FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Formuesforvaltning Aktiv Forvaltning AS
Styret og daglig leder
Postboks 1777 Vika
0122 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
20/4972			23.12.2020

Tilsynsrapport

1. INNLEDNING

Finanstilsynet gjennomførte et stedlig tilsyn i Formuesforvaltning Aktiv Forvaltning AS (heretter omtalt som Foretaket) med elektroniske møter 15. mai, 22. og 23.juni 2020.

Foretaket har konsesjon til å tilby investeringstjenestene som nevnt i verdipapirhandelloven (vphl.) § § 2-1 (1) nr. 1, 2, 4, 5 og 6, samt tilknyttede tjenester nr, 1,2, 3,4,5, og 6 iht. vphl. § 2-6 (1).

Foretaket yter uavhengig investeringsrådgivning. Foretaket oppgir å være Norges største ikke-bankeide investeringsrådgiver med 80 milliarder kroner under forvaltning på vegne av sine kunder. Målgruppen er formuende personer som har mer enn 1 mill. USD plassert i finansielle aktiva.

Foretaket mottok foreløpig tilsynsrapport (Rapporten) i brev av 12. november 2020, og har gitt sine kommentarer til denne i brev av 5. desember 2020 (Tilsvaret).

2. ORGANISERING AV KONTROLLFUNKSJONEN

2.1 Rettslig utgangspunkt

Det følger av verdipapirhandelloven § 9-16 første ledd nr. 1 at et verdipapirforetak skal ha tilstrekkelige og betryggende retningslinjer, rutiner og kontrollmetoder som skal sikre at foretaket, dets ledere, ansatte og tilknyttede agenter etterlever sine forpliktelser etter lov og forskrifter. Videre følger det av artikkel 25 i delegert kommisjonsforordning (EU) 2017/565, jf. verdipapirforskriften § 2-2, at verdipapirforetak som fordeler funksjoner internt skal sikre at den øverste ledelsen har ansvar for å sikre at foretaket oppfyller sine forpliktelser etter verdipapirhandelloven.

Det følger av forordningens artikkel 22 nr. 2 at verdipapirforetak skal innføre og opprettholde en fast og effektiv compliancefunksjon som opptrer uavhengig og har nærmere bestemte ansvarsområder. Som følge av at compliancefunksjonen skal være uavhengig har Finanstilsynet i punkt 3.2 i rundskriv 5/2015 Kontrollfunksjonen (Compliancefunksjonen) i verdipapirforetak, lagt til grunn at daglig leder som hovedregel ikke kan være complianceansvarlig i foretaket. Et unntak gjelder for mindre foretak, dersom kontrolloppgavene samtidig utkontrakteres, jf. rundskrivets

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Leif Roar Johansen
Dir. tlf 22 93 98 10

punkt 6. Mindre foretak kan også ha en samlet risikostyrings- og compliancefunksjon, forutsatt at funksjonene rapporterer direkte til styret og dette ikke svekker compliancefunksjonens effektivitet og uavhengighet. Dersom funksjonene er samlet, må foretaket dokumentere og begrunne dette.

Etter forordningens artikkel 22 nr. 3 bokstav b) og d) skal foretakets ledelsesorgan utnevne og erstatte en person som skal ha ansvar for compliancefunksjonen, og som ikke selv er involvert i utførelsen av de tjenestene eller virksomhetene som overvåkes. På denne bakgrunn har Finanstilsynet i rundskriv 5/2015 punkt 3.2 lagt til grunn at heller ikke faktiske ledere for foretakets investeringstjenestevirksomhet kan utpekes som complianceansvarlig i foretaket.

Det følger imidlertid av forordningens artikkel 22 nr. 4 at verdipapirforetaket ikke trenger å overholde nr. 3 bokstav d) dersom det kan godtgjøre at det, i betraktning av virksomhetens art, størrelse og kompleksitet samt arten og omfanget av foretakets investeringstjenester og -oppgaver, ikke er forholdsmessig å kreve dette, og at foretakets etterlevelsesfunksjon fortsatt er effektiv. I så fall skal verdipapirforetaket vurdere om etterlevelsesfunksjonens effektivitet er forringet. Vurderingen skal ajourføres regelmessig.

Utkontraktering av compliancefunksjonen er tillatt med de begrensningene som følger av verdipapirhandelloven § 9-16 annet ledd og forordningens artikkel 30 og 31. Finanstilsynet har i rundskriv 5/2015 punkt 6 lagt til grunn at foretak som utkontrakterer samtlige kontrolloppgaver som hører under compliancefunksjonen, likevel skal utpeke en medarbeider i foretaket som complianceansvarlig. Vedkommende må følge opp tjenesteyter og påse at oppgavene blir utført i tråd med avtalen.

I henhold til rundskriv 5/2015 punkt 7 skal verdipapirforetak løpende sende melding til Finanstilsynet om endringer i hvem som er utpekt som complianceansvarlig og kontaktinformasjon til vedkommende.

2.2 Finanstilsynets foreløpige vurderinger i Rapporten

Det fremgår av stillingsinstruks for Ansvarlig for Compliance & Risk at daglig leder er utpekt som compliance- og risikostyringsansvarlig, og at disse funksjonene er utkontraktert til morselskapet Formuesforvaltning AS. Daglig leder har som compliance- og risikostyringsansvarlig ansvaret for å følge opp det utkontrakterte arbeidet. Videre fremgår det av stillingsinstruksen for Head of Compliance i Formuesforvaltning AS at denne rapporterer til styret i Foretaket.

Som nevnt er det adgang til å utkontraktere verdipapirforetakets compliancefunksjon, blant annet under forutsetning av at det samtidig utpekes en medarbeider i foretaket som complianceansvarlig. Formålet med dette er å sikre oppfølging av det utkontrakterte arbeidet. Foretaket har her plassert dette ansvaret hos daglig leder, som også er faktisk leder for Foretakets plasseringsvirksomhet. Etter Finanstilsynets vurdering er dette ikke i samsvar med forordningens artikkel 22 nr. 2 og nr. 3 bokstav d). Siden vesentlige deler av compliancefunksjonens arbeid vil gå ut på å kontrollere faktisk leders arbeid, kan ikke faktisk leder samtidig være utpekt som ansvarlig for å følge opp det utkontrakterte arbeidet. Dette gjelder selv om vedkommende tredjepart rapporterer direkte til Foretakets styre. For ordens skyld tilføyes at unntaket i artikkel 22 nr. 4 ikke synes å være anvendelig i dette tilfellet.

Finanstilsynet bemerker for øvrig at foretaket ikke kan anses som et mindre foretak, og stilte derfor spørsmål ved om Foretaket har anledning til å operere med en samlet compliance- og risikostyringsfunksjon, jf. rundskriv 5/2015 punkt 3.2.

Finanstilsynet gjorde videre oppmerksom på at det ikke kunne se å ha mottatt noen melding fra Foretaket i forbindelse med at daglig leder ble utpekt som complianceansvarlig, jf. rundskriv 5/2015 punkt 7. Formålet med meldeplikten er nettopp å gi Finanstilsynet anledning til løpende å kontrollere at compliancefunksjonen er tilfredsstillende organisert.

2.3 Foretakets kommentarer i tilsvaret

Foretaket viser til at konsernets Compliance & Risk-funksjon (heretter omtalt som C&R) fungerer som en permanent og uavhengig kontrollfunksjon og har definerte ansvarsområder og vurderes å ha nødvendig autoritet, ressurser og kunnskap i overenstemmelse med krav i delegert kommisjonsforordning (EU) 2017/565 artikkel 22 nr. 3 bokstav a). Gjeldende organisering er slik at konsernets C&R velges og løpende evalueres av styret i Foretaket i overenstemmelse med forordningens artikkel 22 nr. 3 bokstav b). All rapportering fra C&R gjennomføres til styret i Foretaket.

Foretaket viser til at ansvaret for å følge opp den utkontrakterte tjenesten er knyttet til det ansvaret daglig leder har for å sikre betryggende organisering av virksomheten i henhold til verdipapirhandelloven § 9-16. I gjeldende organisering utpekes C&R av styret i Foretaket. Tilsvarende gjelder at styret godkjenner enhetens kontrollplan etter innstilling fra Revisjonsutvalget. Både Revisjonsutvalget og styret gjør løpende evaluering av C&R sine leveranser. C&R rapporterer direkte til styret på gjennomførte kontroller. Enhetens governance-prinsipper anses derfor de facto å være oppfylt sett mot krav i forordningens artikkel 22. Rollen til daglig leder i oppfølging av utkontraktert C&R er derfor snarere en del av hans rolle for å sikre at det er forsvarlig fordeling av ansvar i virksomheten og at det er forsvarlig internkontroll, herunder at foretaket har en fungerende C&R funksjon, jf. også internkontrollforskriften § 4, som pålegger daglig leder det formelle ansvaret for at risikostyring og internkontroll er forsvarlig etablert i tråd med retningslinjer fastsatt av styret. Daglig leder har ingen formell eller reell instruksjonsrett over C&R. Daglig leder utfører heller ingen kontrolloppgaver. Daglig leders rolle i Foretaket går ikke ut over det som følger av internkontrollforskriften § 4. Foretaket vurderer at dagens organisering med utkontraktert C&R er likestilt med organiseringen av C&R som en intern funksjon i Foretaket.

Foretaket er enig med Finanstilsynet i at plassering av complianceansvaret hos daglig leder samtidig som han er faktisk leder for foretakets plasseringsvirksomhet kan medføre en potensiell konflikt. Foretaket har igangsatt en prosess for å utpeke en annen ansatt som faktisk leder for plasseringsvirksomheten. Dette vil medføre at selskapets daglige leder ikke vil være operativt ansvarlig for driften av noen av tjenestene. Foretaket presiserer at foretakets plasseringsvirksomhet har et svært begrenset omfang og kun innenfor garantistillelse.

Foretaket har videre igangsatt en prosess for å tydeliggjøre ansvarsdeling mellom daglig leder og styret i stillingsinstruksen til daglig leder. Foretaket beklager at det ikke ble innsendt melding om at daglig leder ble utpekt som complianceansvarlig. For å sikre kompletthet av meldinger til Finanstilsynet vil Foretaket fremover vurdere meldeplikt ved enhver personal- eller organisasjonsendring.

Når det gjelder samlet compliance- og risikostyringsfunksjon viser Foretaket til at dette har vært vurdert opp mot de krav som stilles i Finanstilsynets Rundskriv 5/2015. Foretakets vurdering legger vekt på at regelverket ser for seg en risikostyringsfunksjon for større foretak, der funksjonen kan dekke blant annet markedsrisiko, kredittrisiko, valutarisiko og operasjonell risiko. Foretaket har ingen markedsrisiko (på egen balanse), svært begrenset kredittrisiko og valutarisiko (kun for kundefordringer og bankinnskudd), men er primært eksponert for operasjonell risiko hvor compliancerisikoen er den helt dominerende. Det er operasjonell risiko som er hovedfokus i arbeidet til C&R. Operasjonell risiko har veldig tett relasjon til etterlevelsen av interne retningslinjer, som dekkes av en tradisjonell C&R enhet. Foretakets tjenestespekter er konsentrert til investeringsrådgivning og porteføljeforvaltning. Tjenestene ordreformidling og ordreutførelse tilbys i tilknytning til investeringsrådgivningen. Foretaket har konsesjon til garantistillelse, men som beskrevet i konsesjonssøknaden for denne tjenesten er dette kun for å sikre kunders tilgang til fond som krever fulltegningsgaranti. Denne tjenesten fungerer dermed i praksis som et aksessorium til de øvrige tjenestene, og representerer ikke et selvstendig virksomhetsområde. Bruken av tjenesten er også i praksis svært begrenset.

Foretaket har videre ingen tilknyttede agenter. De norske filialene representerer primært en compliancerisiko, men filialene er sterkt sentralstyrt og har ingen lokale fullmakter til å avvike fra Foretakets regelverk. Foretaket vurderer at det er viktige synergieffekter av å ha en samlet C&R-enhet der flere av vurderingene vil være glidende mellom styring av operasjonell risiko og vurdering av etterlevelsen av interne og eksterne krav. Foretaket vurderer at en samlet C&R-enhet bidrar til å gjøre bedre vurderinger av prosesser man ofte ser i forbindelse med kontroller på etterlevelsen av lovkrav, interne retningslinjer og årsaker til innrapporterte operasjonelle hendelser, og at en samlet organisering er viktig for å kunne sikre et best mulig internkontrollopplegg, en best mulig regelverksetterlevelse og en høyest mulig kvalitet i de tjenester som ytes til foretakets kunder.

2.4 Finanstilsynets konklusjon

Finanstilsynet tar til etterretning at Foretaket vil igangsette en prosess for å utpeke en annen ansatt enn complianceansvarlig som faktisk leder for plasseringsvirksomheten, og at Foretaket vil gjennomgå sine rutiner med hensyn til innmelding av relevante personalendringer til Finanstilsynet.

Finanstilsynet tar videre til etterretning Foretakets redegjørelse for hvorfor foretaket anser det forsvarlig og hensiktsmessig å operere med en samlet compliance- og risikostyringsfunksjon. Ved eventuelle endringer i det totale risikobildet ved Foretakets virksomhet legger Finanstilsynet til grunn at spørsmålet om å ha separate compliance- og risikostyringsfunksjoner tas opp til fornyet vurdering.

3. INFORMASJONS- OG KOMMUNIKASJONSTEKNOLOGI

3.1 Rettslig utgangspunkt

Det følger av forskrift om informasjons- og kommunikasjonsteknologi (IKT-forskriftens) §2 første ledd at Foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten. Det skal 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.

Det følger av IKT-forskriftens §5 at foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

Det følger av IKT-forskriftens §3 at Foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene. Foretaket skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten. Prosessen skal blant annet definere klare ansvarsforhold og omfatte oppfølging av tiltak som iverksettes som et resultat av den gjennomførte risikoanalysen. Foretaket skal 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.

Videre følger det av IKT-forskriftens §12 at foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles etter denne forskrift. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretak under tilsyn også gis rett til å kontrollere, herunder revidere de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal også sikre håndtering av taushetsbelagt informasjon. Avtalen skal videre sikre at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Finanstilsynet finner det nødvendig som et ledd i tilsynet med foretaket. Foretaket skal sikre, i egen regi eller gjennom et formalisert samarbeid med andre foretak enn IKT-leverandøren, at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalen."

3.2 Finanstilsynets foreløpige vurderinger i Rapporten

Retningslinjer for bruk av eksterne sikkerhetstestere
Foretaket benytter seg av eksterne leverandører av etiske innbruddstjenester for å teste og forbedre Foretakets digitale forsvarsevne. Foretaket opplyste at det ikke var utformet retningslinjer eller policy for bruk av slike tjenester. Ved å benytte eksterne leverandører til denne typen tjenester kan Foretaket komme i situasjoner der leverandøren får tilgang til sensitiv informasjon, eventuelt skape situasjoner som kan true sikkerhet og stabilitet for Foretakets systemer. For best mulig å sikre seg mot nevnte uønskede situasjoner, er det Finanstilsynets vurdering at Foretaket bør etablere retningslinjer for utvelgelse av leverandører til slike tjenester, jf. IKT-forskriften §5 første setning. Retningslinjene bør stille krav til frekvens og utførelse av tjenesten. Retningslinjer for bruk av eksterne leverandører for bør også bygges på allment aksepterte standarder.

Bruk av lokale administrasjonsrettigheter
Foretaket benytter seg av lokale administratorbrukere på Foretakets arbeidsstasjoner. Lokale administratorrettigheter kan gi virksomhetens brukere og eventuelle angripere skriverettigheter til systemområder. Dette medfører at Foretakets systemportefølje blir lettere tilgjengelig for uønskede hendelser og digitale angrep. Sluttbrukere har generelt ikke behov for administratorrettigheter til lokale arbeidsstasjoner og det anbefales derfor å fjerne administratorrettigheter fra vanlige kontorbrukere og heller distribuere virksomhetsgodkjent programvare fra et felles distribusjonspunkt i Foretaket.

Risikoanalyser for IT-området
Finanstilsynet kunne ikke se av Foretakets risikoanalyse for IT-området at Foretaket gjennomfører vurderinger av hvor lang tid Foretaket kan unnvære tilgang til sine systemer og hvor mye data man kan tape før en situasjon blir kritisk for virksomheten. Risikovurderinger skal foregå årlig eller ved vesentlige endringer i forhold som omhandler Foretakets IT-systemer der leverandørrisiko for viktige IT-løsninger er et moment, jf. IKT-forskriften §3 tredje ledd. Risikovurderingene skal dokumenteres.

Leverandøravtaler for kritiske og viktige systemer.
Finanstilsynet kunne ikke se at Foretakets avtaler om utkontraktering av IT-systemer gir Foretaket uinnskrenket tilgang til revisjon og kontroll hos systemleverandører av alle elementer som kan påvirke en leveranse, jf. IKT-forskriften §12 første ledd. Uinnskrenket revisjons og kontrollrettighet skal også omfatte Finanstilsynet, jf. IKT-forskriften §12 andre ledd. Videre forventer Finanstilsynet at utkontrakteringsavtaler også regulerer exit-bestemmelser, gjennomføring av beredskapstester og leverandørens bruk av underleverandører.

3.3 Foretakets kommentarer i tilsvaret

Foretaket tar Finanstilsynets kommenter angående retningslinjer for bruk av eksterne sikkerhetstestere til etterretning og vil utarbeide spesifikke rutiner for sikkerhetstester.

Når deg gjelder bruk av lokale administrasjonsrettigheter viser Foretaket til at vanlige brukere ikke har disse rettighetene, men det har vært enkelte spesialister med behov som er løst med å gi lokal administrasjonsrett. Foretaket har igangsatt arbeid med å løse dette på en annen måte.

Foretaket tar Finanstilsynets kommentar om risikoanalyser for IT-området til etterretning og vil implementere en mer nyansert risikovurdering.

Foretaket tar videre Finanstilsynets kommentar angående leverandøravtaler for kritiske og viktige systemer til etterretning og vil sikre at avtaler oppdateres med viktige klausuler.

3.4 Finanstilsynets konklusjon

Finanstilsynet tar Foretakets tiltak til etterretning og ber Foretaket å prioritere det igangsatte arbeidet med lokale administrasjonsrettigheter. Det bes om en orientering straks dette er løst. Det bes også om orientering når avtalene er endret og om kopi av endrede retningslinjer for bruk av eksterne sikkerhetstestere når det er utarbeidet.

For Finanstilsynet

Roy V. Halvorsen
seksjonssjef

Leif Roar Johansen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.