Sykehuset Innlandet HF
Styremøte 01.06.18

SAK NR 049 – 2018
VEDTAK OM OVERTREDELSESGEBYR FRA DATATILSYNET

Forslag til

VEDTAK:

Styret tar saken til orientering.

Brumunddal, 25. mai 2018

Alice Beathe Andersgaard
administrerende direktør

SAKSFREMSTILLING

SAK NR. 049 – 2018

Sykehuset Innlandet mottok vedtak om overtredelsesgebyr fra Datatilsynet 19.04.18. Brevet med vedtaket er vedlagt. Datatilsynet viser til varsel om vedtak av 24.10.2017 og Sykehuset Innlandets svar av 2.01.2018. Datatilsynets varsel om vedtak gjelder pålegg mot Sykehuset Innlandet HF om å betale overtredelsesgebyr for brudd på bestemmelsene i pasientjournalloven, personopplysningsloven og personopplysningsforskriften i forbindelse med beslutningen om å tjenesteutsette driften av helseregionens IKT-infrastruktur.

Datatilsynets vurdering er at det er fem forhold i den konkrete kontraktsinngåelsen som etter datatilsynets vurdering innebærer brudd på bestemmelsene i pasientjournalloven § 22 og personopplysningsloven §§ l 3-15:

- De behandlingsansvarlige helseforetakene har ikke hatt tilstrekkelig eierskap til, eller kontroll med de planlagte endringene knyttet til informasjonssystemet.
- Helseforetakene har overlatt ansvaret for beslutninger som har betydning for pasientenes personvern og informasjonssikkerheten knyttet til behandling av personopplysninger, til databehandleren og til ansatte lenger ned i organisasjonen.
- Det ble ikke gjennomført nødvendige risiko- og sårbarhetsvurderinger før det ble besluttet å konkurranse utsette avtale om strategisk partnerskap, herunder drift og vedlikehold av IKT-infrastruktur.
- Det ble ikke gjennomført nødvendige risiko- og sårbarhetsanalyser i forkant av beslutningen om valg av underleverandør i Bulgaria.
- Valgt underleverandør har i et begrenset tidsrom hatt tilgang til pasientopplysninger i strid med ledelsens forutsetning om tilgangskontroll.

Datatilsynet mener det er svært alvorlig at denne avtalen ble inngått uten at det forelå tilstrekkelige risikovurderinger og uten at restrisiko ble vurdert og akseptert av de behandlingsansvarlige i forkant av avtaleinngåelsen.

Datatilsynets endelige konklusjon

Datatilsynet har vurdert kommentarene fra Sykehuset Innlandet HF i brev av 2.01.2018, og tar disse til etterretning.

Konklusjonen er at det ikke er gjort innsigelser som påvirker vurderingen av avvik eller vurderingen av om overtredelsesgebyr bør ilegges. Størrelsen på gebyret er uendret.

Administrerende direktørs vurdering

Sykehuset Innlandet aksepterer foretaksboten på kr. 800.000 fra Datatilsynet. Det er viktig at Sykehuset Innlandet er bevisst ansvaret som databehandlingsansvarlig, følger opp databehandlere og styrker arbeidet med relevante risikovurderinger og restrisiko.

Erfaringene og oppfølgingspunktene av denne saken vil bli tatt inn i det pågående arbeidet med å innføre ny personopplysningslov i virksomheten som trer i kraft 1. august i år.
Som oppfølgingspunkter vil Sykehuset Innlandet se på avtalen med Sykehuspartner HF, regeletterlevelse generelt på området, innføringen i helseforetaket og kunnskapsheving/opplæring. Det vil komme en egen styresak om tema informasjonssikkerhet og ny personvernlovgivning (GDPR) i septembermøtet.