FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

NOROPPGJØR AS
Styret
Postboks 199 Bogstadveien
0323 OSLO

Vår referanse
25/8483
Deres referanse

01.12.2025

Tilsynsrapport

1 Innledning

Finanstilsynet har gjennomført tilsyn med Noroppgjør AS (heretter omtalt "foretaket"). Formålet med tilsynet var kontroll med foretakets risikovurdering og rutiner etter hvitvaskingsloven og eiendomsmeglingsloven, etterlevelse av dette regelverket i oppdragsgjennomføringen og gjennomføring av internkontroll, samt kontroll med og behandling av klientmidler.

Det ble også gjennomført IT-tilsyn hos foretaket. Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og IKT-tjenester. Tilsynet ble avgrenset til elektronisk forsvar og tilhørende emner innen IKT-sikkerhet, og styring og kontroll med IKT-virksomheten. Videre ønsket Finanstilsynet å gjøre en vurdering av foretakets beredskapsarbeid relevant for IKT-området, herunder vurdere beredskapen i foretaket for utkontrakterte IKT-tjenester, samt overholdelse av regulatoriske krav på IKT-området.

Finanstilsynet gjennomførte møte med foretaket 1. september 2025. Denne tilsynsrapporten bygger på Finanstilsynets foreløpige rapport fra 26. september 2025 og styrets kommentar til denne fra 20. oktober 2025.

2 Finanstilsynets oppsummering

Finanstilsynet avdekket flere avvik under tilsynet med Noroppgjør AS. Finanstilsynet påpeker mangler i foretakets internkontroll, hvor det ikke forelå dokumentasjon på at internkontrollen faktisk overvåkes, samt at foretaket ikke fører oppgjørsjournal. Foretaket må etablere ekstern overvåking av internkontrollen og føre oppgjørsjournal etter kravene i eiendomsmeglingsforskriften.

På hvitvaskingsområdet har foretaket mangler knyttet til den virksomhetsinnrettede risikovurderingen, rutiner for oppfølging av utkontrakterte kundetiltak og enkelte mangler i etterlevelsen av regelverk og rutiner i gjennomføringen av eiendomsmeglingsoppdrag. Foretaket må revidere sin risikovurdering og sikre tilstrekkelig oppfølging av kvaliteten på de utkontrakterte kundetiltakene.

Finanstilsynet mener at foretakets oppfølging av IKT-risiko er mangelfull og ikke i samsvar med regelverket, jf. forskrift om risikostyring og kontroll § 4. Finanstilsynet forventer at styregodkjente styringsdokumenter, som strategier og policyer, implementeres og følges opp for å sikre at foretakets drift og planer utføres i henhold til foretakets overordnede strategi.

Foretaket har ikke i tilstrekkelig grad gjennomført egne kontroller av IKT-virksomheten for å kunne vurdere sin etterlevelse eller risiko. Finanstilsynet vurderer at uten en forretningsmessig konsekvensanalyse vil foretakets kriseplan, jf. IKT-forskriften § 11, være utarbeidet uten forretningsmessige prioriteringer.

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
post@finanstilsynet.no
finanstilsynet.no

Saksbehandler
Marianne Kalleberg
Dir. tlf. 22 93 98 00

Finanstilsynets mener at foretakets etterlevelse av IKT-forskriftens § 11 ikke er tilstrekkelig ivaretatt, da foretakets testing av kriseløsninger er mangelfull. Finanstilsynets vurdering er at det er viktig at foretaket sikrer at krav, blant annet fra sikkerhetspolicyen for den interne organisasjonen, også gjøres gjeldende for leverandører.

Finanstilsynet ber foretaket etablere og dokumentere en egen prosess med rutiner for håndtering av endringer og at prosess med rutiner sikrer at det er foretaket som står som eier og ansvarlig for alle endringer som innføres i foretakets IKT-virksomhet.

3 Finanstilsynets vurderinger

3.1 Internkontroll

Etter eiendomsmeglingsforskriften § 2-8 skal fagansvarlig sørge for at internkontrollen blir gjennomført, dokumentert og overvåket på en forsvarlig måte, og at avvik rapporteres til foretakets styre. Dette innebærer at det skal foreligge skriftlige rutiner for å kontrollere at rutinene er blitt fulgt (kontrollrutiner). Kontrollrutinene skal angi hva som skal kontrolleres og kontrollens intensitet, for eksempel et bestemt antall saker for hver ansvarlig megler innenfor et nærmere angitt tidsrom, og hvordan kontrollen skal gjennomføres. Rutinene kan være dynamiske, for eksempel slik at avvik på ett område eller hos én megler vil medføre forsterket kontroll i en periode. Avvik skal rapporteres til styret. Dokumentasjon av kontrollen og rapporteringen til styret må forefinnes skriftlig, og kan f.eks. være kontrollrapporter hvor det framgår hva som er kontrollert, om det er funnet avvik, samt dokumentasjon på hvordan eventuelle avvik er blitt fulgt opp.

Det framgår av eiendomsmeglingsforskriften § 2-8 at internkontrollen skal overvåkes. Ved å sammenstille dokumentasjonen fra fagansvarligs kontroller med de skriftlige kontrollrutinene vil overvåker kunne kontrollere at fagansvarlig har gjennomført kontrollen. Foretaket har ikke dokumentert at internkontrollen er overvåket.

Foretaket har opplyst at styret har gitt fagansvarlig et klart mandat om å foreta stikkprøvekontroll, og at resultatene av stikkprøvekontrollene dokumenteres og rapporteres til styret hvert kvartal. Foretaket mener at styret dermed overvåker internkontrollen gjennom styrerapporteringen, samt at revisor overvåker i tredjelinje. Foretaket har påpekt at kontrollen gjennomføres i henhold til dagens rutine og prosess, men deler Finanstilsynets vurdering av at overvåkingen kan være bedre dokumentert. Foretaket har gitt tilbakemelding om at det vil sikre god dokumentasjon ved neste kontroll og forelegge dette for styret.

At styret gjennomgår fagansvarligs avviksrapport er noe annet enn å overvåke om fagansvarlig har gjennomført sin kontroll i samsvar med foretakets kontrollrutiner. Finanstilsynet fastholder at foretaket ikke har dokumentert at internkontrollen er overvåket.

3.2 Klientmiddelsikkerhet

Finanstilsynet fant enkelte svakheter ved foretakets rutiner for klientmiddelssikkerhet. Foretaket opplyser at det har innrettet sine rutiner i samsvar med Finanstilsynets påpekninger.

3.3 Renter på klientkonto

Det følger av eiendomsmeglingsforskriften § 3-10 at klientmidler skal plasseres til høyest mulig rente. Rundskriv 7/2014 punkt 4 omhandler hvilke plikter Finanstilsynet mener eiendomsmeglingsforetakene har ved behandling av klientmidler. Vi mener at foretaket jevnlig, og minimum årlig, må forsikre seg om at rentebetingelsene på klientkontoen er markedsmessige. Foretaket må kunne dokumentere at plikten overholdes. Foretaket kan ikke ved avtaler eller på annen måte forplikte seg på en slik måte at regelverket ikke overholdes. Foretaket kan ikke dokumentere å ha foretatt undersøkelser av rentenivået i andre banker, og kan dermed ikke dokumentere at rentebetingelsene på klientkonto er markedsmessige.

Foretaket erkjenner at det ikke er dokumentert at det har innhentet tilbud på rentenivået i andre banker, og har opplyst at det vil endre rutinen slik at det i framtiden oppfyller forskriftens krav og dokumenterer sin vurdering på en tilstrekkelig måte.

3.4 Journalføring

Etter eiendomsmeglingsforskriften § 3-4 skal foretaket føre oppgjørsjournal. Det er krav om betryggende innretning av journalføringen, jf. eiendomsmeglingsforskriften § 3-1. Det som er ført i journalene må ikke ved overstrykninger eller på annen måte gjøres uleselig. Dersom rettelser foretas i elektronisk journal, skal tidligere registrerte opplysninger være sporbare, og det skal kunne tas ut en oversikt som viser alle endringer som er foretatt.

Foretaket førte ikke oppgjørsjournal. Foretaket har ikke en samlet journal, men kun oversikt over oppdragene i saksbehandlingssystemene de bruker, som kan eksporteres til regneark (Excel) ved behov. Dette oppfyller ikke kravet til sporbarhet, idet foretaket fritt kan endre eller slette registreringer uten at dette framkommer av journalen. Videre oppfyller ikke føringene i regneark kravet om at det må kunne tas ut en samlet oversikt over endringer i elektroniske journaler. Journalen er heller ikke ført i tidsrekkefølge, da oppgjør gjennomført i ulike saksbehandlingssystem ikke journalføres samlet.

Foretaket erkjenner at dagens praksis for føring av oppgjørsjournal ikke fullt ut oppfyller kravene som er stilt i eiendomsmeglingsforskriften § 3-4. Videre har foretaket svart at det tar Finanstilsynets bemerkninger til etterretning, og at det vil undersøke mulighetene for en bedre digital journalføring, i dialog med relevante systemleverandører, for å kunne etablere en betryggende og forskriftsmessig løsning.

Reglene om journalføring er begrunnet med hensynet til notoritet og Finanstilsynets kontrollfunksjon. Finanstilsynet anser det kritikkverdig at foretaket ikke har oppfylt regelverket om journalføring. Finanstilsynet ber foretaket snarest, og senest innen 1. mai 2026, bekrefte at foretakets journalføring er brakt i samsvar med regelverket.

3.5 Garanti etter avhendingsloven § 2-11

Det følger av avhendingsloven § 2-11 at ved salg av bolig eller fritidsbolig innen seks måneder etter ferdigstillelse, skal det stilles garanti etter boligoppføringsloven § 12. Entreprenøren skal stille garantien straks etter avtaleinngåelsen, eller straks etter frafall av forbehold gitt i medhold av boligoppføringsloven § 12 andre ledd. For å ivareta sin omsorgsplikt overfor kjøper, må megler følge opp at selger oppfyller denne kontraktsforpliktelsen. Dersom dette ikke fører frem, plikter megler å informere kjøper om selgers manglende oppfyllelse, samt hvilke konsekvenser dette kan få for kjøper, herunder at ingen del av kjøpesummen forfaller til betaling før garanti er stilt. Megler kan dermed ikke kreve innbetaling av noen deler av kjøpesummen før garanti er stilt. Omsorgsplikten gjelder også ved oppdrag som er begrenset til kontrakt og oppgjør.

Finanstilsynet avdekket to oppdrag hvor garanti var stilt for sent, uten at foretaket kunne dokumentere at det hadde orientert kjøperne om selgers mislighold og om betydningen av dette. Foretaket tar til etterretning at garantiene i disse tilfellene ble stilt for sent, og erkjenner at foretaket ikke har dokumentert at det har informert kjøperne om dette eller om konsekvensene av forsinkelsen. Foretaket opplyser at det vil utbedre sine rutiner på dette området.

Finanstilsynet mener foretaket i disse oppdragene ikke har ivaretatt rådgivningsplikten overfor kjøperne, jf. eiendomsmeglingsloven § 6-3 andre ledd.

3.6 Hvitvasking

3.6.1 Risikovurdering

Etter hvitvaskingsloven § 7 skal eiendomsmeglingsforetak og advokatmeglere identifisere og vurdere risikoen for hvitvasking og terrorfinansiering knyttet til sin virksomhet.

En forsvarlig risikovurdering forutsetter at foretaket har konsultert relevante kilder. Sentrale kilder i risikovurderingen vil for det første omfatte foretakets egne erfaringer fra virksomheten, for eksempel relatert til omfanget av det enkelte produkt/tjeneste, eksponering mot utenlandstransaksjoner, omfang av avdekkede indikatorer på mistanke, samt svakheter i etterlevelsen av regelverk og rutiner avdekket gjennom interne kontroller. Når det gjelder eksterne kilder, må virksomheten minimum benytte gjeldende Nasjonal risikovurdering av hvitvasking og terrorfinansiering, samt Finanstilsynets risikovurdering. Det forventes videre at virksomheten også benytter andre relevante trussel- og risikovurderinger, eksempelvis rapporter fra Økokrim, Kripos, PST og NTAES. Større foretak bør også konsultere internasjonale kilder, som for eksempel EU-kommisjonens overnasjonale risikovurdering, samt relevante FATF-rapporter. Det bør framgå av risikovurderingen hvilke eksterne kilder som er benyttet. Det framkommer ikke av foretakets risikovurdering at noen av de ovennevnte kildene er benyttet.

Det er en forutsetning for en robust risikovurdering at foretaket eksplisitt tar stilling til kvaliteten av de tiltak som skal iverksettes for å håndtere den identifiserte risikoen. Foretaket må vurdere om rutinen fullt ut er tilstrekkelig for å møte risikoen, eller om det er behov for endringer – før gjenværende risiko angis. Foretaket har etter det Finanstilsynet kan se, ikke vurdert effektiviteten av iverksatte tiltak.

Finanstilsynet legger til grunn at foretakets risikovurdering bygger på beskrivelser av detaljer og underliggende risikodrivere i risikomatrisen. Dette innebærer at feil og svakheter ved risikomatrisen kan være av vesentlig betydning for foretakets forståelse av egen risiko i risikovurderingen.

Foretakets risikomatrise er delt opp i ulike risikodrivere, hvor risikoscoren er angitt basert på sannsynlighet og konsekvens vurdert på en skala fra 1-6. Den totale risikoen er sannsynlighet ganger konsekvens. Det er også angitt en restrisiko som skal reflektere risiko etter at tiltak er gjennomført. Foretaket har identifisert de fleste sentrale risikoer, men Finanstilsynet stiller spørsmål ved måten disse risikoene er vurdert på.

For det første er det ikke oppgitt noen skala som angir hva risikoscorene betyr. Det er ikke mulig å lese ut av risikomatrisen hva som anses som lav, moderat eller høy risiko. Dette blir særlig problematisk når foretakets rutiner for vurdering av risiko i oppdragsgjennomføringen viser til risikomatrisen for veiledning.

For det andre er for eksempel kundetyper med en svært ulik risikoprofil vurdert som en helhet. Et punkt i risikomatrisen er kalt "Organisasjonsform", og dette punktet inkluderer blant annet aksjeselskap, norsk utenlandsk filial, kommunale organer og offentlige organer i samme vurdering, hvor alle er gitt samme score for sannsynlighet og konsekvens. Slik Finanstilsynet tolker dette, mener altså foretaket at disse ulike kundetypene har lik risiko for hvitvasking, selv om risikodriverne for disse kundetypene kan være svært ulike.

Det samme gjelder punktet "Eierskaps- og kontrollstruktur", hvor foretak registrert på norsk børs og foretak som har unormalt avansert eller kompleks eierstruktur er vurdert som en helhet. Dette til tross for at foretak registrert på norsk børs er et moment som tilsier lavere risiko, jf. hvitvaskingsforskriften § 4-6, mens unormalt kompleks eierstruktur er et moment som tilsier høyere risiko etter § 4-9. Foretaket drøfter riktignok de ulike risikodriverne til en viss grad i beskrivelsesfeltet i risikomatrisen, men risikoscoren som angis er likevel felles for begge disse momentene.

Etter Finanstilsynets vurdering er risikovurderingene så generelt utformet at den endelige risikoscoren som angis kan framstå noe vilkårlig. Poenget med å angi en risikoscore er at den må være treffende for den eller de momentene som vurderes. Når momenter med helt ulikt risikobilde inngår i samme vurderingsfelt framstår risikoscoren som tilfeldig, og det er uklart hva som egentlig ligger til grunn for vurderingen av sannsynlighet og konsekvens. Dermed framstår risikomatrisen uegnet som hjelpemiddel til å vurdere risikoen i det enkelte oppdraget. Finanstilsynet forutsetter at foretaket gjennomfører en helhetlig revidering av risikomatrisen.

Foretaket svarer at det tar Finanstilsynets vurdering til etterretning, og at det vil utbedre sin risikovurdering.

3.6.2 Rutiner for utkontraktering

Avtale om utkontraktering av oppgaver etter hvitvaskingsregelverket skal være skriftlig, jf. hvitvaskingsloven § 23. Der virksomheten i medhold av skriftlig avtale har utkontraktert oppgaver i medhold av § 23, eller legger til grunn kundetiltak utført av tredjeparter i medhold av § 22, må virksomhetens rutiner omfatte tiltak for oppfølging av slike kundetiltak eller tredjeparter.

Foretakets arbeidsrutiner omfatter kontroll av de utkontrakterte kundetiltakene i det enkelte oppdrag, men inneholder ikke rutiner for en periodisk og mer systematisk kontroll med kvaliteten på de utkontrakterte kundetiltakene. I stikkprøvekontrollen ble det avdekket enkelte tilfeller av at sentrale utkontrakterte kundetiltak ikke var gjennomført, eller ikke korrekt gjennomført se pkt. 3.6.4. Dersom avtalemotparten ikke gjennomfører riktige kundetiltak eller kundetiltak med tilstrekkelig god kvalitet, må foretaket ha rutiner for å følge opp dette med avtalemotparten. Utkontrakterte kundetiltak bør inngå i internkontrollen og foretaket bør gi tilbakemelding om gjentakende eller alvorlige avvik til avtalemotparten slik at nødvendige tiltak kan gjennomføres. Denne tilbakemeldingen bør gis til avtalemotpartens ledelse eller hvitvaskingsansvarlig og ikke kun skje i forbindelse med enkeltoppdrag.

Foretaket svarer at det foretar en samlet og overordnet vurdering av kvaliteten på kundetiltakene over tid, og at gjentakende eller alvorlige avvik følges opp med avtalemotparten, blant annet i kundemøter der fagansvarlig/hvitvaskingsansvarlig alltid involveres. Foretaket er enig i at den overordnede oppfølgingen av utkontrakterte kundetiltak ikke er godt nok beskrevet i de skriftlige rutinene, og vil sikre at periodisk og systematisk oppfølging av utkontrakterte kundetiltak framgår klart av rutiner og inngår i foretakets internkontroll.

3.6.3 Internkontroll

Hyppigheten og omfanget av internkontrollen må være forsvarlig og bero på en vurdering av blant annet virksomhetens art og omfang, og ansattes kompetanse på hvitvaskingsområdet Finanstilsynet mener at oppdrag hvor risikoen er vurdert å være høy, alltid bør inngå i internkontrollen, se rundskriv 11/2019, Veiledning til etterlevelse av hvitvaskingsregelverket i eiendomsmeglingsvirksomhet, punkt 11. Foretakets internkontrollrutiner inneholder ikke bestemmelser om at alle oppdrag med høy risiko skal inngå i internkontrollen, eller kontroll av at rutine for forsterkede kundetiltak er fulgt i oppdrag med høy risiko.

Foretaket svarer at det har etablert en indikatorliste hvor alle oppdrag med høy risiko legges inn, og at samtlige saker på listen blir gjennomgått av hvitvaskingsansvarlig. Foretaket mener praksisen er i tråd med Finanstilsynets krav om at oppdrag med høy risiko skal inngå i internkontrollen, og at den fungerer som en ekstra kvalitetskontroll på alle saker med indikator på høy risiko, selv om praksisen ikke nødvendigvis utgjør en full internkontroll i form av tilfeldige stikkprøvekontroller.

Finanstilsynet mener fremdeles at rutinen ikke inneholder bestemmelser om at alle oppdrag med høy risiko skal inngå i internkontrollen, eller bestemmelser om kontroll av at rutine for forsterkede kundetiltak er fulgt i oppdrag med høy risiko. Foretakets rutine for internkontroll inneholder bestemmelser om at i saker der det er identifisert høy risiko, er det to mulige utfall: I saker der

foretaket vurderer at risikoen «anses avklart», skal hvitvaskingsansvarlig ved tvil foreta kontroll med vurdering av om det er foretatt tilstrekkelige forsterkede tiltak, og om ansvarlig meglers vurdering er grundig og godt begrunnet. Slik Finanstilsynet forstår det, er det oppgjørsansvarlig/ ansvarlig megler som vurderer om risikoen anses avklart, og om det foreligger tvil om det er foretatt tilstrekkelige forsterkede kundetiltak. Finanstilsynet legger til grunn at dette innebærer at ikke alle saker der risiko anses avklart blir gjennomgått av hvitvaskingsansvarlig i foretakets internkontroll, selv om det også i disse sakene er identifisert høy risiko for hvitvasking. I saker der risikoen ikke anses avklart skal hvitvaskingsansvarlig ifølge foretakets rutine følge opp saken med nærmere undersøkelser.

Det er uklart hva foretaket mener med «anses avklart», men det kan synes som om oppdrag har blitt nedjustert fra høy risiko til normal risiko hvis enkelte forsterkede kundetiltak ikke førte til funn av noe mistenkelig. I så fall bygger dette på en feilaktig forståelse av hva risikoklassifiseringen skal gi uttrykk for. Det at det ikke avdekkes noe mistenkelig betyr ikke nødvendigvis at risikoen reduseres. I vår stikkprøvekontroll ble det for øvrig avdekket ett tilfelle av slik nedjustering, se nedenfor.

3.6.4 Oppsummert om funn i stikkprøvekontroll

Etter hvitvaskingsloven § 12 første ledd, jf. § 15 tredje ledd, skal virksomheten – der kunde eller medkontrahent er en fysisk person – innhente opplysninger om navn, fødselsnummer (eller D-nummer eller annen entydig identitetskode) og adresse. De samme opplysningene skal innhentes om den som handler på vegne av kunden, og at vedkommende kan handle på vegne av kunden. De samme opplysninger skal innhentes om den som er gitt disposisjonsrett over kontoer som benyttes til inn- og utbetaling av kjøpesum. I ett oppdrag var spørsmålet om det fantes disponenter på kontoen til kjøper formulert på en måte som ikke gjorde at det kom tydelig nok fram at også ansatte, eiere eller andre med en tilsvarende tilknytning til kjøperen må identifiseres dersom de har disposisjonsrett.

Etter hvitvaskingsloven § 12 andre ledd skal opplysninger om kundens, medkontrahenten og fullmektigens identitet bekreftes ved personlig frammøte ved gyldig legitimasjon. I ett oppdrag ble bekreftelse av kundens identitet med gyldig legitimasjon utført etter oppdragsinngåelsen. Kundetiltaket ble utført for sent, jf. § 11 første ledd.

Etter hvitvaskingsloven § 13 første ledd skal foretaket gjennomføre egnede tiltak for å forstå eierskaps- og kontrollstrukturen i kunden. I ett oppdrag var denne kontrollen ikke tilstrekkelig dokumentert til at det var mulig å forstå eierskapsstrukturen.

Virksomheten skal kunne påvise at omfanget av utførte tiltak er tilpasset den aktuelle risiko, det vil si at risikoen er konkret vurdert og tilstrekkelig tatt hensyn til ved omfanget og intensiteten av kundetiltakene, jf. § 9. Dette innebærer at megler rutinemessig i alle oppdrag må foreta en klassifisering av risiko knyttet til både oppdragsgiver, oppdragsgivers medkontrahent og transaksjon. I ett oppdrag ble selger først identifisert som høy risiko, men senere nedjustert til moderat. Dette ble begrunnet med at det ikke forelå mistanke. Som nevnt i punkt 3.6.3 over, bygger dette på en feilaktig forståelse av hva risikoklassifiseringen skal gi uttrykk for. I ett oppdrag ble transaksjonen vurdert som normal risiko selv om det var avtalt selgerkreditt. I ett oppdrag ble kjøper vurdert til normal risiko, selv om kjøper hadde tilknytting til en høyrisikobransje, uten at foretaket har begrunnet dette. I samme oppdrag ble også risikoen ved transaksjonen vurdert som lav, selv om eiendommen ble solgt til langt under markedspris.

Foretaket må ha rutiner for å innhente og kontrollere nødvendig informasjon for å avdekke indikasjoner på mistenkelige transaksjoner. Ifølge indikatorlisten fra NTAES er selgerkreditt, eller at selger aksepterer tap, mistenkelig. Ved mistenkelige forhold skal det iverksettes nærmere undersøkelser jf. § hvitvaskingsloven § 25. I ett oppdrag unnlot foretaket å gjennomføre nærmere undersøkelser selv om det ble gitt selgerkreditt. I et annet oppdrag ble det ikke gjennomført tilstrekkelige nærmere undersøkelser til å avkrefte mistanken, selv om foretaket var kjent med at

selger aksepterte et betydelig tap. Der mistanken ikke lar seg avkrefte skal transaksjonen rapporteres til Økokrim.

Etter § 30 skal foretaket oppbevare opplysninger og dokumenter som er innhentet i forbindelse med kundetiltakene. I flere oppdrag er opplysninger som er innhentet i forbindelse med kundetiltak kun registrert som kommentarer i meglersystemet, uten at dokumentene som disse opplysningene er hentet fra er lagret. Dette gjelder for eksempel dokumentasjon på at kontroll- og eierstruktur er kontrollert for juridiske personer, og opplysninger om kundeforholdets formål og tilsiktede art.

Det er Finanstilsynets vurdering at det er enkelte mangler ved etterlevelsen av regelverk og rutiner ved gjennomføring av det enkelte oppdrag.

Foretaket har i sitt svar vist til at som oppgjørsforetak har det i mange tilfelle ikke hatt mulighet til å gjennomføre nødvendige kundetiltak før oppdraget formelt er overført fra salgsmegler. Foretaket erkjenner at dette ikke fritar det for ansvar for overholdelse av bestemmelsene i hvitvaskingsloven. I tilfeller der foretaket oppdager at det ikke foreligger tilstrekkelig dokumentasjon fra salgsmegler, gjennomfører foretaket kundetiltak før andre deler av oppdraget utføres. Foretaket har videre opplyst at det som følge av avsløringsforbudet i enkelte tilfeller bevisst har unnlatt å lagre dokumentasjon i meglers system.

Etter Finanstilsynets oppfatning er ikke eiendomsmeglingsforetak å anse som "tredjeperson" etter ordlyden i hvitvaskingsloven § 28 når det utfører kundetiltak for et annet rapporteringspliktig foretak i henhold til en utkontrakteringsavtale regulert av hvitvaskingsloven § 23. Eiendomsmeglingsforetak kan derfor utveksle informasjon om at det foreligger mistanke om hvitvasking til oppdragsgiveren i utkontrakteringsavtalen. Adgangen til utveksling av informasjon er imidlertid begrenset til mistanke som bygger på kundetiltak eiendomsmeglingsforetaket har utført på vegne av oppdragsgiveren i henhold til utkontrakteringsavtalen. Det er ikke til hinder for informasjonsutveksling at kundetiltakene er gjennomført som et ledd i eiendomsmeglingsforetakets egen etterlevelse av hvitvaskingsregelverket, så lenge de også er gjennomført som en del av utkontrakteringsavtalen.

Foretaket må lagre dokumentasjon og informasjon innhentet i forbindelse med nærmere undersøkelser i samsvar med § 30, på en måte som sikrer at ansatte hos den rapporteringspliktige som ikke har tjenstlig behov for informasjonen, ikke får tilgang til informasjonen, jf. rundskriv 4/2022, Veileder til hvitvaskingsloven, punkt 6.3.3. Foretakets praksis, der det i enkelte tilfeller har unnlatt å lagre dokumentasjon i meglers system, er i strid med bestemmelsen i hvitvaskingsloven § 30 første ledd.

Foretaket har opplyst at det har iverksatt tiltak for å skjerpe interne rutiner, styrke dokumentasjonspraksisen og fortsette å sikre at ingen oppdrag påbegynnes uten at nødvendige kundetiltak er gjennomført og dokumentert. Foretaket har også opplyst at det vil utarbeide bedre rutiner for utkontraktering, og involvere fagansvarlig/hvitvaskingsansvarlig hos avtalemotpart, slik at manglende tiltak etter hvitvaskingsloven kan avdekkes tidligere i prosessen.

3.6.5 Screening mot sanksjonslister

Foretaket plikter å ivareta de finansielle restriksjonene i det norske regelverket, som igjen bygger på sanksjoner fra FNs sikkerhetsråd og restriktive tiltak fra EU. Sanksjonslistene fremkommer gjennom forskrifter til lov om gjennomføring av internasjonale sanksjoner. Det vises til Veiledning om frysbestemmelsene.

For å kunne fryse midler og eiendeler tilhørende listeførte personer, må screening mot sanksjonslistene gjennomføres overfor foretakets kunde og medkontrahent, inkludert reelle rettighetshavere og disponenter på konto som benyttes i kundeforholdet, avsender og mottaker i transaksjoner, samt når det gjøres endring i oversikten over listeførte personer.

Under tilsynet opplyste foretaket at det var usikker på om disponenter på konto ble screenet. Det opplyste også at mottaker og avsender i transaksjonen ikke ble screenet der dette var andre personer enn kjøper og selger. I sitt svar til foreløpig rapport har foretaket opplyst at det har iverksatt nødvendige tiltak og oppdatert sine rutiner for å sikre at rutinene framover oppfyller kravene til screening mot sanksjonslister og frysbestemmelser.

3.7 IT-tilsyn

3.7.1 Organisering

Styret skal fastsette prinsipper for risikostyring for foretaket som en helhet og innenfor hvert enkelt virksomhetsområde, jf. forskrift om risikostyring og internkontroll § 3. Videre framgår det av § 4 at daglig leder skal påse en forsvarlig risikostyring og internkontroll på basis av en vurdering av aktuelle risikoer, i henhold til retningslinjer fastsatt av styret.

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretaket, for å sikre god styring og kontroll over egen IKT-virksomhet – inkludert utkontrakterte tjenester – bør gjennomføre egne kontroller både knyttet til risiko og etterlevelse. Det ble videre understreket at foretaket må etablere rutiner for egne kontroller av IKT-risiko og etterlevelse hos leverandører og underleverandører.

Finanstilsynet vurderer det som viktig at foretaket har tilstrekkelig IKT-kompetanse og ressurser i forsvarslinjene for å kunne etablere og følge opp et robust kontrollrammeverk.

Finanstilsynet kan ikke se at styret i sitt tilsvar har kommentert direkte på de punktene som ble påpekt i foreløpig tilsynsrapport herunder manglende egne kontroller av IKT-risiko, svak uavhengighet i informasjonssikkerhetsfunksjonen og utilstrekkelig kompetanse i forsvarslinjene.

Finanstilsynet forventer at oppfølgingen av IKT-risiko er i tråd med bestemmelser i risikostyring og internkontroll § 4, ettersom foretaket i hovedsak baserer seg på leverandørrapportering uten egne faste kontroller. [redacted] Foretaket må sikre at andrelinjen har nødvendig kompetanse og kapasitet til å kontrollere at sikkerhetspolicyen er operasjonalisert, også hos leverandører og underleverandører.

3.7.2 Overordnet risikostyring

Foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten, jf. IKT-forskriften § 2 første ledd. Videre skal foretaket fastsette grenser for akseptabel risiko knyttet til bruk av IKT-systemene, jf. § 3 første ledd, og ha en dokumentert prosess for gjennomføring av risikoanalyser minst én gang årlig eller ved endringer som har betydning for IKT-sikkerheten, jf. § 3 annet ledd. Risikoanalysene skal sikre at IKT-risikoen styres innenfor akseptable grenser i forhold til foretakets virksomhet, og resultatene skal dokumenteres. I tillegg stiller forskrift om risikostyring og internkontroll § 6 første ledd krav om at foretaket løpende vurderer hvilke vesentlige risikoer som er knyttet til virksomheten.

Finanstilsynet bemerket i foreløpig tilsynsrapport at foretakets IKT-strategi er styregodkjent, men ikke i samsvar med hvordan IKT-virksomheten faktisk er organisert og utvikles. Det gjennomføres ingen kontroller eller oppfølging av om styrende dokumenter, herunder strategier og policyer, etterleves.

Finanstilsynet kan ikke se at styret i sitt tilsvar har kommentert direkte på de punktene som ble påpekt i foreløpig tilsynsrapport, herunder kravene i IKT-forskriften §§ 2–3 om fastsettelse av mål, strategier, sikkerhetskrav og akseptabel risiko, samt dokumenterte risikoanalyser minst årlig. Videre gjelder forskrift om risikostyring og internkontroll § 6 om løpende vurdering av vesentlige risikoer.

Finanstilsynet forventer at styregodkjente dokumenter implementeres og følges opp for å sikre samsvar mellom drift og strategi. Det vurderes som hensiktsmessig at andrelinjen har kontrolloppgaven med å følge opp strategier og policyer, mens førstelinjen har ansvar for implementering.

3.7.3 Risikovurderinger for IKT-området

Foretaket skal fastsette kriterier for akseptabel risiko, jf. IKT-forskriften § 3 første ledd. Videre skal foretaket ha en dokumentert prosess for gjennomføring av risikoanalyser for IKT-virksomheten, jf. § 3 annet ledd. Prosessen skal definere klare ansvarsforhold og omfatte oppfølging av tiltak som skal iverksettes basert på resultatene fra analysene. Risikoanalyser skal gjennomføres minst én gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, jf. § 3 tredje ledd. Analysene skal sikre at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet, og resultatene skal dokumenteres.

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretakets årlige IKT-risikoanalyse deler risiko mellom leverandørrisiko, lokal risiko og organisering av IKT-virksomheten. Finanstilsynet har merket seg at risikoene knyttet til leverandørene i hovedsak beskriver bortfall av tjenester og i liten grad omhandler risiko for feil i systemer eller tap av data.

Finanstilsynet kan ikke se at styret har kommentert direkte på de punktene som ble påpekt i foreløpig tilsynsrapport. Dette gjelder særlig anbefalingen om å adressere risiko for brudd på integritet, konfidensialitet og sikkerhetshendelser i IKT-risikoanalysen, slik at vurderingen kan gjøres opp mot foretakets fastsatte akseptable risikonivå. Styrets tilsvar omtaler ikke disse forholdene.

Finanstilsynet anbefaler at foretaket tydelig adresserer risiko for brudd på integritet (feil i systemer), konfidensialitet (tap av data) og sikkerhetshendelser i IKT-risikoanalysen, slik at vurderingen kan gjøres opp mot foretakets fastsatte akseptable risikonivå.

3.7.4 Rapportering av IKT-risiko

Foretakets styre skal, jf. forskrift om risikostyring og internkontroll § 8, føre tilsyn med den daglige ledelsen og foretakets virksomhet basert på vurderingene etter § 6 annet ledd og § 7 annet ledd. Styret skal sørge for at daglig leder regelmessig gir styret informasjon om foretakets virksomhet. Foretakets overordnede målsetting er å være landets ledende tilbyder av oppgjørstjenester, med fokus på service, kompetanse og effektivitet, slik det fremgår av foretakets IKT-strategi, oppdatert 24. april 2025 og godkjent av styret. Under tilsynet stilte Finanstilsynet spørsmål om hvilke kontrollaktiviteter foretakets første og andre linje gjennomfører på IKT-området.

Finanstilsynet påpekte i den foreløpige tilsynsrapporten at foretaket, som har utkontraktert det meste av IKT-virksomheten, må gjennomføre egne kontroller av leverandørens tjenester for å sikre etterlevelse av IKT-strategien.

Finanstilsynet kan ikke se at styret har kommentert direkte på de punktene som ble påpekt i den foreløpige tilsynsrapporten.

Finanstilsynet forventer at det etableres kontroller som omfatter styrende dokumenter, tilgangsstyring, endringshåndtering, utvikling og prosjektstyring, beredskap, kompetanse og ressursstyring. Dette gjelder særlig vurderingen om behovet for egne kontroller av leverandørens IKT-tjenester for å sikre etterlevelse av foretakets IKT-strategi.

3.7.5 Forretningsmessig konsekvensanalyse

Foretaket skal ha oppdatert dokumentasjon for hvert IKT-system som er av betydning for virksomheten, jf. IKT-forskriften § 13. Det skal etableres hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet basert på konsekvensanalyser av foretakets kritiske

forretningsprosesser. Forretningsmessig konsekvensanalyse skal sikre at beredskapsplanene utarbeides med utgangspunkt i forretningsmessig kritikalitet og foretakets prioriteringer for gjenoppretting av forretningskritiske tjenester og prosesser. Prioriteringene skal bygge på analysens resultater, inkludert akseptabel nedetid for hvert IKT-system. Beredskapsplanene, som viser foretakets prioriteringer for gjenoppretting, bør formidles til relevante leverandører. For å verifisere at det er etablert fungerende planer og løsninger, skal det gjennomføres regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretaket ikke har gjennomført en forretningsmessig konsekvensanalyse, men kun utarbeidet en systemoversikt fra IKT-avdelingen uten involvering av forretningssiden. Oversikten angir ikke systemenes kritikalitet for virksomheten.

Finanstilsynet kan ikke se at styret har kommentert direkte på de punktene som ble påpekt i foreløpig rapport, noe som indikerer manglende oppfølging av styrets ansvar for å sikre at kriseplaner bygger på forretningsmessige prioriteringer og at kravene i IKT-forskriften § 11 etterleves.

Finanstilsynet forventer at foretaket utarbeider konsekvensanalyser ledet av forretningssiden, som tydelig angir systemkritikalitet, akseptabel nedetid og formidles til leverandører. Det skal etableres en rutine for dette som en del av ordinær drift.

3.7.6 Krise og beredskap

Foretaket skal ha en dokumentert kriseplan som kan iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Planen skal beskrive nødvendige prosedyrer for håndtering av krisesituasjoner, inkludert ansvar, kommunikasjon og gjenoppretting av kritiske systemer. Det skal minst én gang årlig gjennomføres opplæring, øvelse og testing av kriseløsningen, med dokumentasjon av testresultater som viser at løsningen fungerer som forutsatt, jf. IKT-forskriften § 11.

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretaket er ansvarlig for årlig opplæring, øvelse og testing av kriseløsningen, og at testene må gjennomføres på foretaksnivå for å vurdere egnethet og robusthet. Beredskapsplaner skal oppdateres når forretningsmessig konsekvensanalyse foreligger, og testresultater skal dokumenteres.

Finanstilsynet kan ikke se at styret har kommentert direkte på de punktene som ble påpekt i foreløpig tilsynsrapport, noe som indikerer manglende oppfølging av styrets ansvar for å sikre at beredskapsplaner og tester oppfyller kravene i IKT-forskriften § 11.

Finanstilsynet legger til grunn at foretaket etablerer rutiner som sikrer at beredskapstester som gjennomføres, både internt og hos leverandører, skal gjennomføres basert på foretakets sikkerhetspolicy og virksomhetens konsekvensanalyse.

3.7.7 Utkontraktering

Foretaket skal ha retningslinjer som sikrer at utkontraktert IKT-virksomhet oppfyller kravene i IKT-forskriften § 12, jf. § 2. Dette innebærer at det foreligger skriftlige avtaler som gir foretaket rett til å kontrollere og revidere leverandørens aktiviteter, samt at Finanstilsynet har tilgang til nødvendige opplysninger og mulighet til å føre tilsyn hos IKT-leverandøren. Videre skal avtaler om utkontraktering av IKT-virksomhet og endringer i slike avtaler behandles av styret. Styret skal presenteres en plan for utkontrakteringen, en risikovurdering av utkontrakteringsforholdet og en beskrivelse av hvordan foretaket skal sikre leveransene.

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretaket ikke kunne framlegge avtale med en av hovedleverandørene under tilsynsmøtet; avtalen ble ettersendt, men er ikke i samsvar med IKT-forskriften § 12 om innsynsrett for foretaket eller tilsynsmyndigheten. Avtalen inneholder heller ikke krav til leverandøren om å oppfylle alle krav som stilles i IKT-forskriften, jf. bestemmelsen i § 12.

Finanstilsynet kan ikke se at styret har kommentert direkte på de punktene som ble påpekt i foreløpig tilsynsrapport, noe som indikerer manglende oppfølging av styrets ansvar for å sikre at avtaler med leverandører oppfyller kravene i IKT-forskriften § 12 og foretakets egne sikkerhetspolicy.

Finanstilsynet forventer at foretaket gjennomgår alle avtaler om kjøp av IKT-tjenester for å sikre at de oppfyller gjeldende regelverk, jf. IKT-forskriften § 12. Foretaket har ansvar for risikostyring og internkontroll også ved utkontraktering, og må ha tilstrekkelig kompetanse til å forvalte avtalene. Store deler av IKT-virksomheten er utkontraktert, men krav fra foretakets sikkerhetspolicy brukes ikke som grunnlag for leverandørkrav. Foretaket må sikre at interne krav også gjelder leverandører og underleverandører, og at avtalene inneholder bestemmelser om innsynsrett for nødvendig oppfølging.

3.7.8 IKT-sikkerhet

Foretaket skal ha prosedyrer som sikrer beskyttelse av utstyr, systemer og informasjon av betydning for virksomheten mot skader, misbruk, uautorisert adgang, endring og hærverk, jf. IKT-forskriften § 5. Foretaket har ansvar for risikostyring og internkontroll også der hele eller deler av virksomheten er utkontraktert, jf. § 12, og må sikre at leverandørens aktiviteter kontrolleres.

Videre skal det foreligge retningslinjer for tildeling, endring, sletting og kontroll av autorisasjon for tilgang til IKT-systemene. I tillegg stiller IKT-forskriften § 13 krav om at foretaket har en oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Finanstilsynets vurdering er at dette omfatter oppdaterte oversikter over IT-systemer, nettverksenheter, databaser etc. og at utstyrsoversikten bør inneholde tilstrekkelige konfigurasjonsdata og angi avhengigheter mellom utstyr/komponenter.

Finanstilsynet påpekte i foreløpig tilsynsrapport at foretakets sikkerhetspolicy også skal gjelde utkontraktert IKT-virksomhet, og at det må stilles krav til utstyrsoversikter (CMDB) med dokumentasjon av sammenhenger og eierskap. Foretaket mangler en fullstendig utstyrsoversikt og må sikre at leverandører innfrir sikkerhetskravene, inkludert sårbarhetsstyring, livssyklushåndtering og oppdateringer.

Finanstilsynet kan ikke se at styret har kommentert direkte på de punktene som ble påpekt i foreløpig tilsynsrapport, noe som indikerer manglende oppfølging av styrets ansvar for å sikre at sikkerhetspolicyen etterleves og at tilgangsstyring er forsvarlig i tråd med IKT-forskriften.

Finanstilsynet legger til grunn at foretaket etablerer prosesser og rutiner for å sikre bestemmelsene i IKT-forskriftens § 5 slik at leverandører innfrir sikkerhetskravene, inkludert sårbarhetsstyring, livssyklushåndtering og oppdateringer.

3.7.9 Endringsledelse

Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift jf. IKT-forskriften § 9 fjerde ledd.

Finanstilsynet pekte i foreløpig rapport på at foretaket har rutiner for endringshåndtering, men mangler en dokumentert endringsprosess.

Finanstilsynet kan ikke se at styret har kommentert direkte på de punktene som ble påpekt i foreløpig tilsynsrapport, noe som indikerer manglende oppfølging av styrets ansvar for å sikre kontroll og eierskap til endringsprosesser i tråd med gjeldende regelverk.

Finanstilsynet forventer at foretaket etablerer og dokumenterer en egen endringsprosess med rutiner som sikrer at foretaket står som eier og ansvarlig for alle endringer i IKT-virksomheten.

4 Videre oppfølging

Vi ber foretaket sende kopi av dette brevet til revisor.

For Finanstilsynet

Arne Solberg
seksjonsleder

Marianne Kalleberg
seniorrådgiver

Dokumentet er godkjent elektronisk.