HELSETJENESTENS DRIFTSORGANISASJON
Nødnett

Saksframlegg

Referanse

Saksgang:

Styre	Møtedato
Styret Helsetjenestens driftsorganisasjon for nødnett HF	11. juni 2018

SAK NR 25-2018 HDO GDPR og personvern

Forslag til vedtak:

1. Styret tar saken til orientering.
2. Styret har, basert på orienteringen fra administrerende direktør, fått tydelighet på at HDO vil følge GDPR, med de justeringer som gjøres i normen.

Gjøvik, 4. juni 2018

Lars Erik Tandsæther
Administrerende direktør

SAK NR 25-2018 HDO GDPR og personvern

1 Administrerende direktørs anbefaling

Administrerende direktør anbefaler at:

1. Styret tar saken til orientering.
2. Styret har, basert på orienteringen fra administrerende direktør, fått tydelighet på at HDO vil følge GDPR, med de justeringer som gjøres i normen.

2 Faktabeskrivelse

Saken legges fram for Styret for å orientere om status og framdrift i arbeidet med GDPR og personvern i HDO.

2.1 Rammer for arbeidet med personvern i HDO

EUs forordning for personvern (GDPR) blir norsk lov i 2018. Eksakt tidspunkt for når forordningen trer i kraft er ikke fastsatt - ifølge Datatilsynet tidligst ila. juli. Loven vil gjelde for alle norske virksomheter som behandler personopplysninger, derfor også HDO.

I følge **Oppdragsdokument** 2018 fra eierne skal HDO blant annet:

> «… *sørge for tilfredsstillende informasjonssikkerhet med utgangspunkt i vurdering av risiko og sårbarhet, og oppfølging gjennom internkontroll, og styrke kompetansen….»*
>
> *«… holde seg orientert om arbeidet med personvernforordningen, og gjøre nødvendige forberedelser for å implementere nytt regelverk…»*

Normen (Bransjenorm for personvern og informasjonssikkerhet i helse- og omsorgstjenesten) stiller krav til HDOs informasjonssikkerhet for helse- og personopplysninger som behandles i forbindelse med anmodning og tilbud om og ytelse av helsehjelp og tjenester.

Som en følge av ny lov for behandling av personopplysninger, revideres Normen. Etterlevelse av de kravene som stilles i Normen vil således også sikre etterlevelse av GDPR. Versjon 6 av Normen vil være en fullstendig revidert utgave tilpasset GDPR og er planlagt til vinteren 2019. I dag foreligger versjon 5.3. Denne er restrukturert og tilpasset slik at det ikke er avvik mellom Normen og de krav som stilles i GDPR.

2.2 Kort om status personvern i HDO

HDO har i sitt arbeid med personvern og informasjonssikkerhet ivaretatt mange av kravene som stilles i oppdrag, norm og lovgivning. Dette omfatter blant annet fokus på informasjonssikkerhet generelt, oversikt over systemer som behandler personopplysninger, gjennomføring av risikovurderinger, sikkerhetshåndbok, databehandleravtaler og taushetserklæringer.

Etablering av DPO i kontrollerende rolle (personvernombud) sammen med etableringen av operativt ansvar for personvern, tilfredsstiller både krav om personvernombud iht. GDPR, og er samtidig en god måte å operasjonalisere arbeidet med personvern.

Innleie av eksterne ressurser innenfor informasjonssikkerhet og personvern bidrar med kompetanse, framdrift og kvalitet på arbeidet med personvern. Innleie er planlagt gjennom hele 2018. I forlengelsen av dette vil det være fokus på å overføre kompetanse knyttet til personvern og GDPR til organisasjonen i HDO generelt og spesielt til personvernombudet (DPO).

2.3 GDPR aktiviteter 2018

Med bakgrunn i oppdrag, ny personvernlovgivning og seneste versjonen av Normen:

- Plan personvern og implementering av GDPR er etablert
- Oversikt og kategorisering av behandlinger er gjennomført
- Videreføre kartlegging av behandlinger av helse- og personopplysninger.
- Etablere og implementere styringssystem for å ivareta krav i GDPR og i Normen (v5.3) (høst 2018).
- Bidra til implementering av personvernombud og implementering av operativt ansvar for personvern (påbegynt).
- Utarbeide og inngå databehandleravtaler basert på de krav som stilles i GDPR og Normen (påbegynnes juni 2018).

Følgende punkter vil påbegynnes i 2018 og videreføres inn i 2019:

- Implementere arbeidet med personvern i virksomheten, herunder gjennomføre opplæring.
- Lukke avvik og forbedre arbeidet med personvern iht. den gjennomførte kartleggingen.

Løpende fokusområder:

- Risikovurdering – videreutvikle risikostyringssystemet og herunder styrke ivaretakelse av personvern, sikre identifisering av vesentlige risikoer, ivareta konsekvensvurdering i forhold til personvern samt tydeliggjøre forhold mellom risiko og avvik.
- Avvikshåndtering - forsterke bruk av system for rapportering av avvik knyttet til personvern og informasjonssikkerhet
- Styringssystem - ivareta personvern innenfor HDOs styrende dokumentasjon og HDOs formelle styringssystem som del av dette.
- Opplæring - styrking av kompetanse innenfor personvern, GDPR og Normen hos personer med nøkkelroller og øvrig ansatte.

2.4 Om kartleggingen av behandling av helse- og personopplysninger

Kartlegging av behandling av sensitive personopplysninger er allerede iverksatt og gjennomført, og tilhørende risiko og sårbarhetsanalyser pågår. Kartleggingen av ytterligere behandling er planlagt gjennomført i løpet av juni 2018. Kartleggingen omfatter de krav som stilles i GDPR der HDO er behandlingsansvarlig for egne opplysninger og der HDO behandler opplysninger på vegne av andre. Det prioriteres de behandlinger og systemer der HDO er databehandler og behandler opplysninger på vegne av helseforetak og kommuner som er underlagt Normen.

Formålet med kartleggingen er:

- å dokumentere behandlingen i henhold til GDPRs krav om protokoll
- avdekke avvik (GAP) i forhold til de krav som stilles til HDO som databehandler og behandlingsansvarlig
- identifisere tiltak for å lukke avvik/redusere GAP
- utvikle kompetanse hos nøkkelpersoner iht. de krav som stilles i GDPR

2.4 Om styringssystem (internkontroll)

GDPR stiller krav om styring og kontroll på flere områder, men angir ikke noe eksplisitt krav om et styringssystem. Normen er mer konkret og stiller krav om at v*irksomhetens øverste ledelse skal etablere styringssystemet og gjøre dette kjent i virksomheten*. HDOs styringssystem innenfor personvern skal utvikles for å etterleve GDPRs til krav om styring og kontroll samt etterlevelse av de krav som stilles Normen. Styringssystemet etableres innenfor rammene av HDOs formelle styringssystem.

3 Administrerende direktørs vurderinger

Administrerende direktør mener det er viktig at Styret er inneforstått med arbeidet for ivaretakelse av personvernet og implementering av de krav som stilles i GDPR og i kommende versjoner av Normen.

HDO legger i dag stor vekt på å ivareta informasjonssikkerheten på alle steder der personopplysinger behandles. En rekke av tiltakene som kreves i GDPR og Normen er allerede implementert i form av risikovurdering, avvikshåntering, sikkerhetshåndbok, tekniske og organisatoriske sikkerhetstiltak, personvernombud m.m. HDOs styringssystem vil gi gode rammer for etterlevelse av de krav som stilles både i GDPR og Normen.

Det videre arbeidet vil bestå i å sikre at HDO etterlever GDPR i sin helhet og deretter de krav som stilles i ny versjon av Normen. God opplæring og øvrige personverntiltak skal sikre en god kultur for ivaretakelse av personvernet i alle deler av organisasjonen. Plan for dette arbeidet er etablert, og tiltak iverksatt. Admininstrerende direktør mener at bistand fra ekstern fagkompetanse er sentralt for å sikre gjennomføring i henhold til de planer som legges. Planen inkluderer også en overlevering til og opplæring av HDOs organisasjon.

Admininsterende direktør mener at de planer og tiltak som nå er iverksatt er dekkende for de krav som stilles til personvern, og at HDO er godt rustet til å innføre disse i takt med kommende revisjoner av Normen.