasje og hærverk. Trusselaktører tar kontinuerlig i bruk nye verktøy og metoder som krever at alle virksomheter jevnlig holder seg oppdatert, kjenner til nye trusler og sårbarheter, og vurderer om man har etablert tilstrekkelig sikring.

I personvernregelverket understrekes det at arbeidet med informasjonssikkerhet er en kontinuerlig prosess. Det stilles blant annet krav til å sikre vedvarende robusthet i tillegg til konfidensialitet, integritet og tilgjengelighet. Det betyr blant annet at virksomheten plikter å ta hensyn til den tekniske utviklingen, altså hvilken teknologi som er tilgjengelig på markedet til enhver tid. Det betyr at den teknologien som var akseptabel for å sikre virksomhetens behandlinger i fjor, ikke nødvendigvis er akseptabel i år.

For å sørge for tilstrekkelig sikkerhet står det i artikkel 32 at virksomheten må ta hensyn til behandlingens art, formål, omfang og sammenheng, hva som finnes av tilgjengelig teknologi, kostnader ved gjennomføring, og hva sannsynligheten og konsekvensen er for at uønskede eller ulovlige hendelser skal inntreffe. Informasjonssikkerhet oppnås ved hjelp av tekniske og organisatoriske tiltak. Sikkerhetstiltakene og informasjonssystemet skal dokumenteres og inngå som en del av internkontrollen i virksomheten.

Ved innføring av internkontroll må virksomheten først identifisere hvilke personopplysninger som behandles. Deretter må det utarbeides en risikovurdering.

Dokumentasjon og oppbygging av styringssystem for informasjonssikkerhet

Personvernforordningen stiller krav til tilstrekkelig informasjonssikkerhet ved innføring av egnede tekniske og organisatoriske tiltak. Vi anbefaler at man følger anerkjente standarder som beskriver styringssystem for informasjonssikkerhet, for eksempel "ISO/IEC 27001– Ledelsessystem for informasjonssikkerhet". Man kan også bruke rammeverk og veiledere som er utviklet av andre organisasjoner, slik som Direktoratet for forvaltning og IKT (Difi) og Nasjonal sikkerhetsmyndighet (NSM).

Nedenfor går vi gjennom noen viktige elementer som bør være med i et styringssystem for informasjonssikkerhet.

Sikkerhetsmål

Sikkerhetsmålene omfatter ledelsens beslutninger om hva IKT skal brukes til i virksomheten og hvordan den skal benyttes for å nå virksomhetens øvrige mål. Konkrete sikkerhetsmål vil slik utgjøre en del av virksomhetens beskrivelse av sin totale målsetning. Sikkerhetsmålene bør i størst mulig grad være målbare, men dette er ikke alltid enkelt. Uansett skal de være retningsgivende for strategien.

Sikkerhetsstrategi

Sikkerhetsstrategien skal omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette går på fordeling av arbeidsoppgaver mellom ledelse og driftspersonell, og beslutning om eventuelt å ta i bruk eksterne leverandører i sikkerhetsarbeidet. Forholdet mellom ledelse, driftspersonell, sikkerhetspersonell og den enkelte bruker må avklares her. Sikkerhetsstrategien skal gjøre rede for organisatoriske og tekniske strategiske valg, og må være utformet på en måte som gjør at de ansatte forstår hva ledelsen har bestemt. Strategien beskriver hvilke virkemidler virksomheten velger å bruke for å nå målene. Det kan velges ulike strategier for å tilfredsstille samme mål.

Ledelsens gjennomgang

Ledelsen skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Ledelsen skal kontrollere at disse er i samsvar med virksomhetens behov og eventuelt oppdatere mål, strategi og organisering. Gjennomgangen utføres etter rutine beskrevet i ledelsens gjennomgang.

I ledelsens gjennomgang av informasjonssystemet kan blant annet følgende vurderes:

- Resultater fra sikkerhetsrevisjoner og kontroller utført av offentlig myndighet
- Endringer med betydning for drift av informasjonssystemet eller for informasjonssikkerheten, herunder endringer i offentlige sikkerhetskrav, endringer i personopplysninger som virksomheten skal behandle, endringer i trusselbildet som blant annet beskrevet i rapport fra utførte risikovurderinger
- Om informasjonssystemet bør endres, eksempelvis som følge av ønske om ny funksjonalitet
- Overordnet behandling av alvorlige avvik og hendelser

Organisering

Det må klargjøres roller og ansvar knyttet til personvern og sikkerhet internt i virksomheten. Det inkluderer for eksempel hva som ligger i linjeansvar og hva som ligger i nøkkelroller som personvernombud, personvernrådgiver, sikkerhetsleder, IKT-ansvarlig, HR-ansvarlig, prosjektledere, produkteiere, systemeiere, systemforvaltere mv. Klare ansvars- og myndighetsforhold etableres med utgangspunkt i beslutninger tatt av virksomhetens ledelse. Rolle- og ansvarsfordeling skal være dokumentert.

I mindre organisasjoner kan det være samme person som ivaretar ulike oppgaver. For større organisasjoner lages et organisasjonskart som viser de nevnte funksjonene og deres plassering i forhold til ledelsen og virksomheten for øvrig.

Akseptabelt risikonivå / toleransenivå for sikkerhet

Risikovurdering handler om å identifisere konsekvenser ved ulike hendelser eller scenarier, og å vurdere hvor sannsynlig eller lett en uønsket hendelse kan inntreffe. Det er virksomhetens ledelse som avgjør hvor stor risiko (risikoappetitt) virksomheten skal ta ved ulike scenarier. Dette kalles toleransenivå for sikkerhet. Toleransenivå gir føringer for hvilke tiltak og ressurser som må settes inn for at behandlingen ikke skal overskride det definerte toleransenivået.

Beslutning om akseptabelt risikonivå skal blant annet uttrykkes i virksomhetens sikkerhetsmål. Sikkerhetsmålet skal, på et overordnet nivå, beskrive formålet med bruken av IKT og angi sikkerhetsbehov med hensyn til konfidensialitet, integritet, tilgjengelighet og robusthet. Det er også nødvendig med en detaljert beskrivelse av akseptabelt risikonivå. Denne beskrivelsen bør angi hvilke personopplysninger og behandlinger som berøres, hendelser med betydning for personvernet og akseptable nivåer for sannsynlighet og konsekvens. Beskrivelsen må angi prioritering mellom forskjellige sikkerhetsbehov og, på overordnet nivå, beskrive risikoreduserende tiltak.

Noen scenarier vil ha nulltoleranse for risiko, mens for andre kan virksomheten bestemme seg for å ta en viss risiko. Detaljert beskrivelse av akseptabelt risikonivå skal inngå i underlag for gjennomføring av risikovurdering.

Risikovurderinger og sikkerhetstiltak

Risikovurderinger og etablering av tekniske og organisatoriske tiltak for å oppnå et tilfredsstillende sikkerhetsnivå er grunnleggende krav til virksomhetens informasjonssikkerhet. Risikovurderingen må ta høyde for hvilke risikoer som er forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller uautorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

En risikovurdering begynner med en kartlegging av verdier som bør sikres. Personvernregelverket definerer personopplysninger som en verdi. Det bør gjøres en trusselvurdering av hvilke aktører som kan være interessert i verdiene og hvilke angrepsvektorer de ulike trusselaktørene benytter. Deretter gjøres en vurdering av om verdiene er sårbare for de gitte truslene. Standarder for informasjonssikkerhet kan bidra til å avdekke sårbarheter og dermed også krav som må stilles til sikkerhet.

Resultatet av risikovurderingen vurderes opp mot toleransenivå for sikkerhet. Dersom risikonivået er høyere enn fastlagt nivå for akseptabel risiko, skal det iverksettes tiltak for å redusere risikoen. Det må også fastsettes hvem som er ansvarlig for tiltaket og settes en frist for implementering. I artikkel 32 i personvernforordningen nevnes noen tiltak:

1. Pseudonymisering og kryptering av personopplysninger
2. Evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i system og tjenester som behandler personopplysninger
3. Evne til å gjenopprette tilgjengelighet og tilgang til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse
4. En prosess for regelmessig testing, analysering og vurdering av hvor effektive de tekniske og organisatoriske sikkerhetstiltakene er.

Både den behandlingsansvarlige og databehandleren skal treffe tiltak for å sikre at de som behandler personopplysninger i, eller på vegne av, virksomheten, kun behandler personopplysninger på instruks fra den behandlingsansvarlige. Dette innebærer blant annet at man sørger for å ha tilgangsstyring basert på tjenstlig behov, taushetserklæringer, sikkerhetsinstrukser, opplæring i rutiner og bruk, og databehandleravtaler. Dette er for å sikre at den behandlingsansvarlige har kontroll over behandlingen og dermed kan forsikre seg om at virksomheten etterlever personvernregelverket.

Rutiner for informasjonssikkerhet

Virksomheten skal konfigurere informasjonssystemet (infrastruktur, nettverk, servere, programvare mv.) slik at tilfredsstillende informasjonssikkerhet oppnås etter risikovurdering og beslutninger om sikkerhetstiltak. Lag en beskrivelse av informasjonssystemet.

Det er i tillegg viktig at man tar hensyn til brukersikkerhet, lager instrukser for ulike typer roller og gir opplæring i disse. Instruksene dokumenteres og kan deles opp i sikkerhetsinstrukser for bruker, leder og sikkerhetsansvarlig.

For å sørge for sporbarhet er det viktig å logge autorisert bruk og forsøk på uautorisert bruk. Det er imidlertid viktig å være klar over at personopplysninger som fremkommer som følge av logging for drifts- og sikkerhetsformål ikke senere kan benyttes for å overvåke eller kontrollere enkeltpersoner. Hensikten med logging av autorisert bruk er å i ettertid kunne spore hvem som gjorde hva med hvilke personopplysninger, og på hvilket tidspunkt. Rutine for logging beskrives i driftsrutiner. Loggfiler og formater beskrives i dokumentasjonen av informasjonssystemet.

Organisatoriske tiltak vil kunne beskrives i ulike dokumenter, slik som informasjonshåndteringsrutine, sjekkliste nyansatt / ansatte som slutter, og taushetserklæring. Tekniske tiltak vil kunne skildres i dokumentasjon av informasjonssystemet, driftsrutiner, beredskapsplan og fysisk sikkerhet.

Våre nettsider inneholder noe informasjon om sikring av personopplysninger, slik som kryptering, bruk av sterk autentisering og anonymisering.

Vi vil i tillegg anbefale et par eksterne sider for god veiledning om sikring av henholdsvis IKT-systemer og personopplysninger:

- Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet. Disse grunnprinsippene definerer hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser. Grunnprinsippene beskriver hva en virksomhet bør gjøre for å sikre et IKT-system. De beskriver også hvorfor det bør gjøres, men ikke hvordan.
- Den franske datatilsynsmyndigheten (CNIL) sin veileder «Security of Personal Data».

Oppfølging og opplæring

Arbeidet med internkontroll er en kontinuerlig prosess. Virksomheten må sørge for å kunne håndtere avvik, kontrollere at rutiner og tiltak brukes og fungerer etter hensikten. Etter at internkontrollen er etablert og forankret, må man sørge for at den gjøres kjent og etterleves blant de ansatte i virksomheten.

Avvikshåndtering

Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på informasjonssikkerheten, skal virksomheten iverksette avviksbehandling. Formålet med avviksbehandling er å lukke avviket så raskt som mulig, gjenopprette normaltilstand og hindre gjentakelse. Dersom det ikke er samsvar mellom fastlagte rutiner og hvordan personopplysninger håndteres eller informasjonssystemet benyttes, skal resultatet fra avviksbehandlingen brukes som grunnlag ved gjennomgang og endring av aktuelle rutiner.

Avviksbehandling består av:

- Å oppdage avviket.
- Kartlegge årsaken til og omfanget av avviket så langt det er mulig.
- Rapportering utføres normalt av den medarbeideren som oppdager avviket. Avviket rapporteres til virksomhetens sikkerhetsansvarlig eller etter annen intern organisering.
- Iverksettelse av strakstiltak, blant annet med det formål å avgrense eventuelle følgeskader.
- Vurdere om det er et brudd på personopplysningssikkerheten og vurdere risikoen for de registrertes rettigheter og friheter.
- Iverksettelse av korrigerende tiltak for permanent å gjenopprette normaltilstand. Vurdering av hvorvidt korrigerende tiltak fungerer etter sin hensikt.

Avviksbehandling skal dokumenteres i en rapport som inneholder opplysninger om selve avviket, gjennomførte strakstiltak, iverksatte korrigerende tiltak, resultater fra evaluering av det korrigerende tiltakets effekt over tid, samt opplysninger om hvilke medarbeidere som har vært involvert i behandling av avviket.

Dersom det har vært et brudd på personopplysningssikkerheten og det er en risiko for fysiske personers rettigheter og friheter, skal Datatilsynet varsles.

Dersom det har vært et brudd på personopplysningssikkerheten og det er en høy risiko for fysiske personers rettigheter og friheter, skal også de registrerte varsles.

Sikkerhetsrevisjon og egenkontroll

Virksomheten skal kontrollere at rutinene for håndtering av personopplysninger brukes og fungerer etter hensikten. Virksomheten må jevnlig teste, vurdere og evaluere hvor effektive sikkerhetstiltakene er. En sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak, og bruk av sikkerhetsparter og databehandlere.

Sikkerhetsrevisjon består vanligvis av egenkontroller, internrevisjon og revisjon av eksterne parter. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik. Resultatet fra sikkerhetsrevisjon skal dokumenteres og være en del av ledelsens gjennomgang.

Rutiner for rapportering og forslag til tiltak

Det er viktig å innføre faste rutiner for å forbedre internkontrollen. Det bør derfor innføres rutiner for å lære av uønskede hendelser, dokumentere erfaring og forbedre arbeidsprosessene slik at færrest mulig hendelser oppstår i fremtiden.

Virksomheten skal ha rutine for rapportering og mal for rapport til ledere og ansvarlige fra sikkerhetshendelser, avvikshåndtering og egenkontroll. Rapporten skal også omfatte erfaringer som er gjort og forslag til forbedringer, både tekniske tiltak og prosessforbedringer.

Opplæring

Målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt, og at de er gitt mulighet til å etterleve dette i sitt daglige arbeid. Opplæring bør være tilpasset ulike målgruppers behov for opplæring og fordeles over tid. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.

Opplæring i internkontroll og informasjonssikkerhet

Før ansatte i organisasjonen og eventuelle tredjepartsbrukere får tilgang til informasjon eller tjenester, bør de få hensiktsmessig opplæring. Dette omfatter krav til internkontroll og informasjonssikkerhet, juridisk ansvar og interne sikringstiltak, så vel som opplæring i riktig bruk av informasjonssystemer. Dette inkluderer for eksempel innloggingsprosedyrer, bruk av programvare, sikkerhetsinstruks, og rapportering av avvik. I tillegg bør de får regelmessig oppdatering i organisasjonens policy og rutiner.

Taushetserklæring

Taushetserklæringer brukes for å gjøre oppmerksom på at det forekommer konfidensiell informasjon i virksomheten. De ansatte skal undertegne en slik erklæring samtidig med ansettelseskontrakten. Taushetserklæringen oppbevares i den ansattes personalmappe under hele ansettelsesforholdet.

Midlertidig ansatte og tredjepartsbrukere som ikke allerede er dekket av eksisterende kontrakt med taushetserklæring, bør undertegne en tilsvarende erklæring før de får tilgang til informasjonssystemer. Betingelsene og ansettelsesvilkårene bør opplyse om den ansattes ansvar for informasjonssikkerhet. Der det er relevant bør dette ansvaret også gjelde i en nærmere spesifisert periode etter at ansettelsesforholdet er avsluttet.

Taushetserklæringer bør gjennomgås på nytt når ansettelsesforholdet endres, særlig når ansatte skal forlate organisasjonen, eller kontrakter utløper.

Personvernombud

For virksomheten kan det være en stor fordel å ha en bestemt person å henvende seg til med spørsmål rundt behandling av personopplysninger knyttet til sin virksomhet. Personvernforordningen styrker ordningen med personvernombud. Regelverket lovfester hvilken rolle og hvilke oppgaver ombudet skal ha, og gjør ordningen obligatorisk for mange virksomheter.

Internkontrollens struktur

Det er nyttig å etablere en struktur for internkontrollsystemet. Dette gjør det lettere for aktørene som skal bidra i prosessen til å forstå hvilken funksjon systemet skal ha. Dokumentasjon av internkontrollsystemet skal vise den reelle situasjonen i virksomheten. Berørte parter bør derfor delta i utformingen.

Noen ganger medfører innføring av nytt regelverk at rutiner og instrukser må endres. Det er viktig at dette faktisk skjer i virksomheten og ikke bare i systembeskrivelsen.

I neste kapittel finner dere maler og eksempler som kan lastes ned og benyttes i arbeidet med dokumenteringen av internkontrollsystemet.

Styrende dokumentasjon

Styrende dokumentasjon gir en systembeskrivelse som inneholder policy og målsetning, identifiserte krav og plikter, intern organisering, ansvar og myndighet. Styrende dokumentasjon er overordnet i sin form og er spesielt ledelsesorientert.

Styrende dokumentasjon bør inneholde:

1. virksomhetens mål og retningslinjer for vern av personopplysninger. Se spesielt personvernforordningen artikkel 1.
2. identifisering av at tiltenkt lagring og behandling av personopplysninger samsvarer med lovens grunnkrav, se artikkel 5 og 6 i personvernforordningen. Det legges spesielt vekt på saklig behov og konkret definering av formål, herunder at opplysningene som lagres samsvarer med formålet.
3. identifisering av hvilke generelle forpliktelser som er relevant for virksomheten, se artikkel 24-43 i personvernforordningen
4. organisering av virksomheten der intern delegering av ansvar og myndighet skal være entydig definert, se spesielt artikkel 24, 26, 28, 32, 37-39.
5. beskrivelse av hvordan virksomheten ivaretar informasjonssikkerheten. Se artikkel 32-34.

6. beskrivelse av hvordan ledelsen vil sørge for at virksomhetens aktiviteter er i samsvar med kravene i regelverket. En slik beskrivelse vil normalt ende opp i behov for gjennomførende dokumentasjon og kontrollerende dokumentasjon.

Eksempler på dokumentasjon:

- Styringsdokument internkontroll
- Sikkerhetsmål og sikkerhetsstrategi
- Rutine for ledelsens gjennomgang
- Organisering

Gjennomførende dokumentasjon

Gjennomførende dokumentasjon beskriver de organisatoriske og tekniske tiltak som er foreslått som følge av at virksomheten har vurdert risiko for rettigheter og friheter, for eksempel tiltak for å ivareta ulike rettigheter for de registrerte, tiltak for innebygd personvern, og tiltak for å oppnå tilstrekkelig informasjonssikkerhet.

Det er spesielt viktig å entydig definere hvem som har ansvaret for hva. Gjennomførende dokumentasjon vil i volum ofte utgjøre den største delen av internkontrollsystemet.

Gjennomførende dokumentasjon bør inneholde:

1. rutiner og prosedyrer
2. arbeidsinstrukser

Gjennomførende dokumentasjon er et knippe av mekanismer som skal sikre at aktiviteten i virksomheten samsvarer med virksomhetens definerte mål og retningslinjer for personvern og reglene for øvrig. I forhold til ansatte i virksomheten kan gjennomførende dokumentasjon være et sett med interne kjøreregler som sikrer at virksomheten ikke begår lovbrudd med noen av sine aktiviteter.

Eksempler på dokumentasjon:

- Rutiner for innhenting av samtykke, å gi informasjon og innsyn, å sørge for retting, sletting, begrenset behandling, gi adgang til å protestere, dataportabilitet, at automatiserte avgjørelser er lovlig og ivaretagelse av særskilte rettigheter for beskyttelse av barns personvern.
- Risikovurdering
- Beskrivelse av informasjonssystem
- Sikkerhetstiltak, for eksempel tilgangskontroll, logging, informasjonshåndteringsrutine, sjekkliste for nyansatte, sjekkliste for ansatte som slutter, taushetserklæring
- Fysisk sikring
- Driftsrutiner
- Beredskapsplan
- Sikkerhetsinstrukser for brukere, ledere og sikkerhetsansvarlig

Kontrollerende dokumentasjon

Kontrollerende dokumentasjon er dokumenter som har til formål å verifisere at aktivitetene har foregått i samsvar med fastsatte rutiner og instrukser. Eksempler er rapporter, sjekklister og logg. Kontrollerende dokumentasjon kan betraktes som et «sikkerhetsnett» som bidrar til at styringsdokumentene følges og at eventuelle avvik lettere oppdages. Dokumentene skal ikke være statiske, men endre seg i tråd med virksomhetens utvikling og den rettslige utvikling.

Kontrollerende dokumentasjon bør inneholde:

1. sjekklister
2. skjema for avviksrapportering
3. rapporter
4. logg

Kontrollerende dokumentasjon består ofte av to deler: En del som brukes under interne revisjoner og en del som brukes i det daglige arbeidet. Skjema for avviksrapportering er for eksempel ment til bruk

dersom det oppdages aktiviteter eller hendelser som ikke samsvarer med fastlagte rutiner og/eller instrukser, og brudd på personopplysningssikkerheten.

Det er et klart skille mellom gjennomførende og kontrollerende dokumentasjon. Det første skal sikre at aktivitetene er i samsvar med mål og retningslinjer. Det siste skal bidra til at avvik fra mål og retningslinjer oppdages og rettes.

Eksempler på dokumentasjon:

- Ledelsens gjennomgang
- Avvikshåndtering
- Egenkontroll
- Sikkerhetsrevisjon
- Oppfølging av databehandlere, inkludert sikkerhetsrevisjon

10.4 Norm for informasjonssikkerhet og personvern innen helse- og omsorg

Om Normen

1.1 Bakgrunn for Normen

Normen er en bransjenorm utarbeidet og forvaltes av organisasjoner og virksomheter i sektoren med sikte på å bidra til tilfredsstillende informasjonssikkerhet og personvern hos den enkelte virksomhet og i sektoren generelt, samt å bidra til at det etableres mekanismer hvor virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Personvern- og helselovgivningen stiller krav til informasjonssikkerhet og personvern. Disse kravene gjelder uavhengig av Normen, og aktuelle tilsynsmyndigheter (særlig Datatilsynet og Helsetilsynet) kan kontrollere den enkelte virksomhets etterlevelse av det til enhver tid gjeldende regelverk. Personvern- og helselovgivningen stiller også en rekke andre krav til behandling av helse- og personopplysninger enn det som er tema for Normen, f.eks. flere problemstillinger rundt sekundærbruk, spesifikke krav til registre som har egne forskrifter, rettsgrunnlag for behandling av helse- og personopplysninger samt plikt til og krav til journalføring. I tillegg vil også blant annet den kommende sikkerhetsloven vil kunne få betydning.

Normen stiller krav som detaljerer og supplerer gjeldende regelverk. Normens krav er krav som helsetjenesten mener er sentrale for sektorens tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern.

Normen er en selvreguleringsmekanisme som kan benyttes av alle aktører i helse- og omsorgssektoren. Overholdelse av kravene i Normen kan brukes for å påvise at virksomhetens forpliktelser etter regelverket overholdes. Gjennom avtale kan aktørene i sektoren forplikte seg til å følge kravene i Normen. Slik avtale gir andre virksomheter grunnlag for å innrette seg i tillit til at vedkommende virksomhet har tilfredsstillende informasjonssikkerhet og personvern.

Normen har krav som dekker de fleste områdene innen informasjonssikkerhet og personvern; mennesker, prosesser og teknologi. Normen har også støttedokumenter i form av veiledningsmateriell. Dette omtales videre i kap. 6.2

1.2 EUs personvernforordning (GDPR)

Personopplysningslovens § 1 gjennomfører EUs personvernforordning (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. Personvernforordningen er implementert i norsk lovgivning med grunnlag i Norges forpliktelser etter EØS-avtalen.

I versjon 5.3 av Normen er enkelte artikler fra forordningen innarbeidet. Det vil derfor være ulikt fra kapittel til kapittel hvor stor tilpasning som er gjort. Alle krav i Normen er gjennomgått med tanke på å sikre at det ikke er motstrid mellom Normen og den nye personopplysningsloven.

Tiltak for å sikre personopplysninger, herunder det som i personvernforordningen kalles personopplysningssikkerhet, har stort fokus forordningen. Tiltakene skal være "egnede". Dette betyr at for å finne de riktige tiltakene så må bl.a. både opplysningenes egenart, informasjonsbehandlingens omfang og egenarten til de som behandler opplysningene tas hensyn til. Tiltakene skal velges basert på risikovurderinger og tiltakene skal være forholdsmessige. Dette kan bety at en liten virksomhet som behandler personopplysninger i lite omfang bør ha andre tiltak enn en større virksomhet som behandler et større omfang av personopplysninger.

1.3 Formål

Formålet med Normen er å bidra til å sikre at en virksomhet som etterlever og innretter seg etter Normen har egnede tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger. De som samhandler med en virksomhet som har forpliktet seg til å innrette seg etter Normens krav, skal kunne stole på at denne virksomheten har egnede tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger.

Normen skal bidra til at ansatte, pasienter og brukere sikres et godt personvern.

Normen er ment å være et hjelpemiddel i den enkelte virksomhets arbeid med informasjonssikkerhet og personvern.

Normen skal, innenfor, lovverkets rammer, søke en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet. Normen skal bidra til å understøtte gode helsetjenester, god pasientsikkerhet, de ansattes personvern, og en aktiv pasientrolle. Med en aktiv pasientrolle menes at pasienten og brukerens rettigheter til egne helseopplysninger ivaretas, men også utviklingen der digitale tjenester etablerer kontakt mellom helsepersonell og innbyggere, pasienter og brukere, og derigjennom bidrar til større delaktighet.

1.4 Målgruppe – hvem Normen gjelder for

Normen gjelder for enhver virksomhet som ved avtale har forpliktet seg til å følge Normen

1.5 Virkeområde – hva Normen regulerer

Normen beskriver og stiller krav til virksomhetenes arbeid med informasjonssikkerhet og personvern for helse- og personopplysninger som behandles i forbindelse med yte, administrere og kvalitetssikre helsehjelp. Normen angir hvilke organisatoriske og tekniske tiltak som anses egnede for å oppnå tilfredsstillende informasjonssikkerhet og personvern for slike behandlinger av helse- og personopplysninger

En virksomhet håndterer i tillegg personopplysninger om egne ansatte. Normens sikkerhetskrav gjelder ikke direkte i denne sammenhengen, men virksomheten skal ivareta de ansattes personvern iht. gjeldende lover og forskrifter og spilleregler i arbeidslivet. Det er spesielt viktig at opplysninger om de ansattes bruk av informasjonssystemene (logging) i hovedsak kun benyttes i sikkerhetsøyemed, slik at unødvendig overvåking av de ansatte unngås. Den ansatte har rett til innsyn i opplysninger som gjelder den ansatte selv (jf. personvernforordningen artikkel 15).

Normen regulerer den registrertes innsyn i logger.

Normens krav om ledelse og ansvar, risikovurdering og informasjonssikkerhet er relevante for primær (behandlinger av helse- og personopplysninger som følger av pasientjournalloven) og sekundærbruk (helseregisterloven) av data. Normens krav om personvern og pasientrettigheter gjelder i versjon 5.3 primærbruk, men kan brukes på sekundærbruk så langt de passer. Neste versjon av Normen vil omfatte sekundærbruk i større grad.

Behandling av helse- og personopplysninger i forskningssammenheng følger helseforskningsloven, men er også underlagt all annen lovgivning på området. Før virksomheten iverksetter et forskningsprosjekt, må Regional komité for medisinsk og

helsefaglig forskningsetikk (REK) søkes om forhåndsgodkjennelse.

Normen regulerer virksomhetenes manuelle og elektroniske behandlinger av helse- og personopplysninger, men er særlig innrettet mot de elektroniske behandlingene.

1.6 Normens utvikling og forvaltning

Normen er utarbeidet og forvaltes av en styringsgruppe fra helse- og omsorgstjenesten, se liste på https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for- informasjonssikkerhet/om-normen#styringsgruppe-for-normen

I prinsipielle spørsmål som behandles i styringsgruppa søkes enstemmighet.

Direktoratet for e-helse er sekretariat for styringsgruppens arbeid, med fast deltakelse fra Norsk Helsenett (NHN).

Kontakt oss

Ole Willy Fundingsrud
Direktør
T +47 40 63 96 92
E ole.willy.fundingsrud@kpmg.no

Veronica Storlid Kvinge
Senior Manager
T +47 95 85 50 55
E veronica.kvinge@kpmg.no

kpmg.no