



Styret i EIENDOMSMEGLER 1 OSLO AKERSHUS AS
Postboks 385 Sentrum
0102 OSLO

VÅR REFERANSE
23/3460

DERES REFERANSE

DATO
12.02.2024

Tilsynsrapport

Finanstilsynet gjennomførte IKT-tilsyn i Eiendomsmegler 1 Oslo Akershus AS, Avd. Oppgjør (foretaket) 10. mai 2023. Tilsynet hadde som formål å gjøre en vurdering av hvordan foretaket administrerer, drifter, vedlikeholder og sikrer tjenester og IKT-systemer knyttet til oppgjørsfunksjonen. Finanstilsynet ønsket å foreta en samlet vurdering av IKT-risikoen i foretaket og hvilken kontroll foretaket har med denne.

Finanstilsynets foreløpige rapport datert 23. oktober 2023 og foretakets tilsvarende rapport i brev av 29. november 2023 ligger til grunn for tilsynsrapporten.

Finanstilsynet har følgende merknader etter tilsynet:

Forhold knyttet til virksomhetens konsekvensanalyse

Finanstilsynet pekte i foreløpig rapport på at foretaket ikke hadde utarbeidet forretningsmessig konsekvensanalyse (BIA) for virksomheten. Finanstilsynet forventer at foretaket utarbeider konsekvensanalyse, hvor viktige og kritiske prosesser evalueres av forretningsdelen med innspill fra andre områder i foretaket. Resultatet av konsekvensanalysen gir oversikt over foretakets systemportefølje og angir kritikaliteten systemene har for foretakets virksomhet. Videre bør det framgå av analysen hva som er akseptabel nedetid for foretakets ulike virksomhetsprosesser og de enkelte IKT-systemer. Resultatet av analysen bør formidles til relevante leverandører. Det legges til grunn at rutine for området etableres og inngår i foretakets ordinære drift.

Finanstilsynet har fra styrets svar merket seg at foretaket har besluttet å utarbeide en rutine for gjennomføring av konsekvensanalyser i foretaket, samt utføre nødvendige konsekvensanalyser.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til kriseberedskap

Finanstilsynet pekte i foreløpig rapport på at foretakets beredskapsplan i liten grad vektlegger IKT. Planen bærer preg av å være kopi av Alliansens beredskapsplan. Akseptabel nedetid fremgår av utkontrakteringsavtaler, men ikke av beredskapsplanen, ei heller av kontaktpunkter mot leverandører.

Under tilsynsmøtet fremkom det videre at foretaket ikke har gjennomført beredskapstester på IKT-området. Finanstilsynet forventer at foretak under tilsyn gjennomfører regelmessig testing av sine

beredskapsløsninger i samsvar med regelverket, for å vurdere egnetheten til kriseløsningen og robustheten til organisasjonen. Resultatet skal dokumenteres slik at det er mulig å kontrollere.

Finanstilsynet har fra styrets svar merket seg at "*beredskapsplanen må videreutvikles*". Styret bekrefter at deler av beredskapsplanen er hentet fra Sparebank 1 Gruppen og at styret vurderer denne som langt på vei dekkende med de tilpasninger som er gjort. Styret erkjenner at opplæring av de ansatte og øvelse i krisehåndtering ikke har vært tilstrekkelig. Det bekreftes videre at foretaket vil oppdatere rutiner og planverk, lage opplæringsplan, forestå opplæring og iverksette øvelse.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til retningslinjer for sikkerhetstesting

I foreløpig rapport stilte Finanstilsynet spørsmål ved om foretaket var forberedt på å håndtere en alvorlig sikkerhetshendelse og om foretaket hadde tilstrekkelige rutiner og planer for periodisk sikkerhetstesting, og for hvordan foretaket vil sikre at kritisk infrastruktur blir omfattet av testingen.

Styret erkjenner i sitt svar til foreløpig rapport at foretaket selv ikke har foretatt sikkerhetstesting, men opplyser videre at ulike sikkerhetstester er foretatt av Sparebank 1 Utvikling og av foretakets leverandører.

Foretaket har innhentet og oversendt dokumentasjon fra to av sine leverandører som gjennomfører penetrasjonstester på sine systemer. Dette var dokumentasjon som ikke var tilgjengelig på tilsynstidspunktet.

Styret erkjenner videre at det er en svakhet i at foretaket har lent seg på opplysninger fra leverandørene og at resultatet av testene ikke har vært tilgjengelig for foretaket og Finanstilsynet tidligere. Foretaket vil fremover følge opp testene og resultatene i møter med leverandørene. Foretaket bekrefter videre at det er en pågående dialog med leverandør om å foreta en test av kriseløsningen i 2024. Foretaket vil samarbeide med leverandør om planlegging og gjeninnføring av denne.

Finanstilsynet tar styrets svar til etterretning.

Forhold knyttet til tilgangsstyring

Finanstilsynet pekte i foreløpige rapport på mangler ved styring og kontroll med tjenesteleverandørers tilganger i foretakets systemer. Finanstilsynet understreket at det er viktig at tilganger vurderes ut ifra tjenstlig behov og at kontroller av tilgangsrettigheter gjøres regelmessig.

Styret har i sitt tilsvaret gitt redegjørelse for kontroll med tilgangsstyringen.

Finanstilsynet tar styrets svar til etterretning.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Gisle Solemsjø Haugseth
seniorrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.