NORDLANDSSYKEHUSET
NORDLÁNDA SKIPPIJVIESSO

Styresak 008-2020
Internrevisjonsrapport om behandling av personopplysninger i sykehusforetakene i Helse Nord

Saksbehandler: Jørgen Knudsen Sandø
Dato dok: 11.01.2021
Møtedato: 18.2.2021
Vår ref: 2020/2404

Vedlegg (t):
1. Internrevisjonsrapport 10/2020 – Behandling av personopplysninger i Nordlandssykehuset HF
2. Internrevisjonsrapport 11/2020 – Behandling av personopplysninger i sykehusforetakene i Helse Nord, oppsummering

Innstilling til vedtak:
Styret tar saken til orientering.

Bakgrunn:
Nordlandssykehuset HF mottok 24.4.2020 melding fra Helse Nord RHF om internrevisjon for behandling av personopplysninger i Nordlandssykehuset HF. Dette var i henhold til revisjonsplanen for 2020/2021 og tilsvarende revisjoner er blitt gjennomført ved alle sykehusforetakene i regionen.

Formålet med revisjonen var å bekrefte at Nordlandssykehuset har en samlet oversikt over de databehandlinger som utføres av sykehuset under vårt ansvar i henhold til lovpålagt plikt til protokollføring, at behandling skjer i henhold til kravene i personvernforordningen (GDPR), at oppdaterte databehandleravtaler med eksterne leverandører foreligger og prosesser for å holde oversikt over disse. Revisjonen så også på Personvernombudets rolle og oppgaver.

Nordlandssykehuset HF har ikke fått påpekt mangler ved sin databehandling. Internrevisjonen kom med tre anbefalinger for videre arbeid med ivaretakelse av sykehuset sitt behandlingsansvar. Disse tre anbefalingene er blitt oppfylt innen februar 2021.

Direktørens vurdering:
Foretaket arbeider kontinuerlig og systematisk med ivaretakelse av personvernet ved all behandling av personopplysninger. Dette gjenspeiles godt i Internrevisjonens rapport.

Direktøren er tilfreds med Internrevisjonens funn og måten foretaket behandler personopplysninger på i utførelsen av vårt oppdrag.

Innledning

Nordlandssykehuset HF mottok 24.4.2020 melding fra Helse Nord RHF om internrevisjon for behandling av personopplysninger i Nordlandssykehuset HF. Dette var i henhold til revisjonsplanen for 2020/2021 og tilsvarende revisjoner er blitt gjennomført ved alle sykehusforetakene i regionen.

Formålet med revisjonen var å bekrefte at Nordlandssykehuset har en samlet oversikt over de databehandlinger som utføres av sykehuset under vårt ansvar i henhold til lovpålagt plikt til protokollføring, at behandling skjer i henhold til kravene i personvernforordningen (GDPR), at oppdaterte databehandleravtaler med eksterne leverandører foreligger og prosesser for å holde oversikt over disse. Revisjonen så også på personvernombudets rolle og oppgaver.

Revisjonsprosessen ble gjennomført med intervjuer av avdelingsleder for kvalitet og e-helse, informasjonssikkerhetsansvarlig og personvernombud. Det er også blitt oversendt dokumentasjon som har vist hvordan Nordlandssykehuset ivaretar sitt ansvar som databehandler for personopplysninger.

Internrevisjonens rapport for Nordlandssykehuset HF ble oversendt 23. september. Den samlede rapporten for internrevisjon for alle sykehusforetakene i regionen sin behandling av personopplysninger ble oversendt 25.9.2020 og ble behandlet i styret i Helse Nord RHF 28.10.2020.

Revisjonens konklusjon

Internrevisjonen har vurdert at Nordlandssykehuset har tilfredsstillende oversikt over databehandlerrelasjoner med eksterne leverandører og oppdaterte databehandleravtaler med disse. Personvernombudets oppgaver er i henhold til de lovpålagte kravene. Den samlede oversikten Nordlandssykehuset har over behandlinger som utføres under vårt ansvar ble vurdert som å i hovedsak tilfredsstille kravene i GDPR.

Nordlandssykehuset HF har ikke fått påpekt mangler ved sin databehandling. Internrevisjonen kom med tre anbefalinger for videre arbeid med ivaretakelse av sykehuset sitt behandlingsansvar:

1. Å utarbeide en spesifisert framdriftsplan for utarbeidelse av ny versjon av protokoll over behandlingsaktiviteter,
2. Styrke oppfølgingen av framdriften i arbeidet med ny protokoll, og
3. Inkludere personvernombudet i beskrivelsen av foretakets organisering av informasjonssikkerhet.

Oppfølgingsarbeid etter revisjonen

Anbefalingen i punkt 3 er allerede oppfylt ved at personvernombudet er tatt med i beskrivelsen av foretakets organisering av informasjonssikkerhet i den interne retningslinjen PR49242.

Vedrørende punkt 1 og 2 har Nordlandssykehuset arbeidet med ferdigstillelse av ny protokoll. Dette arbeidet skjer i samarbeid med de øvrige helseforetakene i regionen, der protokollen vil gå over fra å føres i regneark til å føres i et digitalt system hos den eksterne leverandøren Sureway. Dette vil føre til en mer komplett, oversiktlig og tilgjengelig protokollføring av sykehusets databehandlingsaktiviteter. Internrevisjonen ble fremvist dette systemet ved gjennomføring av intervju i revisjonsprosessen.

Framdriften i arbeidet for å ferdigstille protokollen i systemet har vært avhengig av at alle sykehusforetakene har kunnet gjennomføre interne utredninger av behov og koordinert dette arbeidet i mellom seg, og at ekstern leverandør har kunnet levert den funksjonaliteten som foretakene har etterspurt. Dette arbeidet har vært prioritert, men det har på bakgrunn av samarbeid og koordinering med eksterne parter vært utfordrende å spesifisere en nøyaktig framdriftsplan for sluttføring av prosessen.

Protokoll i Sureway har blitt innført som sykehuset sin oversikt over behandlingsaktiviteter fra og med februar 2021. Nordlandssykehuset har med dette innfridd de tre anbefalingene Internrevisjonen kom med i sin rapport.

Helse Nord RHF har bedt sykehusforetakene om å legge fram handlingsplaner for oppfølging av internrevisjonens anbefalinger til februar 2021. Nordlandssykehuset HF har lagt fram at alle anbefalinger er innfridde.

HELSE NORD

Internrevisjonsrapport 10/2020

Behandling av personopplysninger i Nordlandssykehuset HF

Internrevisjonen i Helse Nord RHF, 23.09.2020

Innholdsfortegnelse

Vedlegg:
1. Revisjonskriterier
2. Dokumentoversikt

Sammendrag

Denne rapporten er utarbeidet etter internrevisjon i Nordlandssykehuset i perioden april - september 2020.

Formål og omfang av revisjonen
Formålet med revisjonen har vært å bekrefte at Nordlandssykehuset har en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, i samsvar med kravene i personvernforordningen, og at nødvendige databehandler-avtaler foreligger.

Metoder
Internrevisjonen er gjennomført ved dokumentgjennomgang og intervjuer.

Konklusjon
Nordlandssykehuset har etablert en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, som i hovedsak tilfredsstiller kravene i personvernforordningen. Det pågår arbeid med en mer formålstjenlig protokoll, men det er usikkert når denne ferdigstilles. Foretaket har oversikt over hvilke aktører som behandler personopplysninger på dets vegne, og om det foreligger databehandleravtale som sikrer at personopplysninger behandles i samsvar med gjeldende regelverk. Personvernombudets oppgaver er i henhold til forordningens krav.

Anbefalinger
Internrevisjonen anbefaler Nordlandssykehuset å:
1. Utarbeide en spesifisert framdriftsplan for utarbeidelse av ny versjon av protokoll over behandlingsaktiviteter.
2. Styrke oppfølgingen av framdriften i arbeidet med ny protokoll.
3. Inkludere personvernombudet i beskrivelsen av foretakets organisering av informasjonssikkerhet.

1 Innledning

Denne rapporten er utarbeidet etter internrevisjon i Nordlandssykehuset i perioden april- september 2020. Internrevisor Hege Knoph Antonsen har vært oppdragsleder og revisjonssjef Janny Helene Aasen har hatt det overordnede ansvaret. Tilsvarende revisjon er gjennomført i alle regionens sykehusforetak.

Revisjonen har bestått av:
- Melding om internrevisjon sendt 24.04.2020
- Dokumentgjennomgang av interne dokumenter for Nordlandssykehuset
- Intervjuer med sentrale nøkkelpersoner 10.06.2020.
- Oppsummeringsmøte med Nordlandssykehuset 20.08.2020.
- Rapportutkast sendt 27.08.2020, tilbakemelding mottatt 16.09.2020.

1.1 Bakgrunn

Den nye loven om behandling av personopplysninger (personopplysningsloven) trådte i kraft i juli 2018 og inkluderer EUs personvernforordning. Loven gjelder automatisert og ikke-automatisert behandling av personopplysninger. Det framgår av forordningen at den behandlingsansvarlige skal føre en protokoll over behandlingsaktivitetene som utføres under deres ansvar. Denne protokollen skal inneholde vesentlig informasjon om behandlingen. Behandlingsansvarlige som benytter seg av andre leverandører til å utføre behandlingsaktiviteter har plikt til å ha en databehandleravtale som regulerer dette. Forordningen stiller også krav om utpeking av personvernombud, og til personvernombudets stilling og oppgaver.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, Normen, er en bransjenorm detaljerer og supplerer gjeldende regelverk, og alle som er tilknyttet Norsk Helsenett er forpliktet til å følge den.

Oppdragsdokumentene fra Helse Nord RHF til helseforetakene i perioden 2017-2020, viser til at helseforetakene gjennom systematiske tiltak skal sørge for at nasjonale krav til personvern og informasjonssikkerhet blir ivaretatt. Det har vært stilt spesifikke krav om etablering av personvernombud i 2017, og om oversikt over databehandlere og innholdet i «ledelsens gjennomgang» i 2018.

1.2 Revisjonsgrunnlag

Følgende regelverk og nasjonale føringer er særlig aktuelle i denne revisjonen:
- LOV-2018-06-15-38, Lov om behandling av personopplysninger (personopplysningsloven), inkludert EUs personvernforordning 2016/679
- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), v. 6.0

Regionale føringer:

- Oppdragsdokumentene fra Helse Nord RHF til HF-ene i årene 2017-2020
- DS6121, Felles styringssystem informasjonssikkerhet

2 Formål og omfang

2.1 Formål med revisjonen

Formålet med revisjonen har vært å bekrefte at Nordlandssykehuset har en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, i samsvar med kravene i personvernforordningen, og at nødvendige databehandleravtaler foreligger.

2.2 Omfang, fokusområder og avgrensninger

Revisjonen har omfattet og vært konsentrert om følgende fire fokusområder:

- Hvorvidt helseforetakets oversikt over behandlingsaktiviteter (protokoll) er utarbeidet og inneholder påkrevd informasjon.
- Om det foreligger oppdaterte databehandleravtaler med leverandører som behandler personopplysninger på vegne av foretaket.
- Personvernombudets rolle og oppgaver.
- Foretakets prosesser for å holde protokollen og databehandleravtalene oppdaterte.

Innenfor hvert av fokusområdene er det definert revisjonskriterier basert på revisjonsgrunnlaget, jf. kap. 1.2. Disse er presentert samlet i *Vedlegg 1 – Revisjonskriterier*, samt innledningsvis i delkapitlene til kapittel 4. Revisjonskriteriene er de krav og forventninger som revisjonens observasjoner sammenlignes med.

Denne revisjonen har ikke omfattet foretakets øvrige plikter knyttet til informasjonssikkerhet og personvernforordningen.

3 Metoder

Følgende metoder er benyttet i revisjonsoppdraget:

Dokumentgjennomgang:
Dokumenter mottatt fra Nordlandssykehuset, eller innhentet fra foretakets websider, er gjennomgått og vurdert opp mot revisjonskriteriene, samt benyttet i forberedelser til intervjuene. Se *Vedlegg 2 – Dokumentoversikt*.

Intervjuer:
Det er gjennomført intervjuer med tre nøkkelpersoner i foretakets stabsfunksjoner.

4 Observasjoner og vurderinger

4.1 Helseforetakets protokoll over behandlingsaktiviteter

I henhold til personvernforordningens artikkel 30, skal helseforetaket føre en protokoll over behandlingsaktiviteter som utføres under dets ansvar. Protokollen skal inneholde navnet på og kontaktopplysningene til den behandlingsansvarlige, til den felles behandlingsansvarlige dersom det er relevant, og til personvernombudet. Videre skal blant annet følgende informasjon om behandlingsaktivitetene være registrert: kategorier av registrerte, kategorier av personopplysninger, formål og planlagt tidsfrist for sletting. Datatilsynet anbefaler at protokollen suppleres med tilleggsinformasjon som kilde, behandlingsgrunnlag og navn på databehandlere.

4.1.1 Observasjoner

Foretaket har lagt fram en protokoll i Excel inndelt i: Forskningsprosjekter, Kvalitetsprosjekter, Løsning/system, Medisinsk utstyr. Vi fikk opplyst at oversiktene skal være nokså fullstendige. Protokollen inneholder ikke navn på behandlingsansvarlig og personvernombud, slik forordningen krever. Protokollen inneholder for øvrig de obligatoriske feltene vi har kontrollert, med unntak for planlagt tidsfrist for sletting.

Det pågår et arbeid med omlegging fra en systemorientert til en behandlingsorientert protokoll ved hjelp av applikasjonen Sureway[1]. Her legges det opp til å inkludere alle påkrevde opplysninger, samt supplerende informasjon basert på Datatilsynets anbefalinger. Sykehusforetakene samarbeider om dette arbeidet, med bistand fra leverandøren av Sureway. Internrevisjonen er ikke kjent med at det foreligger formelle dokumenter som beskriver organiseringen av dette arbeidet (eksempelvis mandat), og det foreligger ikke en tidfestet framdriftsplan.

4.1.2 Internrevisjonens vurderinger av protokollen

Internrevisjonen konstaterer at foretaket har etablert en protokoll over sin behandling av personopplysninger, som i hovedsak innfrir personvernforordningens krav. Vi anser den behandlingsorienterte protokollen som er under utvikling, som mer formålstjenlig, og legger til grunn at denne skal innfri forordningens krav når den er ferdigstilt. Vi vurderer imidlertid at det er usikkert når den nye protokollen vil foreligge, ettersom det ikke er utarbeidet en framdriftsplan. Det synes hensiktsmessig å styrke oppfølgingen av arbeidet med etablering av protokoll.

4.2 Databehandleravtaler

Dersom en databehandler skal utføre behandling av personopplysninger på vegne av foretaket, skal behandlingen være underlagt en skriftlig avtale.
Personvernforordningens artikkel 28 stiller krav til inngåelse og innhold i slike avtaler.

[1] Sureway: personvernløsning (applikasjon) fra ekstern leverandør

4.2.1 Observasjoner

Nordlandssykehuset har en egen prosedyre som beskriver prosessen ved behov for inngåelse av nye databehandleravtaler, PR46307. Seksjon for E-helse er ansvarlig enhet for avtaleforvaltning i sykehuset og utformer derfor alle databehandleravtaler. Utkast til databehandleravtaler kvalitetssikres av informasjonssikkerhetsansvarlig, før de signeres av administrerende direktør.

Internrevisjonen har mottatt Nordlandssykehusets oversikt over leverandører som behandler personopplysninger på deres vegne, med saksnummer til tilhørende databehandleravtale i arkivsystemet, Elements, og eventuelle merknader om status for den enkelte avtale. Det framkommer av oversikten at foretaket har avtale med 63 av de 79 oppgitte leverandørene, at Helse Nord IKT har inngått avtaler med 12 av leverandørene, og at avtaler med de resterende 4 leverandørene er under utarbeidelse. Vi fikk opplyst at det ikke er gjennomført noen gjennomgang av gamle databehandleravtaler ved innføring av ny personvernlovgivning, men at mange avtaler likevel har blitt oppdatert i forbindelse med andre endringer. Det ble videre opplyst at databehandleravtaler kan søkes opp i arkivsystemet, basert på kategori.

Helse IKT HF er en viktig databehandler av helse- og personopplysninger, i og med at de drifter de fleste av regionens IKT-systemer. Siden 2018 har det pågått et arbeid med oppdatering av databehandleravtalene mellom Helse Nord IKT og helseforetakene, etter klare krav i oppdragsdokumentene for 2018 og 2019. Internrevisjonen konstaterer at det foreligger oppdatert, signert databehandleravtale mellom Nordlandssykehuset HF og Helse Nord IKT HF, utstedt 24.01.2020. Nordlandssykehusets informasjonssikkerhetsansvarlig er oppgitt som kontaktperson i avtalen.

Det legges opp til at ny protokoll i Sureway skal inneholde opplysninger om databehandlere og referanse til aktuelle databehandleravtaler.

4.2.2 Internrevisjonens vurderinger av databehandleravtaler

Internrevisjonen vurderer at Nordlandssykehuset har en god oversikt over hvilke aktører som behandler personopplysninger på vegne av foretaket, og om det finnes en tilhørende databehandleravtale som regulerer dette. Det ser ut til at protokollen som er under utvikling vil legge til rette for en god kobling av disse to oversiktene. Vi viser videre til vurderingen i kap. 4.1.2.

4.3 Personvernombudets rolle og oppgaver

Personvernforordningen stiller i artikkel 37-39, en rekke krav relatert til personvern-ombudsrollen, blant annet at foretaket plikter å offentliggjøre aktuell kontakt-informasjon og at personvernombudet skal rapportere direkte til det høyeste ledelsesnivået i foretaket. Personvernombudet skal minst ha følgende oppgaver:

- informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har,

- kontrollere overholdelsen av personvernforordningen, annet regelverk og interne retningslinjer om personvern,
- på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den,
- samarbeide med tilsynsmyndigheten,
- fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, og ved behov rådføre seg med tilsynsmyndigheten.

Foretaket plikter å sikre at eventuelle andre oppgaver som personvernombudet utfører, ikke medfører interessekonflikt.

4.3.1 Observasjoner

Personvernombud i 100 % stilling er organisert i Avdeling for kvalitet og e-helse, og funksjonen er beskrevet i avdelingens organisasjonsplan, FB0960. Det er presisert at ombudet skal gi ledelsen råd og veiledning «og på en uavhengig måte vurdere virksomhetens regeletterlevelse på dette feltet, i samsvar med personvernforordningen kapittel 4». På foretakets nettsider er det oppgitt navn, epostadresse og telefonnummer direkte til personvernombudet.

Internrevisjonen har sammenstilt mottatt informasjon om personvernombudets oppgaver og konstaterer at forordningens oppgavekrav blir ivaretatt. Kontrolloppgaven inkluderer gjennomføring av egne interne revisjoner innenfor temaet, noe som er innarbeidet i foretakets revisjonsplan. I tillegg er personvernombudet i Nordlandssykehuset tillagt oppgaven med «å føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene» og har hovedansvaret for at denne er oppdatert.

Den regionale retningslinjen RL6911, Organisering av informasjonssikkerhetsarbeidet i Helse Nord, stiller krav om et eget dokument som beskriver foretakets sikkerhetsorganisering, herunder personvernombudets rolle. Nordlandssykehuset har utarbeidet et slikt dokument, PR49242, men personvernombudet er ikke nevnt i dette.

Internrevisjonen fikk opplyst at avdelingsleder har ukentlige statusmøter med personvernombud og informasjonssikkerhetsansvarlig, at de rapporterer årlig til ledelsen og styret, og at de ut over dette har en hendelsesstyrt rapportering til adm. direktør.

4.3.2 Internrevisjonens vurderinger av personvernombudets rolle og oppgaver

Internrevisjonen vurderer at det er etablert en personvernombudsordning i Nordlands-sykehuset i henhold til kravene i personvernforordningen. Dette forutsetter at det operative ansvaret med å føre og oppdatere protokollen som personvernombudet i tillegg er tillagt, ikke medfører interessekonflikter. Vi anser det derfor som avgjørende at det er behandlingsansvarlige som beslutter formålet med behandlingsaktivitetene og melder fra om oppføringer og endringer i protokollen.

Det er positivt at det også er lagt opp til at ombudet skal gjennomføre/delta i interne revisjoner innenfor temaet.

Det framstår som en mangel i henhold til den regionale retningslinjen RL6911 om organisering av informasjonssikkerhetsarbeidet i Helse Nord, at personvernombudet i Nordlandssykehuset ikke omtales i PR49242.

4.4 Foretakets prosesser for å holde protokollen og databehandler-avtalene oppdaterte

En løpende prosess er nødvendig for å holde protokollen og oversikt over databehandleravtaler oppdaterte. Minst én gang årlig skal foretakets ledelse gjennomgå og vurdere om styringssystemet innen informasjonssikkerhet og personvern fungerer som forutsatt, slik foretaket har fått føringer om i oppdragsdokumentene. «Ledelsens gjennomgang» skal også styrebehandles.

4.4.1 Observasjoner

I PR46511, Prosedyre for melding om bruk av personopplysninger, framkommer det at dersom bruken av personopplysningene opphører eller endres, må den enkelte behandlingsansvarlige («melderen») sende endringsinformasjon til personvern-ombudet. Personvernombudet i Nordlandssykehuset er tillagt hovedansvaret for at protokollen er oppdatert, slik det tidligere er opplyst i kap. 4.3.1.

Temaet informasjonssikkerhet og personvern inngikk i ledelsens gjennomgang for 2018, styrebehandlet i sak 60-2019. Styret har også behandlet egne styresaker om status innen informasjonssikkerhet, herunder arbeidet med personvern og protokoll, i mai 2019 (sak 48-2019) og mai 2020 (sak 46-2020). I sak 46-2020 framkom det at det er startet et arbeid der foretaket nå implementerer et elektronisk system for å administrere en komplett oversikt over behandlingene, og at dette gjøres i nært samarbeid med de andre helseforetakene i Helse Nord. Styresaken inneholdt ingen informasjon om planlagt tidspunkt for ferdigstillelse av protokollen.

4.4.2 Internrevisjonens vurderinger av prosesser for oppdateringer

Internrevisjonen anser de separate statusorienteringene til styret som sidestilte med ledelsens gjennomgang i denne sammenhengen, og legger derfor til grunn at det har vært årlige gjennomganger innenfor temaet. Vi vurderer det imidlertid som en svakhet at styret ikke har fått informasjon om når protokollen forventes ferdigstilt. Vi viser til vurderingen i kap. 4.3.2 når det gjelder prosessen for å holde protokollen oppdatert.

5 Konklusjon og anbefalinger

5.1 Konklusjon

Nordlandssykehuset har etablert en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, som i hovedsak tilfredsstiller kravene i personvernforordningen. Det pågår arbeid med en mer formålstjenlig protokoll, men det er usikkert når denne ferdigstilles. Foretaket har oversikt over hvilke aktører som behandler personopplysninger på dets vegne, og om det foreligger databehandleravtale som sikrer at personopplysninger behandles i samsvar med gjeldende regelverk. Personvernombudets oppgaver er i henhold til forordningens krav.

5.2 Anbefalinger

Internrevisjonen anbefaler Nordlandssykehuset å:

1. Utarbeide en spesifisert framdriftsplan for utarbeidelse av ny versjon av protokoll over behandlingsaktiviteter.
2. Styrke oppfølgingen av framdriften i arbeidet med ny protokoll.
3. Inkludere personvernombudet i beskrivelsen av foretakets organisering av informasjonssikkerhet.

Vedlegg 1 – Revisjonskriterier

Følgende fokusområder og kriterier er lagt til grunn for internrevisjonens arbeid og vurderinger:

1. Helseforetakets protokoll over behandlingsaktiviteter
    a. Det foreligger en samlet oversikt (protokoll) over foretakets behandlingsaktiviteter.
    b. Oversikten (protokollen) inneholder navnet på og kontaktopplysningene til:
    -den behandlingsansvarlige
    -den felles behandlingsansvarlige (dersom det er relevant)
    -personvernombudet.
    c. Registrert informasjon om behandlingsaktivitetene omfatter blant annet: kategorier av registrerte (a), kategorier av personopplysninger (a), formål (a), kilde (b), behandlingsgrunnlag (b), navn på databehandlere (b) og planlagt tidsfrist for sletting (a)
    a: krav i personvernforordningen / b: anbefaling fra Datatilsynet

2. Databehandleravtaler
    a. Det foreligger databehandleravtale med databehandlere som er identifisert i foretakets protokoll over behandlingsaktiviteter.
    b. Avtalen er oppdatert i samsvar med kravene i personvernforordningen.

3. Personvernombudets rolle og oppgaver
    a. Kontaktopplysninger til personvernombudet er offentliggjort på foretakets webside.
    b. Personvernombudet rapporterer direkte til foretaksdirektør.
    c. Personvernombudets oppgaver inkluderer de som er påkrevd gjennom forordningen.
    d. Personvernombudet har ikke andre oppgaver som kan medføre interessekonflikt.

4. Foretakets prosesser for å holde protokollen og databehandleravtalene oppdaterte
    a. Foretaket har etablert en løpende prosess for å holde behandlingsoversikten oppdatert.
    b. «Ledelsens gjennomgang» innen informasjonssikkerhet og personvern gjennomføres minst en gang i året.

Vedlegg 2 – Dokumentoversikt

Oversikt over dokumenter som er gjennomgått i forbindelse med revisjonen.

- Erklæring om behandling av personopplysninger ved Nordlandssykehuset, https://nordlandssykehuset.no/personvern#sykehusets-personvernombud, hentet 27.04.2020
- Oversendelsesbrev til Internrevisjonen i Helse Nord RHF, 15.05.2020
- Oversikt over behandling av helse- og personopplysninger, mottatt 15.05.2020, inndelt i:
  - Forskningsprosjekter
  - Kvalitetsprosjekter
  - Løsning-system
  - Medisinsk utstyr
- Dokumenter som beskriver status i pågående med ny protokollen via Sureway per 01.05.2020:
  - Utkast til oversikt over behandlingsaktiviteter ved sykehuset
  - Utkast til protokoller for pasientbehandling
  - Utkast til protokoller for tilstøtende sykehustjenester
- Eksempel på personvernerklæring basert på opplysninger i ny protokoll, kirurgisk behandling, mottatt 20.08.2020
- Oversikt over leverandører og databehandleravtaler, mottatt 10.06.2020
- Utlysningsteksten for stillingen som personvernombud, 27.10.2019
- FB0960, Organisasjonsplan for avdeling for kvalitet og e-helse, versjon 2
- PR46511, Prosedyre for melding om bruk av personopplysninger, versjon 1, med tilhørende lenker til meldeskjemaer i Redcap
- PR46307, Inngåelse av databehandleravtale - Nordlandssykehuset HF, versjon 1
- MS0272, 4-årsplan for internrevisjon på foretaksnivå, 2020-2023
- OL0231, 1-årsplan for internrevisjon i 2020, systemrevisjoner som utføres av Avdeling for kvalitet og e-helse på foretaksnivå
- Referat fra ledelsens gjennomgang for 2017, Avdeling for kvalitet og e-helse, 20.06.2018
- Styresak 48/2019, Orienteringssak – Informasjonssikkerhet pr mai 2019
- Styresak 60-2019, Rapport fra ledelsens gjennomgang av foretaket 2018
- Styresak 46/2020, Orienteringssak – Informasjonssikkerhet pr mai 2020, unntatt offentlighet
- Avtale om behandling av personopplysninger, Databehandleravtale, mellom Nordlandssykehuset HF og Helse Nord IKT HF, utstedt 24.01.2020

HELSE NORD

Internrevisjonsrapport 11/2020

Behandling av personopplysninger i sykehusforetakene i Helse Nord, oppsummering

Internrevisjonen i Helse Nord RHF, 25.09.2020

Innholdsfortegnelse

Vedlegg:
1. Revisjonskriterier

Sammendrag

Denne rapporten er utarbeidet etter internrevisjon i Universitetssykehuset Nord-Norge, Finnmarkssykehuset, Helgelandssykehuset og Nordlandssykehuset i perioden april - september 2020.

Formål og omfang av revisjonen
Formålet med revisjonen har vært å bekrefte at det enkelte sykehusforetak har en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, i samsvar med kravene i personvernforordningen, og at nødvendige databehandleravtaler foreligger.

Metoder
Internrevisjonen er gjennomført ved dokumentgjennomgang og intervjuer.

Konklusjon
Tre av sykehusforetakene i Helse Nord har ikke etablert en behandlingsprotokoll som tilfredsstiller personvernforordningens krav, to år etter ikrafttredelsen. Det er usikkert når tilfredsstillende protokoller vil foreligge. To av foretakene har heller ikke en oversikt over hvilke aktører som behandler personopplysninger på dets vegne, og om det foreligger databehandleravtale som sikrer at personopplysninger behandles i samsvar med gjeldende regelverk. Personvernombudsordninger er etablert, men rollens oppgaver er noe uklart definert i enkelte av foretakene.

Anbefalinger
Internrevisjonen har, i rapportene til de enkelte foretakene, gitt hvert foretak følgende tre til fem anbefalinger:

1. Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav, inkludert oversikt over databehandlere og tilhørende avtaler.[1]
2. Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll og databehandleravtaler.
3. Inkludere personvernombudet i beskrivelsen av foretakets organisering av informasjonssikkerhet.
4. FIN: Oppdatere avtalen om kjøp av personvernombudstjenester i henhold til ny personopplysningslov.
5. UNN/FIN/HSYK: Etablere en løpende prosess for å holde protokollen oppdatert.

[1] Anbefalingen har en mer begrenset ordlyd til to av foretakene.

1 Innledning

Denne rapporten er utarbeidet etter internrevisjon i regionens sykehusforetak i perioden april-september 2020. Internrevisor Hege Knoph Antonsen har vært oppdragsleder og revisjonssjef Janny Helene Aasen har hatt det overordnede ansvaret.

Denne rapporten oppsummerer revisjonene i helseforetakene, rapportert som følger:

- Universitetssykehuset Nord-Norge HF (UNN), IR-rapport 07/2020, 23.09.2020
- Finnmarkssykehuset HF (FIN), IR-rapport 08/2020, 23.09.2020
- Helgelandssykehuset HF (HSYK), IR-rapport 09/2020, 25.09.2020
- Nordlandssykehuset HF (NLSH), IR-rapport 10/2020, 23.09.2020

1.1 Bakgrunn

Den nye loven om behandling av personopplysninger (personopplysningsloven) trådte i kraft i juli 2018 og inkluderer EUs personvernforordning. Loven gjelder automatisert og ikke-automatisert behandling av personopplysninger. Det framgår av forordningen at den behandlingsansvarlige skal føre en protokoll over behandlingsaktivitetene som utføres under deres ansvar. Denne protokollen skal inneholde vesentlig informasjon om behandlingen. Behandlingsansvarlige som benytter seg av andre leverandører til å utføre behandlingsaktiviteter har plikt til å ha en databehandleravtale som regulerer dette. Forordningen stiller også krav om utpeking av personvernombud, og til personvernombudets stilling og oppgaver.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, Normen, er en bransjenorm detaljerer og supplerer gjeldende regelverk, og alle som er tilknyttet Norsk Helsenett er forpliktet til å følge den.

Oppdragsdokumentene fra Helse Nord RHF til helseforetakene i perioden 2017-2020, viser til at helseforetakene gjennom systematiske tiltak skal sørge for at nasjonale krav til personvern og informasjonssikkerhet blir ivaretatt. Det har vært stilt spesifikke krav om etablering av personvernombud i 2017, og om oversikt over databehandlere og innholdet i «ledelsens gjennomgang» i 2018.

1.2 Revisjonsgrunnlag

Følgende regelverk og nasjonale føringer er særlig aktuelle i denne revisjonen:

- LOV-2018-06-15-38, Lov om behandling av personopplysninger (personopplysningsloven), inkludert EUs personvernforordning 2016/679
- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), v. 6.0

Regionale føringer:

- Oppdragsdokumentene fra Helse Nord RHF til HF-ene i årene 2017-2020
- DS6121, Felles styringssystem informasjonssikkerhet

2 Formål og omfang

2.1 Formål med revisjonen

Formålet med revisjonen har vært å bekrefte at det enkelte sykehusforetak har en samlet oversikt over behandlinger av personopplysninger som blir utført under dets ansvar, i samsvar med kravene i personvernforordningen, og at nødvendige databehandleravtaler foreligger.

2.2 Omfang, fokusområder og avgrensninger

Revisjonen har omfattet og vært konsentrert om følgende fire fokusområder:

- Hvorvidt helseforetakets oversikt over behandlingsaktiviteter (protokoll) er utarbeidet og inneholder påkrevd informasjon.
- Om det foreligger oppdaterte databehandleravtaler med leverandører som behandler personopplysninger på vegne av foretaket.
- Personvernombudets rolle og oppgaver.
- Foretakets prosesser for å holde protokollen og databehandleravtalene oppdaterte.

Innenfor hvert av fokusområdene er det definert revisjonskriterier basert på revisjonsgrunnlaget, jf. kap. 1.2. Disse er presentert samlet i *Vedlegg 1 – Revisjonskriterier*, samt innledningsvis i delkapitlene til kapittel 4. Revisjonskriteriene er de krav og forventninger som revisjonens observasjoner sammenlignes med.

Denne revisjonen har ikke omfattet foretakenes øvrige plikter knyttet til informasjonssikkerhet og personvernforordningen.

3 Metoder

Følgende metoder er benyttet i revisjonsoppdraget:

<u>Dokumentgjennomgang:</u>
Dokumenter mottatt fra foretakene, eller innhentet fra deres websider, er gjennomgått og vurdert opp mot revisjonskriteriene, samt benyttet i forberedelser til intervjuene. Dokumentoversikter følger de foretaksvise rapportene som vedlegg.

Intervjuer:
Det er gjennomført intervjuer med tre-fire nøkkelpersoner i hvert foretaks stabsfunksjoner.

4 Observasjoner og vurderinger

4.1 Helseforetakets protokoll over behandlingsaktiviteter

I henhold til personvernforordningens artikkel 30, skal helseforetaket føre en protokoll over behandlingsaktiviteter som utføres under dets ansvar. Protokollen skal inneholde navnet på og kontaktopplysningene til den behandlingsansvarlige, til den felles behandlingsansvarlige dersom det er relevant, og til personvernombudet. Videre skal blant annet følgende informasjon om behandlingsaktivitetene være registrert: kategorier av registrerte, kategorier av personopplysninger, formål og planlagt tidsfrist for sletting. Datatilsynet anbefaler at protokollen suppleres med tilleggsinformasjon som kilde, behandlingsgrunnlag og navn på databehandlere.

4.1.1 Observasjoner

Det enkelte foretaket har lagt fram sin protokoll over behandling av personopplysninger. Alle foretakene har en protokoll som er innrettet etter IT-system. I varierende grad mangler det påkrevd informasjon hos alle. Finnmarkssykehusets protokoll er bare en liste over IT-systemene som benyttes i foretaket, mens Nordlands-sykehuset har en detaljert oversikt som i hovedsak innfrir forordningens krav.

Det pågår et arbeid med omlegging fra en systemorientert til en behandlingsorientert protokoll ved hjelp av applikasjonen Sureway[2]. Her legges det opp til å inkludere alle påkrevde opplysninger, samt supplerende informasjon basert på Datatilsynets anbefalinger. Sykehusforetakene samarbeider om dette arbeidet, med bistand fra leverandøren av Sureway. Internrevisjonen er ikke kjent med at det foreligger formelle dokumenter som beskriver organiseringen av dette arbeidet (eksempelvis mandat), og ingen av foretakene har utarbeidet en tidfestet framdriftsplan.

4.1.2 Internrevisjonens vurderinger av protokollen

Internrevisjonen vurderer det som uheldig at tre av foretakene ikke kan legge fram en behandlingsprotokoll i henhold til personvernforordningens krav, to år etter at den nye personopplysningsloven trådte i kraft. Vi anser de behandlingsorienterte protokollene som er under utvikling, som mer formålstjenlige, og legger til grunn at disse skal innfri forordningens krav når de er ferdigstilt. Vi vurderer imidlertid at det er usikkert når tilfredsstillende protokoller vil foreligge, ettersom det ikke er utarbeidet framdriftsplaner. Det synes hensiktsmessig å styrke oppfølgingen av arbeidet med etablering av protokoll i det enkelte foretaket.

[2] Sureway: personvernløsning (applikasjon) fra ekstern leverandør

4.2 Databehandleravtaler

Dersom en databehandler skal utføre behandling av personopplysninger på vegne av foretaket, skal behandlingen være underlagt en skriftlig avtale.
Personvernforordningens artikkel 28 stiller krav til inngåelse og innhold i slike avtaler.

4.2.1 Observasjoner

Universitetssykehuset Nord-Norge og Nordlandssykehuset har oversikt over leverandører som behandler personopplysninger på deres vegne, med statusinformasjon om tilhørende databehandleravtaler og saksnummer i arkivsystemet, Elements. Fra Finnmarkssykehuset og Helgelandssykehuset fikk vi opplyst at man ikke har en slik oversikt. Vi har videre fått opplyst at avtaler fra 2018 og eldre bør fornyes slik at de tilfredsstiller kravene i personvernforordningen, men at foretakene ikke har etablert systematiske prosesser for slike fornyelser. Den regionale malen, eventuelt med enkelte modifikasjoner, benyttes når nye avtaler inngås.

Helse IKT HF er en viktig databehandler av helse- og personopplysninger, i og med at de drifter de fleste av regionens IKT-systemer. Siden 2018 har det pågått et arbeid med oppdatering av databehandleravtalene mellom Helse Nord IKT og helseforetakene, etter klare krav i oppdragsdokumentene for 2018 og 2019. Internrevisjonen konstaterer at det foreligger oppdaterte, signerte databehandleravtaler mellom det enkelte sykehusforetaket og Helse Nord IKT HF, alle utstedt 24.01.2020.

Det legges opp til at ny protokoll i Sureway skal inneholde opplysninger om databehandlere og referanse til aktuelle databehandleravtaler.

4.2.2 Internrevisjonens vurderinger av databehandleravtaler

Internrevisjonen vurderer at Universitetssykehuset Nord-Norge og Nordlandssykehuset har en god oversikt over hvilke aktører som behandler personopplysninger på vegne av foretaket, og om det finnes en tilhørende databehandleravtale som regulerer dette.
Vi vurderer det som uheldig at de andre to sykehusforetakene ikke har en slik oversikt. Det ser ut til at protokollen som er under utvikling vil legge til rette for en god integrering av informasjon om databehandlere, jf. vurderingen i kap. 4.1.2.

4.3 Personvernombudets rolle og oppgaver

Personvernforordningen stiller i artikkel 37-39, en rekke krav relatert til personvernombudsrollen, blant annet at foretaket plikter å offentliggjøre aktuell kontaktinformasjon, og at personvernombudet skal rapportere direkte til det høyeste ledelsesnivået i foretaket. Personvernombudet skal minst ha følgende oppgaver:

- informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har,
- kontrollere overholdelsen av personvernforordningen, annet regelverk og interne retningslinjer om personvern,

- på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den,
- samarbeide med tilsynsmyndigheten,
- fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, og ved behov rådføre seg med tilsynsmyndigheten.

Foretaket plikter å sikre at eventuelle andre oppgaver som personvernombudet utfører, ikke medfører interessekonflikt.

4.3.1 Observasjoner

I Universitetssykehuset Nord-Norge har funksjonene personvernombud og sikkerhetssjef/informasjonssikkerhetsansvarlig blitt ivaretatt av samme person i en kombinert stilling, men fra 1. oktober 2020 vil funksjonene splittes og personvernombudsrollen blir egen stilling. Finnmarkssykehuset kjøper personvernombudstjenesten fra Universitetssykehuset Nord-Norge og har inngått egen avtale som regulerer dette. Oppdraget utgjør ca. 30 % stilling. Helgelandssykehuset og Nordlandssykehuset har tilsatt personvernombud i stillingsstørrelse på henholdsvis 50 % og 100 %. På foretakenes nettsider er det oppgitt navn, epostadresse og telefonnummer direkte til personvernombudet.

Noen av foretakene har utarbeidet en egen beskrivelse av personvernombudets rolle og oppgaver, eksempelvis i form av en stillingsbeskrivelse eller som del av avdelingens organisasjonsplan. Tjenesteavtalen mellom Universitetssykehuset Nord-Norge og Finnmarkssykehuset er utarbeidet i henhold til gammel personvernlovgivning, og avtaleteksten bidrar til at oppgavedelingen mellom personvernombud og informasjonssikkerhetsrådgiver oppleves noe uavklart når det gjelder utarbeidelse og vedlikehold av protokollen. Heller ikke i Helgelandssykehuset er det en klar oppgavefordeling mellom disse to funksjonene.

Internrevisjonen har sammenstilt mottatt informasjon om personvernombudets oppgaver i det enkelte foretaket og konstaterer at forordningens oppgavekrav i hovedsak blir ivaretatt. Det er imidlertid noe ulikt hvordan oppgaven med å kontrollere overholdelse av regelverk og interne personvernretningslinjer blir ivaretatt, ut over i enkeltsaker der personvernombudet blir konsultert. I Nordlandssykehuset er det innarbeidet i foretakets revisjonsplan at personvernombudet skal gjennomføre interne revisjoner innenfor temaet.

Personvernombudet i Nordlandssykehuset er i tillegg tillagt oppgaven med «å føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene» og har hovedansvaret for at denne er oppdatert.

Den regionale retningslinjen RL6911, Organisering av informasjonssikkerhetsarbeidet i Helse Nord, stiller krav om et eget dokument som beskriver foretakets sikkerhetsorganisering, inkludert personvernombudets rolle. Tre av foretakene har utarbeidet et

slikt dokument, uten at personvernombudet er nevnt i dette. Universitetssykehuset Nord-Norge har ikke opprettet eget dokument om sin sikkerhetsorganisering.

4.3.2 Internrevisjonens vurderinger av personvernombudets rolle og oppgaver

Internrevisjonen vurderer at foretakene har etablert personvernombudsordninger i henhold til kravene i personvernforordningen, men at noen av foretakene bør oppdatere sin beskrivelse av funksjonen. Vår vurdering forutsetter at det operative ansvaret med å føre og oppdatere protokollen som personvernombudet er tillagt i Nordlandssykehuset, ikke medfører interessekonflikter. Vi anser det som avgjørende at det er behandlingsansvarlige som beslutter formålet med behandlingsaktivitetene og melder fra om oppføringer og endringer i protokollen til personvernombudet.

Vi anser det som en svakhet at personvernombudsrollen i Universitetssykehuset Nord-Norge hittil har blitt kombinert med rolle som sikkerhetssjef/informasjonssikkerhetsansvarlig, da dette kan ha redusert personvernombudets uavhengighet. Pågående splitting av roller vurderes hensiktsmessig og vil styrke personvernarbeidet.

Det framstår som en mangel i henhold til den regionale retningslinjen RL6911 om organisering av informasjonssikkerhetsarbeidet i Helse Nord, at Universitetssykehuset Nord-Norge ikke har opprettet en egen beskrivelse av sin sikkerhetsorganisering, samt at de øvrige foretakene ikke omtaler personvernombudet i sine beskrivelser.

4.4 Foretakets prosesser for å holde protokollen og databehandleravtalene oppdaterte

En løpende prosess er nødvendig for å holde protokollen og oversikt over databehandleravtaler oppdaterte. Minst én gang årlig skal foretakets ledelse gjennomgå og vurdere om styringssystemet innen informasjonssikkerhet og personvern fungerer som forutsatt, slik foretaket har fått føringer om i oppdragsdokumentene. «Ledelsens gjennomgang» skal også styrebehandles.

4.4.1 Observasjoner

I tre av foretakene er det ikke avklart hvordan protokollen og tilhørende oversikt over databehandleravtaler skal holdes oppdatert, når man har etablert og tatt i bruk den nye protokollen i Sureway. Det vises også til informasjon i kap. 4.3.1 om uklarheter i oppgavefordeling mellom personvernombud og informasjonssikkerhetsrådgiver i noen av foretakene.

Nordlandssykehuset har prosedyrefestet at dersom bruken av personopplysningene opphører eller endres, må den enkelte behandlingsansvarlige («melderen») sende endringsinformasjon til personvernombudet. Personvernombudet i Nordlandssykehuset er tillagt hovedansvaret for at protokollen er oppdatert, slik det tidligere er opplyst i kap. 4.3.1.

Temaet informasjonssikkerhet og personvern inngikk i «Ledelsens gjennomgang for 2018», som har blitt styrebehandlet i alle foretakene. Styrene har også behandlet status innen informasjonssikkerhet, herunder arbeidet med personvern og protokoll, i mai 2020. Her fikk styrene informasjon om at det pågår et arbeid om oppbygging av det enkelte foretaks protokoll, og at dette gjøres i nært samarbeid mellom sykehusforetakene i Helse Nord. Styresakene inneholdt ingen informasjon om planlagt tidspunkt for ferdigstillelse av protokollen.

4.4.2 Internrevisjonens vurderinger av prosesser for oppdateringer

Internrevisjonen anser separat statusorientering til styrene om temaet informasjonssikkerhet og personvern som sidestilt med «Ledelsens gjennomgang», og legger derfor til grunn at det har vært årlige gjennomganger innenfor temaet. Vi vurderer det imidlertid som en svakhet at styrene ikke har fått informasjon om når protokollen forventes ferdigstilt. Videre understreker vi viktigheten av å fastsette en løpende prosess for å holde protokollen oppdatert, når den tas i bruk.

5 Konklusjon og anbefalinger

5.1 Konklusjon

Tre av sykehusforetakene i Helse Nord har ikke etablert en behandlingsprotokoll som tilfredsstiller personvernforordningens krav, to år etter ikrafttredelsen. Det er usikkert når tilfredsstillende protokoller vil foreligge. To av foretakene har heller ikke en oversikt over hvilke aktører som behandler personopplysninger på dets vegne, og om det foreligger databehandleravtale som sikrer at personopplysninger behandles i samsvar med gjeldende regelverk. Personvernombudsordninger er etablert, men rollens oppgaver er noe uklart definert i enkelte av foretakene.

5.2 Anbefalinger

Internrevisjonen har, i rapportene til de enkelte foretak, gitt følgende anbefalinger (tall = anbefalingens nummer i den enkelte HF-rapport):

Anbefaling	*UNN*	*FIN*	*HSYK*	*NLSH*
Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav, inkludert oversikt over databehandlere og tilhørende avtaler.		1	1	
Utarbeide en spesifisert framdriftsplan og oppgavefordeling for utarbeidelsen av en protokoll som tilfredsstiller gjeldende krav	1			1*
Styrke oppfølgingen av framdriften i arbeidet med å innfri kravene til protokoll.	2	2	2	2*
Inkludere personvernombudet i beskrivelsen av foretakets organisering av informasjonssikkerhet	3	3	3	3
Oppdatere avtalen om kjøp av personvernombudstjenester i henhold til ny personopplysningslov.		4		
Etablere en løpende prosess for å holde protokollen oppdatert.	4	5	4	

*Anbefalingen har en mer begrenset ordlyd.

Vedlegg 1 – Revisjonskriterier

Følgende fokusområder og kriterier er lagt til grunn for internrevisjonens arbeid og vurderinger:

1. Helseforetakets protokoll over behandlingsaktiviteter
    a. Det foreligger en samlet oversikt (protokoll) over foretakets behandlingsaktiviteter.
    b. Oversikten (protokollen) inneholder navnet på og kontaktopplysningene til:
    -den behandlingsansvarlige
    -den felles behandlingsansvarlige (dersom det er relevant)
    -personvernombudet.
    c. Registrert informasjon om behandlingsaktivitetene omfatter blant annet: kategorier av registrerte (a), kategorier av personopplysninger (a), formål (a), kilde (b), behandlingsgrunnlag (b), navn på databehandlere (b) og planlagt tidsfrist for sletting (a)
    a: krav i personvernforordningen / b: anbefaling fra Datatilsynet

2. Databehandleravtaler
    a. Det foreligger databehandleravtale med databehandlere som er identifisert i foretakets protokoll over behandlingsaktiviteter.
    b. Avtalen er oppdatert i samsvar med kravene i personvernforordningen.

3. Personvernombudets rolle og oppgaver
    a. Kontaktopplysninger til personvernombudet er offentliggjort på foretakets webside.
    b. Personvernombudet rapporterer direkte til foretaksdirektør.
    c. Personvernombudets oppgaver inkluderer de som er påkrevd gjennom forordningen.
    d. Personvernombudet har ikke andre oppgaver som kan medføre interessekonflikt.

4. Foretakets prosesser for å holde protokollen og databehandleravtalene oppdaterte
    a. Foretaket har etablert en løpende prosess for å holde behandlingsoversikten oppdatert.
    b. «Ledelsens gjennomgang» innen informasjonssikkerhet og personvern gjennomføres minst en gang i året.