

Ny personvernlovgeving frå 20. juli 2018 – status på tilpassing i Hordaland fylkeskommune

Fylkesrådmannen viser til protokoll frå møtet i Kontrollutvalet 05.02.18 (PS 5/2018), der utvalet ber om ein status på tilpassinga til ny personvernlovgeving. Fylkesrådmannen ga ein status for arbeidet i møtet 5. februar 2018, 24. september 2018 og 6. mai 2019.

Kontrollutvalet ynskjer ein oppdatert status for arbeidet frå fylkesrådmannen til møtet i november 2019.

I det følgjande gis først ei oppdatert status på spørsmåla frå Kontrollutvalet av 05.02.2018 og til slutt eit eige punkt med avsluttande kommentarar.

1. Er det nokon som jobbar med ny personvernlov?

Alle avdelingane har peikt ut lokale personvernkoordinatorar, som representerer fagavdelingane inn i arbeidet med å gjere tilpassingar til nytt regelverk og koordinerer aktuelle aktivitetar i sine respektive einingar. Det er utarbeidd ein instruks for rolla som personvernkoordinator. Sjølve ansvaret for at kvar eining gjer naudsynte tilpassingar til nytt regelverk og etterlev dette ligg hos kvar einingsleiar, og det er naudsynt at desse samarbeider med sin personvernkoordinator. Tilsvarande har alle vidaregåande skular i både Hordaland og Sogn og Fjordane peikt ut sine personvernkoordinatorer.

Som det er påpeikt tidlegare, er det ynskjeleg at Tannhelse og får på plass ein personvernkoordinator i dei ulike tannhelsekontora. Dette er ikkje oppretta enno, og det bør arbeidast for at dette kjem på plass for tannhelsekontora i heile Vestland fylkeskommune.

Den 24. april 2019 blei det gjennomført ein omfattande opplæringsdag for alle personvernkoordinatorane med rektorane i dei vidaregåande skulane. Formålet var at leiinga ved skulane skulle få opplæring i å handtere personvernspørsmål ved eigen skule, og slik at det vil bli mogleg å utføre internkontroll ved skulane. Relevant personell frå skulane i Sogn og fjordane deltok og denne dagen via streaming.

Tilsvarande vil det i løpet av sein haust vere ein tilsvarande opplæringsdag for personvernkoordinatorar og leiarar i administrasjonen for Vestland fylkeskommune. Det er to advokatar frå eksternt firma som har ansvar for opplæringa.

It seksjonen har også arbeidsoppgåver knytt til personvernlovgevinga. Det arbeidast med å få på plass ein ny sikkerheitsansvarleg i Vestland fylkeskommune og per i dag har ikkje Hordaland fylkeskommune tilsette i denne stillinga.

Skyss har ein eigen tiltaksplan som vert følgt opp lokalt.

2. Er det laga protokoll som viser kva som er samla inn av personopplysningar?

Etter personvernforordning Artikkel 30 skal den behandlingsansvarlege føre protokoll over behandlingsaktivitetar som utførast i fylkeskommunen. Fylkeskommunen har eit stort antal behandlingar som skal dokumenterast ved behandlingsprotokoll svært mange system som behandlar personopplysningar.

Desse behandlingane med oversyn over kva opplysningar som behandlast, heimel for å behandle opplysningane, omfang av opplysningane, om dei delast med nokon og eventuelt kor til, opplysningar om når dei eventuelt skal slettast, om det er naudsynt å gjere ei risikovurdering og ei konsekvensvurdering (DPIA / Data Protection Impact Assessment/) som skal sikre at personvernet til dei som er registrert i løysinga blir ivareteke og liknande, skal ein etter Artikkel 30 ha kontroll på. Dette er eit sentralt styringsdokument for behandlingsansvarleg og som må gjerast til ein del av fylkeskommunens / avdelinganes internkontrollsystem.

Når det gjeld å få på plass behandlingsprotokoll, er det vurdert at dette først må prioriterast for skulane. Dette er grunngeven i at skulane samlar inn store mengder av personopplysningar for elevar, ein gruppe som består av også mindreårige og sårbare personar. Dette er og i tråd med Datatilsynets vurdering om at det må til eit felles løft for personvern og informasjonssikkerheit i skulane. Datatilsynet har syna viktigheten av ein åtferdsnorm i skulane (grunn- og vidaregåande skular).

Status for protokollane er framleis at det arbeidast med å kartlegge personopplysningane i verksemda. Det har vore ein målsetting å få protokolldokumentasjon på plass for elevar, tilsette og pasientar som ein første dokumentasjon innan summer / haust 2019. Dette er framleis ein målsetting, og målsetting at dette kan dokumenterast ved overgangen til Vestland fylkeskommune.

Det presiserast at protokollføringa er eit krevjande arbeid som vil ta tid og det vil og ta tid å sikre at dei einskilde avdelingane tek ansvar for å vedlikehalde desse protokollane framover i tid og gjer dette til ein del av sine rutinar og internkontroll. Ansvar for dei avdelingsvise protokollane må liggje i linja til fylkesrådmannen då det er avdelingane sjølv som har oversikt over kva behandlingar dei har av personopplysningar og i kva system.

Det er og naudsynt å etablere rutinar som sikrar at dei vurderingane som protokollane legg opp til at behandlingsansvarleg skal ha kontroll på og kunne dokumentere etterleving av, blir fulgt opp.

Er det inngått databehandlaravtalar, og er desse oppdatert?

HFK har pt ikkje ei samla oversikt over kva leverandørar som behandlar personopplysningar og har heller ikkje ei samla oversikt som gjer informasjon om naudsynt databehandlaravtale er inngått med den einskilde leverandør eller kva risiko dei ulike systema har. Dette har ikkje endra seg sidan førre statusmelding til Kontrollutvalet. Det er tidlegare orientert om at dette er et stort og krevjande arbeid, som må løysast i linja og dei einskilde avdelingane.

Fylkeskommunen har sin eigen databehandlaravtalemal utarbeidd etter nye personvernreglar, som er fylkeskommunen sin formelle avtale i kontakt med leverandørane. Denne er tilgjengeleg i Kvalitetsportalen i nynorsk og engelsk versjon. Denne er også delt med same føremål til Sogn og Fjordane fylkeskommune. Denne anbefalast å bruke vidare som Vestland fylkeskommune si mal på slike avtalar, men slik at den justerast for nye behov fylkeskommunen erfarer å ville ha meir kontroll på. Personvernombodet ønskjer å påpeike eit viktig moment i denne samanheng. Den teknologiske utviklinga skjer i eit stort tempo og rettsleg står ein i ei ny tid når det gjeld juss og teknologi kor vår bakgrunnsrett skal brukast på eit nytt faktum, teknologisk faktum. Skal Vestland fylkeskommune ligge i forkant og vere ein behandlingsansvarleg som tek sitt ansvar i relasjon til

datasystem og leverandørar, er det naudsynt at fylkeskommunen har tilstrekkeleg kompetanse internt, spesielt knytt til it- og innkjøpsfagleg side, til å forstå kva system vi tek i bruk, kva risiko desse inneheld, korleis risiko påverkar personvernet, kva vilkår ein leverandør set i avtalerelasjonen til fylkeskommunen osv. Vidare at klare definerte rollar styrar etter målarbeid og internkontroll. Det er heilt naudsynt at fylkeskommunen får på plass rollar som tek ansvar for å vurdere system som inneheld risiko for personvern og informasjonssikkerhet før systema vert tekne i bruk og for system som allereie er tekne i bruk. Dette bør prioriterast i Vestland fylkeskommune.

I samband med samanslåinga av fylkeskommunane jobbast det i eit prosjekt med å dokumentera dei systema som skal overførast til Vestland fylkeskommune. Denne dokumentasjonen brukast og til å vurdere kva system som skal gjennomgå ein risikovurdering og det er anbefalt at dette også brukast til å dokumentere status for databehandlaravtalar. Denne systematikken og oversikten må for å ha ein verdi i ny fylkeskommune implementerast og følgjast opp, elles vil denne dokumentasjonen bli raskt utdatert og ikkje gje notoritet framover i tid.

3. Er det oppretta personvernombod / rådgjevar?

Etter ny personvernlovgeving er Hordaland fylkeskommune pålagt å ha eit personvernombod. Kjerneoppgåvene for ombodet er å informere, gi råd, kontrollere og vere eit kontaktpunkt for den registrerte.

Personvernombodet vert tilsett frå 2. april 2018. Personvernombodet har og ombodsrolla for fylkeskommunen i Sogn og Fjordane, men slik at dei sjølv tek ansvar for å bygge opp naudsynte system, rutinar, prosedyrar og rolleavklaringar internt.

Personvernombodet ligg per i dag i fagleg linje til konstituert fylkesrådmann og fylkesdirektør økonomi og organisasjon har personalansvaret. Ved fylkeskommunen i Sogn og Fjordane rapporterer ombodet direkte til ass. fylkesrådmann.

Personvernombodet deltek i eit nasjonalt nettverk for fylkeskommunale personvernombod. Det er tenleg at omboda jobbar i fellesskap om felles løysingar for felles utfordringar og skapar likeins rutinar det det er fornuftig. Personvernombodet er i tillegg aktiv i forhold til å halde foredrag og innlegg, både internt, men også eksternt.

Frå 1. januar 2020 går personvernombodet over i ei ny ekstern stilling. Vestland fylkeskommune må prioritera å få på plass naudsynt kompetanse i rolla innan dette. Det bør vurderast å skilje personvernombodet frå stillinga som personvernrådgjevar og ha ein gjennomgang av korleis den nye fylkeskommunen skal jobbe med informasjonssikkerhet og personvern som eit eige fagområde.

4. Er personvernerklæringa oppdatert?

Fylkeskommunen har utarbeidd personvernerklæringar for besøkande på våre internettsider, elevar, tilsette og pasientar. Personvernerklæringene vil og gjelde for Vestland fylkeskommune. Kvar avdeling må sjå til at den informasjonen som dei gir dei registrerte er oppdatert til ei kvar tid, eventuelt i samråd med personvernombodet.

Er det innebygd personvern i datasystem?

For dette spørsmålet synast det til rapporteringa av september 2018. Det er ikkje kome noko nytt til dette punktet sidan då utover at IT-seksjonen jobbar kontinuerleg med å sikre at alle HFK sine IT-løysingar er i samsvar med GDPR krav. Det gjelder både eksisterande løysingar og framtidige IT-løysingar for Vestland fylkeskommune.

5. Er det vurdert å få vennlegsinna hackere til å teste datasystem?

Hordaland fylkeskommune har høg merksemd på informasjonssikkerheit og fysisk IT-sikkerheit og arbeider kontinuerleg med ulike rutinar og tiltak for å sikre at dette vert følgt opp i den daglege drifta. Det har så langt ikkje vore vurdert å engasjere eksterne hackere for å foreta slike systemtestar, men det bør vurderast om til dømes elevsystem bør vurderast for ein slik uttesting.

I lys av sikkerheitsbrot i kommunane knytt til elevdata og elevsystem, har det gode grunnar føre seg å vurderer eit potensielt behov her.

6. Avsluttande kommentarar

Ved førre statusmelding til Kontrollutvalet ble det nemnd at det var ønskeleg å få på plass eit verktøy / datasystem for å handtere mellom anna behandlingsprotokollar, personvernerklæringar innsyn, risiko med meir. I samband med at fylkeskommunane skal fusjonerast er det vurdert å sette denne prosessen på vent slik at behovet for dette kan bli vurdert i lys av ein ny verksemd frå 1. januar 2020. Dette er framleis gjeldande oppfatning, men slik at dette behovet blir vurdert frå neste år.

Når det gjeld tannhelseforskning så er det inngått ein avtale med NSD (Norsk senter for forskingsdata). Formålet med avtalen er at NSD skal bistå fylkeskommunen med å sikre og påvise at behandling av personopplysningar til forskingsformål skjer i samsvar med personvernforordningen, personopplysningsloven og helselovene (personvernregelverket). I samband med denne avtalen er det inngått ein databehandlaravtale mellom partane samt utarbeidd rutinar internt for å avklare rollar og ansvar i verksemda. På sikt vil det vere naturleg at fylkeskommunen tek denne oppgåva tilbake til eiga verksemd, men det er tenleg med ein slik avtale no slik at forskingsprosjekta vert sikra framover.

Saman med It avdelinga og ekstern konsulent er det ut året prioritert å få på plass policy og rutinar for informasjonssikkerhet og personvern for Vestland fylkeskommune. Vidare er arbeid med behandlingsprotokollar eit prioritert område.

Elev- og pasientdata er særskilt kritiske verdiar for fylkeskommunen, og det må såleis også prioriterast å gjere risiko og personvernkonskvensvurderingar for våre systemløysingar i denne samanheng. Dette er eit krevjande arbeid som må tas ansvar for inn i Vestland fylkeskommune.

Det meldast jevnleg inn sikkerheitsbrot til Datatilsynet. Datatilsynet si tilbakemelding på desse har så langt vore at ein legg verksemdas forklaring på sikkerheitsbrotet til grunn, men slik at dei blir handtert slik som aktuelle tiltak har vore forklart i kvart tilfelle ovanfor tilsynet.

Tilsvarande må ny fylkeskommune ta ansvar for at:

- Roller og ansvar vert definert og dei som har ansvar må forstå kva ansvaret inneber.
- Målsetting for personvern i verksemda vert forankra i toppleiinga og tydeleggjort og etterlevast i ansvarlinja og verksemda elles.
- Policy og rutinar vert implementert i verksemda og vere ein del av eit internkontrollsystem.
- Det er tydeleggjort kva som er våre informasjonsverdiar og at desse klassifiserast i henhold til konfidensialitet, integritet og tilgjengelighet.
- Når verksemda skal sikre riktig prioritering og etterleving av lovpålagte krav leggjast risiko- og personvernkonsekvensvurderingar til grunn for avgjersler.
- Det ligg føre rutinar for forsvarleg tilgangsstyring til våre informasjonsverdiar og system.

Det er framleis ein omfattande jobb å gjere for å etterleve lovpålagte plikter etter personvernlovgjevinga.