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

Notat

Dato: 18.05.2018
Arkivsak: 2018/11165-1
Saksbehandlar: torrutl

Til:	Fylkestinget
Frå:	Fylkesrådmannen

Spørsmål frå representanten Geir Angeltveit knytt til framlegg av ny IT-strategi for Hordaland fylkeskommune, sak 2018/3423, i fylkestinget 6. mars 2018

Bakgrunn
I samband med framlegg til ny IT-strategi for Hordaland fylkeskommune i fylkestinget i mars kom det følgjande spørsmål frå Geir Angeltveit (V):

1. Korleis ser ein for seg at personvern skal bli forankra?
2. Korleis sikre og etterleve krav til databehandlaravtalar med leverandørar?
3. I kva grad tenker ein at øvste leiar skal haldast underretta om status og avvik på slike avtalar?

Fylkesdirektør økonomi og organisasjon svara at fylkesrådmannen har sett i gang eit omfattande arbeid i samband med innføringa av EU si nye personvernforordning (GDPR) som trer i kraft i Noreg i 2018, og tilpassing til denne for Hordaland fylkeskommune. Arbeidet er organisert som eit prosjekt under leiing av fylkesdirektør økonomi og organisasjon og rapporterer til fylkesrådmannen. Som del av prosjektarbeidet er alle fylkeskommunen sine systemleverandørar kontakta for å avklare i kva grad dei er budd for GDPR samstundes som vi søkjer å inngå nye og oppdaterte databehandlaravtalar. Det er fylkesrådmannen som er ansvarleg for handsaminga av personopplysningar i regi av Hordaland fylkeskommune og han vert fortløpande orientert om eventuelle avvik/brot på regelverket samt status for arbeidet med tilpassing til dei nye reglane.

Representanten Torstein Gunnarson (V) følgde opp dette, og meinte at representanten Angeltveit sine spørsmål ikkje vart tilfredsstillande svara ut.
Fylkesrådmannen svara at administrasjonen ville kome attende med meir utdjupande informasjon.

Svar frå fylkesadministrasjon

1. Korleis ser ein for seg at personvern skal bli forankra?

Svar:
Vern av personopplysningar er ein viktig del av arbeidet med informasjonstryggleik. Sikring av informasjonssystema gjerast på nettverks- eller systemnivå, men informasjonstryggleik omfattar i tillegg tiltak som fysisk tryggleik (dørlåsar, tilgangskontroll), personellstyring (opplæring), juridisk støtte, organisasjon, prosessar og avtalar med leverandørar.

GDPR stiller ein del nye krav til handsaming av personopplysningar. Som fylkesdirektør økonomi og organisasjon svara i fylkestinget 6. mars, så har fylkesrådmannen sett i gang eit omfattande arbeid for

tilpassing til GDPR i Hordaland fylkeskommune. Alle systemleverandørar har blitt kontakta for å få avklart i kva grad dei er budd for GDPR. Vidare er det internt i Hordaland fylkeskommune peika ut ansvarlege i alle fagavdelingane for å koordinere arbeidet med å sjå på arbeidsprosessar, rutinar, retningsliner og system sett opp mot behandlingsformål.

Det er fylkesrådmannen som har det overordna, formelle ansvaret for informasjonstryggleik i Hordaland fylkeskommune. I tråd med mål og strategi for informasjonstryggleik i Hordaland fylkeskommune har fylkesrådmannen delegert det operative, daglege arbeidet til fylkesdirektør økonomi og organisasjon.

Vidare er det linjeleiinga sitt ansvar at tryggleiksarbeidet vert utøvd og kontrollert ut frå fastsette krav og rutinar. Linjeorganisasjonen har såleis ansvar for å praktisere arbeidet med informasjonstryggleik og å gjennomføre lokal internkontroll.

Økonomi og organisasjonsavdelinga har peika ut to tryggleiksansvarlege, ein administrativ ansvarleg (rådgjevar informasjonstryggleik) og ein it-teknisk ansvarleg (rådgjevar it-tryggleik) som aktive støttespelarar for dei avdelingsansvarlege. Dei tryggleiksansvarlege skal årleg rapportere status for arbeidet til leiinga.

Avdelingsdirektørane har ansvaret for at fylkeskommunen sine mål og strategiar for informasjonstryggleik vert følgde opp i eiga avdeling og at det vert drive systematisk og kontinuerleg arbeid med personvern.

Seksjonsleiarar/einingsleiarar/rektorar har ansvar for at fylkeskommunen sine mål og strategiar for informasjonstryggleik vert følgde opp i eigen seksjon/eining/skule og at det vert drive systematisk og kontinuerleg arbeid med personvern.

2. Korleis sikre og etterleve krav til databehandlaravtalar med leverandørar?

Svar:
Hordaland fylkeskommune sin bruk av leverandørar vert regulert av kontraktar der også avtalepunkt om informasjonstryggleik skal inngå. Der systemet handsamar personopplysningar, skal desse delane av kontrakten normalt skiljast ut i eigen *databehandlaravtale*, etter mal frå Datatilsynet. Avtalen skal innehalde oversikt over personopplysningar som vert handsama, samt kva tilgang Hordaland fylkeskommune har til innsyn i og måling av sikringstiltak og tryggleiksrevisjonar. Avtalane skal også innehalde ein SLA – *service level agreement*.

I den grad tilsette hos partnarar eller leverandørar får tilgang til personopplysningar eller til utstyr eller programvare som behandlar personopplysningar, skal fylkeskommunen sikre seg oversikt over kven som har slik tilgang. Fylkeskommunen skal syte for at dei aktuelle personane underteiknar *fråsegn om teieplikt*, der det ikkje allereie eksisterer ein Databehandlaravtale som dekkjer dette behovet.

I samband med arbeidet for å tilpasse drifta i Hordaland fylkeskommune til GDPR vert alle databehandlaravtalar gjennomgått. Datatilsynet hadde ikkje publisert ny mal ved førre fylkesting, så fylkeskommunen hadde difor ikkje oppdatert mal til dette arbeidet. Slik det ser ut no vil Datatilsynet utarbeide ei rettleiing knytt til nytt regelverk, og ikkje mal, som Hordaland fylkeskommune må tilpasse eiga verksemd.

3. I kva grad ein tenker at øvste leiar skal haldast underretta om status og avvik på slike avtalar?

Svar:
Kvar leiar og medarbeidar er ansvarleg for å rapportere brot og moglege brot på tryggleiken i tråd med rutinar for avvikshandsaming. Rapporteringa går linjeveg. Alvorlege hendingar som påverkar informasjonstryggleiken skal alltid rapporterast til rådgjevar informasjonstryggleik.

Ved alvorlege hendingar skal rådgjevar informasjonstryggleik og personvernombod involverast i oppfølging og avgjerder rundt korrigerande tiltak knytt til hendinga. Om personopplysningar er på avvege skal alltid Datatilsynet orienterast. Varsling til Datatilsynet skal koordinerast av personvernombod.

Fylkesrådmannen skal alltid orienterast om alvorlege hendingar som gjeld personvern, inklusiv avvik på databehandlaravtalar.