HORDALAND FYLKESKOMMUNE
ØKONOMI - OG ORGANISASJONSAVDELINGA
Stab - Øk - og org avd

Notat

Dato: 11.09.2018
Arkivsak: 2018/7931-2
Saksbehandlar: marseim

Til:	Kontrollutvalget
Frå:	Konstituert fylkesrådmann

Status ny personvernlovgjeving i Hordaland fylkeskommune

Ny personvernlovgjeving 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 personvernlovgjeving. Fylkesrådmannen ga ein status for arbeidet i møtet 05.02.2018 og Kontrollutvalet ba fylkesrådmannen om ein oppdatert status for arbeidet til møtet i september 2018.

I det følgjande gis først ei oppdatert status på spørsmåla frå Kontrollutvalet av 05.02.2018, under punkt I, og under punkt II gis ei status på dei hovudpunkta som blei påpeikt i KPMG si Gap-analyse gjennomført i Hordaland fylkeskommune hausten 2017 som ikkje er nemnd under punkt I.

I. Oppdatert status på spørsmåla frå Kontrollutvalet av 05.02.2018:

1. Er det nokon som jobbar med ny personvernlov?

Hordaland fylkeskommune og Skyss har eit betydeleg arbeid framfor seg for å sikre at interne system, rutinar, prosedyrar og rolleavklaringar er i samsvar med det nye regelverket. Det er utarbeidd ein overordna tiltaksplan, som Økonomi- og organisasjonsavdelinga på vegner av fylkesrådmannen følgjer opp gjennom eit eiget prosjekt.

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 ligg hos kvar einingsleiar, og det er naudsynt at desse samarbeider med sin personvernkoordinator. Personvernkoordinatorane vil vere knytt til eit regelbundet samarbeid med personvernombodet for å få tilført kompetanse og utveksle erfaringar med kvarandre.

It seksjonen med blant anna nytilsett sikkerheitsrådgjevar har også arbeidsoppgåver knytt til personvernlovgjevinga.

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 fleire enn 100 behandlingar som kvar for seg inneheld behandling av personopplysningar og særlege kategoriar av personopplysningar (etter tidlegare lovgjeving omtalt som sensitive personopplysningar). Tilsvarande har fylkeskommunen 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.

Dei ulike avdelingane har etter møte med personvernombod og sikkerheitsansvarleg blitt gitt ein innføring i korleis ein skal svare på spørsmåla i protokollen og dei er gitt eit ansvar for å rapportere tilbake i forhold til dei prosessane dei finn i eiga avdeling for dette. Når det gjeld skulane, ble det i vår satt ned ein pilot av fire skular som har gjennomført denne kartlegginga. For resten av skulane vil denne kartlegginga fortsette hausten 2018 og våren 2019. Tilsvarande gjeld for tannhelsetenesta. Status for protokollane er at det arbeidast med å kartlegge personopplysningane i verksemda.

Dette 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 gjere dette til ein del av internkontrollen.

Det er og naudsynt å etablere rutinar som sikrar at dei vurderingane som protokollane legg opp til at behandlingsansvarleg skal ha kontroll på, blir evaluert ved innkjøp av nye system eller når nye rutinar skal endrast i avdelingar og verksemda for øvrig.

3. **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.

Det er no utarbeidd ein databehandlaravtalemal etter nye personvernreglar som skal vere HFK sin formelle avtale i kontakt med leverandørane. Denne vil vere tilgjengeleg i Kvalitetsportalen i norsk og engelsk versjon.

Å prioritere å få kontroll på leverandørsida er viktig og det arbeidast det med. Det er frå august 2018 satt i gang eit arbeid med ekstern hjelp frå rådgjevingsfirmaet Karabin for å få på plass databehandlaravtalar i samsvar med nytt regelverk og for å få ein samla oversikt over våre sentrale leverandørar.

Karabin vil på vegne av HFK i første omgang følgje opp 80 leverandørar med nye databehandlaravtalar. Det er påreknеleg at nokon av våre leverandørar ønskjer å bruke si eiga mal på avtalen og / eller vil forhandle på innhaldet i avtalen. Det må derfor påreknast noko tid før denne prosessen er heilt ferdig.

Oppfølging av databehandlaravtaler skal vere ein del av HFK sitt internkontrollsystem. Skal ein kunne klare å få dette til, må det etablerast eit felles verktøy for denne typen av kontraktsoppfølging. Fleire sentrale avdelingar, mellom anna IT og Innkjøp, bør sjå på løysinger for dette.

4. Er det oppretta personvernombod / rådgjevar?

Etter ny personvernlovgjeving 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 rolla som personvernrådgjevar, og det må takast høgde for at dette kan medføre interessekonflikt og / eller bli oppfatta å råke ved integritet og habilitet hos vedkommande. Det er derfor lagt inn i arbeidsinstruksen for stillinga at ordninga med denne todelinga skal evaluerast i desember 2018.

Personvernombodet har og ombudsrolla for fylkeskommunen i Sogn og Fjordane, men slik at dei sjølv tek ansvar for å byggje 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 nyoppretta nasjonalt nettverk for fylkeskommunale personvernombod. Det er teneleg at omboda jobbar i fellesskap om felles løysingar for felles utfordringar og skapar likeins rutinar det det er fornuftig.

5. Er personvernerklæringa oppdatert?

Hordaland fylkeskommune har nokre personvernerklæringar i dag. Desse vil bli oppdaterte i tråd med ny personvernlovgjeving. I løpet av hausten 2018 vil erklæringar for gruppene elevar, pasientar og tilsette vere på plass.

6. Er det innebygd personvern i datasystem?

I samband med arbeidet med å oppdatere databehandlaravtalane med leverandørsida, vil ein i denne samanheng kunne få ein oversikt over kva løysinger leverandør har for innebygd personvern. Innebygd personvern er i stort monn knytta til tekniske løysinger, men må og implementerast i arbeidsrutinar (til dømes kven i ei avdeling skal ha tilgang til bestemte system, manuelle sletterutinar, sletting manuelt av e-postar i Outlook).

IT-seksjonen jobbar kontinuerleg med å sikre at alle HFK sine IT-løysinger er i samsvar med GDPR krav. Det gjelder både eksisterande løysinger og framtidige IT-løysinger for Vestland fylkeskommune.

Eksisterende system:

- Vi følgjer Datatilsynet sine anbefalinger.
- Oppdaterer eksisterende tekniske og administrative rutiner for IT, som skal bidra til å forbedre IT-sikkerheitsnivå og sikkerheit til personopplysninger til dømes ny passordrutine og sletting av kontoer til tidlegare ansatte.
- Utarbeider nye IT-prosedyrer som skal heve IT-sikkerheitsnivå: Til dømes IT si håndtering for avvik på sikkerheit.
- Jobbar kontinuerleg med å forbedre tekniske løysinger for blant anna tilgangskontroll, autentisering
    - f.eks.2-faktor pålogging for eFeide.

- Å Gjere penetrasjonstester på system eksponert mot Internett for å avdekke mulige eksisterande avvik som kan føre til personvernbrudd.
- Vi er i prosess med å etablere ny databehandlaravtalemal som overholder GDPR krav
- Kartlegge dataflyt, formål og heimel.

IT-løysinger som skal anskaffes:

- IT-sikkerheitsrådgjevar og verksemdsarkitekt sikrar fokus på personvern gjennom deltaking i delprosjekt som tar for seg anskaffelse av nye IT system for Vestland fylkeskommune.
- IT avdelingene i SFFK og HFK er i prosess med å etablere eit prosjekt for verksemdarkitektur for Vestland fylkeskommune som følgjer TOGAF rammeverket.
- Prinsipp for sikkerheit og personvern skal vere ein integrert del av Vestland fylkeskommune sin arkitektur.
    - Overordna prinsipp for sikkerheit og personvern vil utarbeidast.
    - I tillegg må behov for ytterlegare sikkerheitstiltak og personverntiltak vurderast for kvart tilfelle.

7. 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.

II. Status for dei hovudpunkta som blei påpeikt i KPMG si Gap-analysen gjennomført i Hordaland fylkeskommune hausten 2017 som ikkje er nemnd under punkt I:

Som gap analysen beskriv må det på plass interne rutinar, malar / policy dokumenter for personvern og informasjonssikkerheit for å sikre dei registrertes rettigheter: Til dømes rutinar for førespurnad om sletting, innsyn, korrigering, dataportabilitet og rutine ved brot på sikkerheit.

Hordaland fylkeskommune har ein omfattande jobb å gjere for å innfri lovpålagte plikter etter ny personvernlovgjeving og det er naudsynt at leiarar og ansvarleg tilsette tek sitt ansvar. Vidare er det naudsynt å gjere prioriteringar på kva oppgåver / krav som er viktigast å få på plass først.

Ein ser det som teneleg å prioritere å sikre at HFK har inngått naudsynte databehandlaravtalar med våre leverandørar og dette er eit arbeid som prioriterast for hausten 2018. Tilsvarande er arbeidet med å få oversikt over våre behandlingar av personopplysningar og protokollera desse. Dette er eit pågåande arbeid og som ein må gjere opp status for våren 2019. HFK er ein stor verksemd og det er krevjande å få denne dokumentasjonen på plass og vedlikehalde den. Å få på plass nødvendige rutinar, informasjon, prosedyrar heng saman med dei to nemnde arbeidsprosessane og det er ei målsetting at mykje av dette er på plass vinteren 2019.