FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

KLP Kapitalforvaltning AS
Postboks 400 Sentrum
0103 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
22/5155			08.05.2023

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i KLP Kapitalforvaltning (Foretaket) 5. september 2022. Tilsynet hadde som formål å gjøre en vurdering av hvordan Foretaket ivaretar styring og kontroll innen områdene IKT-sikkerhet og utkontraktering av IKT-tjenester.

Til grunn for merknadene ligger Finanstilsynets foreløpige rapport datert 11. januar 2023 og styrets tilsvar av 15. februar 2023.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Forhold knyttet til utkontraktering av IKT tjenester

IKT-forskriften § 12 stiller krav til at avtale om utkontraktering må sikre at foretak under tilsyn gis rett til å kontrollere, herunder revidere de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal videre sikre at Finanstilsynet gis tilgang til opplysninger fra, og tilsyn hos, IKT-leverandøren der Finanstilsynet finner det nødvendig.

I foreløpig rapport påpekte Finanstilsynet at Foretakets avtaler ved utkontraktering av IKT-tjenester ikke var i henhold til IKT-forskriften §12 når det gjelder Foretakets, og Finanstilsynets, tilgang til opplysninger og mulighet til tilsyn.

Styret har i sitt svar til foreløpig rapport tatt Finanstilsynets merknader til etterretning. Videre framgår det at Foretaket har tatt kontakt med de aktuelle leverandørene med sikte på å gjøre endringer i avtaleforholdet samt gir uttrykk for at slike prosesser med store internasjonale selskaper er tidkrevende

Finanstilsynet forventer at avtaler om utkontraktering av IKT-tjenester som ikke oppfyller IKT-forskriften § 12 blir endret innen 30. juni 2023 slik at regelverket etterleves, og ber om å bli informert når reviderte avtaler foreligger.

Forhold knyttet til IKT-sikkerhet

IKT-forskriften § 5 stiller krav om at foretaket skal ha prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk,

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Gisle Haugseth
Dir. tlf 22 93 97 33

uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

I foreløpig rapport påpekte Finanstilsynet at Foretaket har utstedt anonyme brukertilganger til eksterne konsulenter. Finanstilsynets forventing er at Foretaket ikke benytter seg av anonyme brukertilganger og gjennomfører hensiktsmessig overvåking av data som blir aksessert i Foretakets systemer.

I sitt svar til foreløpig rapport tok styret tilsynets merknader til etterretning og opplyste at det er etablert en løsning med multifaktorautentisering for eksterne brukerne, at det er under utarbeidelse en rutine for administrasjon av eksterne brukere og at de aktuelle brukerne nå har definerte tilganger i henhold til behov.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til tredjeparts-testing av informasjonssikkerhet

IKT-forskriften § 2 stiller blant annet krav til fastsettelse av sikkerhetskrav for IKT-virksomheten. Etter § 2 første ledd, andre setning skal det foreligge beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte. Videre framgår det av IKT-forskriften § 5 at foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk.

Finanstilsynet påpekte i foreløpig rapport at Foretaket ikke hadde egne retningslinjer for testing av informasjonssikkerhet på tilsynstidspunktet.

Finanstilsynet forventer at foretak under tilsyn har etablert retningslinjer for gjennomføring av sikkerhetstester. Eventuell bruk av eksterne leverandører til slik testing bør inngå i retningslinjene. Retningslinjene bør også stille krav til hvor ofte tester skal gjennomføres og hvordan tester skal utføres. Finanstilsynet legger videre til grunn at slike retningslinjer baseres på internasjonalt aksepterte standarder.

I sitt svar tok styret Finanstilsynets merknader til etterretning og opplyste at det nå er utarbeidet en rutine for sikkerhetstesting tilpasset selskapets virksomhet.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til klassifisering av informasjon og dokumenthåndtering

For å etablere riktig beskyttelsesnivå, jf. IKT-forskriften § 5, bør foretaket klassifisere sin informasjon, der det tas hensyn til krav om konfidensialitet, integritet og tilgjengelighet.

Finanstilsynet påpekte i foreløpig rapport mangler ved Foretakets rutiner for informasjonsklassifisering og at Foretaket må ferdigstille arbeidet med informasjonsklassifisering for å sikre at kravene om beskyttelse av informasjon blir tilstrekkelig ivaretatt.

Styret opplyste i sitt svar til foreløpig rapport at det tar Finanstilsynets merknader til etterretning og at foretaket har gjennomført tiltak for å sikre korrekt klassifisering av informasjon. Videre framgår det at Foretaket vil iverksette ytterligere tiltak for å sikre riktig behandling og beskyttelse for de ulike klassene av informasjon.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til IKT-revisjon

Foretaket er etter forskrift om risikostyring og internkontroll § 9 pliktig til å ha internrevisjon, som minimum én gang i året skal avgi rapport om risikostyringen og internkontrollen. Dette gjelder også for IKT-området.

Finanstilsynet påpekte i foreløpig rapport at Foretaket har mangler i revisjoner på IKT-området. Foretaket hadde heller ikke retningslinjer og planer for gjennomføring av revisjoner på området.

Styret har i sitt svar til foreløpig rapport opplyst at det tar Finanstilsynets merknader om at det ikke har vært tilstrekkelig med IKT-revisjoner i Internrevisjonens revisjonsplaner til etterretning. Videre opplyses det om at det er gjennomført IKT-revisjoner på konsernets fellesløsninger i regi av konsernet Foretaket er del av, med relevans for Foretaket. Finanstilsynet har fra styrets svar merket seg at Foretakets internrevisjon nå har planlagt flere IKT-revisjoner for 2023.

Finanstilsynet understreker styrets ansvar for å sikre at det blir gjennomført tilstrekkelig IKT-revisjoner i Foretaket.

Kopi av dette brevet bes sendt til Foretakets valgte revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Gisle Haugseth
seniorrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.