FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Pensjonskassen For Helseforetakene I Hovedstadsområdet
Karenslyst Allé 2
0278 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
22/5194			27.09.2023

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Pensjonskassen For Helseforetakene i Hovedstadsområdet (pensjonskassen) 28. juni 2022 etter å ha varslet om tilsynet 10. mai 2022.

Hensikten med tilsynet var å gjøre en vurdering av hvordan styring og kontroll med IKT-området blir ivaretatt, og med et særskilt fokus på hvordan pensjonskassen ivaretar risikostyring på IKT-området, hvordan IKT-området håndteres i pensjonskassens arbeid med beredskap- og kontinuitet, utkontraktering av IKT-tjenester og temaer innen IKT-sikkerhet.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport av 16. mars 2023 og styrets svar av 28. april 2023.

I styrets svar på foreløpig rapport ble det vist til at foreløpig rapport inneholdt henvisninger til Solvens II-regelverket og retningslinjer (guidelines) som ikke var gjeldende for pensjonskasser. Finanstilsynet har tatt hensyn til dette ved utarbeidelse av tilsynsrapporten. Finanstilsynet anser imidlertid at EIOPAs retningslinjer for IKT-området[1], for utkontraktering av IKT-tjenester til skytjenesteleverandører[2] og for IKT-relevante temaer ifm. styring og kontroll[3], er etablert med utgangspunkt i omforente prinsipper og beste praksis. Finanstilsynet vurderer at EIOPA sine retningslinjer på IKT-området utdyper IKT-forskriften, finansforetaksloven og finanstilsynsloven sine bestemmelser.

Finanstilsynet har følgende merknader etter tilsynet:

1. IKT-Strategi

Det framgår av IKT-forskriften § 2 at foretaket skal fastsette en IKT-strategi for foretaket. Det er Finanstilsynets forventning at foretak som er omfattet av IKT-forskriften fastsetter en IKT-strategi som støtter opp under forretningsstrategien, og at styret og ledelse følger opp at implementeringen av IKT-strategien har nødvendig framdrift i forhold til forretningsmessige planer og målsetninger.

Finanstilsynets vurderte i foreløpig rapport at pensjonskassen ikke hadde fastsatt IKT-strategien i tråd med forventningene når det gjelder innhold, handlingsplan for implementering og en prosess for å følge opp implementeringen av IKT-strategien.

Styret skriver i sitt svarbrev at det vurderer at pensjonskassens policy for IKT ivaretar krav til innhold som følger av IKT-forskriften, men at styret ser at det kan etableres indikatorer som gjør at fremdriften på arbeidet med implementering av IKT-strategien blir mer målbar. Videre framgår det av styrets svar at det i

[1] "EIOPA Guidelines on information and communication technology security and governance" (EIOPA-BoS-20/600)
[2] "EIOPA Guidelines on outsourcing to cloud service providers" (EIOPA-BoS-20-002)
[3] "EIOPA Guidelines on system of governance" (EIOPA-BoS-14/253)

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Jarleif Lødøen
Dir. tlf. 22 93 98 00

forbindelse med revisjon av IKT-policyen vil bli utarbeidet et vedlegg med en handlingsplan som beskriver aktiviteter som skal sikre måloppnåelsen på IKT-området.

Finanstilsynet pekte i foreløpig rapport også på at pensjonskassen bør etablere en prosess for overvåking og oppfølging av handlingsplanene.

Styret skriver i sitt svar at pensjonskassen vil etablere prosess for overvåking og oppfølging av handlingsplanene.

Finanstilsynet tar styrets svar til etterretning.

2. Ansvar og roller på IKT-området

Det vises til IKT-forskriften § 2, første og tredje ledd, hvor det stilles krav til at IKT-prosessene er spesifisert og dokumentert. Dette for å sikre ansvar og myndighet for utførelsen av den enkelte IKT-prosess.

Finanstilsynet pekte i foreløpig rapport på at pensjonskassen må se til at de enkelte prosessene, som inngår i IKT-oppgavene som er tildelt de ulike IKT-rollene, er spesifisert og dokumentert, og at ansvar og myndighet i den enkelte prosess blir klarlagt.

Styret skriver i sitt svar at ansvar og roller er beskrevet i pensjonskassens policy for IKT, policy for utkontraktering og i stillingsbeskrivelsene til relevante fagsjefer. Finanstilsynet registrer imidlertid at styret ser at det er behov for tydeliggjøring av stillingsbeskrivelsene i forhold til de enkelte prosessene, som inngår i IKT-oppgavene som er tildelt de ulike IKT-rollene.

Finanstilsynet tar styrets svar til etterretning.

3. Ledelsen og styrets oppmerksomhet på IKT-området

Det vises til finansforetaksloven § 13-5, første ledd om at foretaket skal ha hensiktsmessige retningslinjer og rutiner for å sikre en betryggende styring og kontroll med foretakets virksomhet, også for IKT-virksomheten.

Finanstilsynet pekte i foreløpig rapport på at den formelle periodiske rapporteringen fra IKT-området til pensjonskassens ledelse om status på IKT-området er begrenset. Finanstilsynet registrerte imidlertid at pensjonskassens kvartalsvise risikostyrings- og etterlevelsesrapportering omfatter noen relevante IKT-temaer.

Videre ble det pekt på at i statusrapporteringen til pensjonskassens ledelse bør det for eksempel redegjøres for driftsstatus, relevant informasjon knyttet til IKT-sikkerhet, eventuelle uforutsette avvik/hendelser, status på prosjekter og status på handlingsplanen for implementering av IKT-strategien.

Det følger av styrets svar at styret er av den oppfatning at det mottas en oppdatert status på IKT-området som er i tråd med finansforetaksloven § 13-5 første ledd gjennom styresaker i henhold til styrets årshjul. Finanstilsynet registrer at pensjonskassen framover vil samle og behandle rapportering på IKT-området som en egen sak i ordinære styremøter og at det i statusen vil redegjøres for driftsstatus, relevant informasjon knyttet til IKT-sikkerhet, uforutsette avvik/hendelser spesielt knyttet til IKT-virksomheten og status på handlingsplanen for implementeringen av IKT-policyen.

Finanstilsynet tar styrets svar til etterretning

4. Andrelinjen (etterlevelse og risikostyring)

Det vises til finansforetaksloven § 8-6, første ledd hvor det framgår at styret har ansvar for at foretaket er forsvarlig organisert, også for IKT-virksomheten, herunder påse at foretaket har forsvarlige styrings- og kontrollsystemer. Videre at daglig leder har ansvaret for at forsvarlige styrings- og kontrollsystemer er

etablert, jf. finansforetaksloven § 8-11, tredje ledd. De etablerte styrings- og kontrollordningene skal være klare og hensiktsmessige, jf. § 13-5, første ledd.

I foreløpig rapport pekte Finanstilsynet på at det er Finanstilsynets forståelse at pensjonskassens etterlevelses- og risikostyringsfunksjon vurderer og følger opp pensjonskassens IKT-virksomhet på et overordnet nivå, men at den ikke stiller krav til eller gjør vurderinger av mer teknisk/IKT-faglig karakter. Videre stilte Finanstilsynet spørsmål ved om pensjonskassen har tilstrekkelig kompetanse til å vurdere risikostyringen på IKT-området, og om valgt organisering sikrer kravet om uavhengighet i andrelinjens vurdering og rapportering av etterlevelse og risiko på IKT-området til styret.

Av styrets svar framgår det at pensjonskassens kritiske eller viktige leverandører er pålagt å ivareta forskrift for IKT og risikostyring og internkontroll slik kravene er utformet i forskrift for pensjonsforetak. Leverandørene av IKT-tjenester skal årlig rapportere til leder for etterlevelse (compliance) i pensjonskassen om at virksomheten er innrettet slik at alle nevnte lov- og forskriftskrav etterleves. Leverandørene skal videre bekrefte at de minimum har en årlig risikovurdering av alle operasjonelle forhold som berører tjenester til pensjonskassen, herunder IKT-området. Det er styrets oppfatning at valgt organisering sikrer kravet om uavhengighet i andrelinjes vurdering og rapportering av etterlevelse og risiko på IKT-området til styret.

Finanstilsynet merker seg fra styrets svar at styret vurderer at den valgte organiseringen sikrer kravet til uavhengighet. Finanstilsynet vil likevel understreke at pensjonskassen sin uavhengige risikostyringsfunksjon må ha tilstrekkelig kompetanse og ressurser, og at risikostyringsfunksjonen må sørge for at det er etablert prosedyrer som sikrer at alle vesentlige IKT-risikoer i pensjonskassen er identifisert, målt og rapportert av de relevante organisatoriske enhetene.

5. Overordnet risikostyring

IKT-forskriften § 2, første ledd stiller krav til at foretaket skal fastsette overordnede mål, strategier, og sikkerhetskrav for IKT-virksomheten. Videre skal foretaket *"minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres"* jf. IKT-forskriften § 3.

I foreløpig rapport var det Finanstilsynets vurdering at pensjonskassen ikke har fastsatt kriterier for akseptabel risiko forbundet med IKT-virksomheten. Finanstilsynet påpekte at pensjonskassen bør utarbeide en rutine som sikrer at vesentlige risikoelementer og årsakssammenhenger analyseres med tanke på å identifisere og kvantifisere IKT-risiko. Basert på fastsatte kriterier for akseptabel IKT-risiko bør rutinen sikre at det iverksettes risikoreduserende tiltak som sikrer at IKT-virksomheten drives innenfor pensjonskassens risikotoleranse.

Det framgår av styrets svar at pensjonskassen har fastsatt kriterier for akseptabel risiko forbundet med operasjonell risiko (herunder IKT-virksomheten). Videre har pensjonskassen en policy for operasjonell risiko som gir retningslinjer på hvordan risiko skal kartlegges og måles, samt en rutine for registrering av hendelser som gir veiledning på hvordan avvik skal måles innenfor forskjellige prosesser.

Finanstilsynet tar styrets svar til etterretning.

6. Rapportering av IKT-risiko

Etter finansforetaksloven § 8-6, fjerde ledd, skal styret føre tilsyn med den daglige ledelse og foretakets virksomhet ellers, og sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet. IKT-forskriftens § 3 stiller videre krav om at det minst årlig skal gjennomføres risikoanalyser på IKT-området.

Finanstilsynet pekte i foreløpig rapport på at pensjonskassens styre må sikre at førstelinjen løpende vurderer og rapporterer risiko knyttet til pensjonskassens IKT-virksomhet. Videre ble det pekt på at det er Finanstilsynets forventning at risikovurderinger, og rapportering av disse til ledelse og styre, er av tilstrekkelig omfang og frekvens.

Av styrets svar framgår det at pensjonskassens førstelinje minimum årlig skal rapportere risikovurderinger til administrerende direktør og risikostyrings- og etterlevelsesfunksjonen. Videre skal risikostyrings- og etterlevelsesfunksjonen rapportere årlig til styret om planlagt kontrollarbeid, hvor risikovurderingene i førstelinjen danner grunnlaget for dette arbeidet.

Finanstilsynet registrerer fra styrets svar at pensjonskassen vil forbedre sin vurdering av IKT-risiko hos leverandørene og risikoer som kan påvirke måloppnåelsen knyttet til handlingsplanen for implementering av IKT-policyen.

Finanstilsynet tar styrets svar til etterretning.

7. Driftsavbrudd og beredskap

Det vises til IKT-forskriftens § 11 om at foretaket har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret.

I foreløpig rapport pekte Finanstilsynet på at planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i forretningsmessige konsekvensanalyser for pensjonskassens kritiske forretningsprosesser. Disse analysene skal sikre at pensjonskassens beredskaps- og kontinuitetsplaner fastsettes på bakgrunn av systemenes forretningsmessige kritikalitet, og gi føringer for pensjonskassens prioritering for gjenoppretting av systemer.

Det framgår fra styrets svar at pensjonskassen ikke har etablert en forretningsmessig konsekvensanalyse siden det ikke gjelder rettslige krav for pensjonskasser om å etablere en slik. Pensjonskassen har en beredskapsplan for håndtering av informasjonskriser hvor kritikaliteten til de forskjellige systemene pensjonskassen bruker er beskrevet i eget vedlegg.

I styrets svar vises det videre til at pensjonskassen ikke har en formalisert beredskapsplan for systemer knyttet til kritiske forretningsprosesser hvor kritiske nedetider er dokumentert og som omfatter alternative løsninger for å opprettholde disse forretningsprosessene slik som ved manuell operasjon, bruk av andre systemer mv. Videre framgår det av styrets svar at pensjonskassen har igangsatt ett arbeid med å få på plass en beredskapsplan for pensjonskassen som ivaretar intern- og ekstern beredskap.

Finanstilsynet merker seg styrets svar og opprettholder sin vurdering om at planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i forretningsmessige konsekvensanalyser for pensjonskassens kritiske forretningsprosesser og at analysene skal sikre at pensjonskassens beredskaps- og kontinuitetsplaner fastsettes på bakgrunn av forretningsmessige kritikalitet, og gi føringer for pensjonskassens prioritering for gjenoppretting av systemer/løsninger.

Det vises til IKT-forskriften § 11 hvor det stilles krav til at pensjonskassen skal ha en dokumentert kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes. Videre at det minst årlig skal gjennomføres opplæring, øvelse og testing som viser at kriseløsningen virker som forutsatt og at resultatet av testen dokumenteres.

Finanstilsynets pekte i foreløpig rapport på at Finanstilsynet forventer at pensjonskassen fastsetter kriterier for iverksettelse av kriseplan og kriseløsninger og at det finnes opplærings- og testplaner som sikrer at pensjonskassens ansatte er forberedt på å håndtere alvorlige IKT-hendelser.

Finanstilsynet merker seg fra styrets svar at pensjonskassen har igangsatt et arbeid med beredskap hvor det også vil bli utarbeidet en opplæring- og testplan.

Finanstilsynet ber styret fastsette kriterier for når beredskapsplanen skal aktiveres, uavhengig av IKT-tjenesteleverandør, og med bakgrunn i de forretningsmessige konsekvensene ved avbrudd.

8. Leverandørstyring

Det vises til IKT-forskriften § 2, annet ledd, hvor det framgår at foretaket ha retningslinjer som sikrer at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Blant annet stilles det krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av § 2, fjerde ledd, at inngåelse og endring av IKT-utkontrakteringsavtaler skal styrebehandles, der styret skal presenteres en plan for utkontrakteringen, en risikovurdering og en beskrivelse av hvordan foretaket skal sikre leveransen.

I foreløpig rapport pekte Finanstilsynet på at pensjonskassen må sikre at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalene. Finanstilsynet stiller spørsmål ved om pensjonskassens første- og andrelinje er tilstrekkelig bemannet, samt har tilstrekkelig kompetanse til å følge opp utkontrakterte IKT-tjenester.

Fra styrets svar har Finanstilsynet merket seg at styret oppfatter at pensjonskassen har tilstrekkelig kompetanse i første- og andrelinje til å forvalte utkontrakteringsavtalene og at bemanningen er forholdsmessig. Styret skriver videre at pensjonskassen likevel vil lage en mer formalisert plan for videreutdanning innen IKT.

Finanstilsynet understreker viktigheten av at pensjonskassen har tilstrekkelig IKT-kompetanse for å kunne følge opp, og foreta hensiktsmessige kontroller av, utkontraktert IKT-virksomhet.

Finanstilsynet pekte i foreløpig rapport også på viktigheten av at pensjonskassen har kunnskap om mulighetene for å tre ut av den enkelte IKT-utkontrakteringsavtale og risiko knyttet til eventuell lock-in. Finanstilsynet ble informert om at risiko forbundet med å tre ut av de ulike IKT-utkontrakteringsavtalene ikke er vurdert.

Finanstilsynet registrerer fra styrets svar at pensjonskassen i kritiske eller viktige avtaler har inntatt bestemmelser om partenes plikter ved opphør av avtalen. Videre vil styret påse at bestemmelser som påpekt inntas i alle framtidige IKT-avtaler.

Finanstilsynet tar styrets svar til etterretning.

9. IKT-sikkerhet

IKT-forskriften § 5 stiller krav til at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal det finnes retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

Finanstilsynets pekte i foreløpig rapport på at pensjonskassen bør ha rutiner for styring og kontroll av IKT-sikkerhet for den utkontrakterte IKT-virksomheten og at pensjonskassen videre bør sikre at tjenesteleverandørene innfrir sikkerhetskravene pensjonskassen har besluttet i egen sikkerhetspolicy.

Av styrets svar framgår det at pensjonskassen vil følge opp at tjenesteleverandørene innfrir sikkerhetskravene, blant annet i leverandøroppfølgingen av pensjonskassens kritiske eller viktige IKT-leverandører.

Finanstilsynet tar styrets svar til etterretning.

10. Tilgangsstyring

IKT-forskriften § 5 stiller krav til retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

I foreløpig rapport pekte Finanstilsynet på at IKT-tjenesteleverandører til pensjonskassen må etablere løsninger for tilgangsstyring og kontrollrutiner som i størst mulig grad sørger for at tilganger tildeles og kontrolleres for det enkelte supportoppdrag.

I styrets svar framgår det at det er iverksatt et arbeid med tilgangsstyring for ansatte hos eksterne leverandører. I forbindelse med dette arbeidet er det ryddet opp i tilganger som ikke var begrunnet utfra tjenstlig behov.

Finanstilsynet tar styrets svar til orientering.

I foreløpig rapport ble det også pekt på at pensjonskassen må etablere rutiner for effektiv kontroll med bruken av data, både hos personell med utvidete tilganger og ordinære systembrukere hos IKT-tjenesteleverandørene, og at likelydende krav til rutiner for tilgangsstyring gjelder for den interne IKT-virksomheten.

I styrets svar framkommer det at pensjonskassen har rutiner for kontroll med bruken av data som også gjelder personell med utvidede tilganger. Det framkom videre at pensjonskassen har egne rutiner for kontroll med tilganger. Pensjonskassen vil foreta en vurdering av rutinene for å sikre effektiv kontroll av tilgangsstyring internt og eksternt.

Finanstilsynet tar styrets svar til etterretning.

11. Datakvalitet

IKT-forskriften § 4 stiller krav til at det skal fastsettes kvalitetsmål for de enkelte deler av IKT-virksomheten knyttet opp mot foretakets øvrige mål.

Finanstilsynet pekte i foreløpig rapport på at pensjonskassen ikke synes å ha etablert et overordnet rammeverk for arbeid med datakvalitet, men at dette inngår i det generelle arbeidet med IKT.

Av styrets svar framgår det at pensjonskassen har utarbeidet retningslinje for datakvalitet.

Finanstilsynet tar styrets svar til orientering.

***

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet. Kopi av tilsynsrapporten bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Jarleif Lødøen
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.