FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

ODIN FORVALTNING AS
Postboks 1771 Vika
0122 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
21/3736			24.11.2021

Tilsynsrapport IT-tilsyn

Finanstilsynet gjennomførte stedlig tilsyn i ODIN Forvaltning AS (Foretaket) 8. og 13. april 2021. Tilsynet ble gjennomført med en IT-del 8. april. Det vises til egen rapport om det generelle tilsynet. Formålet med IT-delen av tilsynet var å gjøre en vurdering av hvordan Foretaket administrerer, drifter, og sikrer sine IT-systemer. Finanstilsynet ønsket å få en samlet vurdering av risiko og hvilken kontroll Foretaket har med disse.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 7. juli 2021 og styrets kommentarer til rapporten i brev av 26. august 2021.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Beredskapstester

Rettslig utgangspunkt:

IKT-forskriften § 11. Driftsavbrudd og kriseberedskap.

I foreløpig rapport påpekte Finanstilsynet at Foretaket ikke har gjennomført årlige beredskapstester for IT-området.

Styret informerer i tilsvaret at covid-19 situasjonen medførte at slike tester ikke ble gjennomført i 2020. Videre opplyste Foretaket at det er gjennomført beredskapstest i mai i 2021 og at Foretaket for fremtiden vil sørge for at slike tester gjennomføres årlig.

Finanstilsynet tar styrets kommentarer til etterretning.

Risikovurderinger for IKT-området

Rettslig utgangspunkt:

IKT-forskriften § 3. Risikoanalyse.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Arild Tømmerås
Dir. tlf 22 93 98 00

Finanstilsynet etterlyste i sin foreløpige rapport at Foretaket gjør bruk av scenariobaserte risikoanalyser på IT-området.

Av styrets tilsvar fremgår det at styret tar Finanstilsynets etterlysning til etterretning og at Foretaket vil implementere rutiner for å systematisere og dokumentere scenariobaserte risikovurderinger på IT-området og legge disse vurderingene til grunn for fremtidige beredskapstester og øvelser.

Finanstilsynet tar styrets kommentar til etterretning.

Tilgangsstyring for IT-leverandører og loggføring i systemer

Rettslig utgangspunkt:

IKT-forskriften § 5. Sikkerhet.

Foretaket hadde på tilsynstidspunktet ikke etablert dokumenterte rutiner for oppfølging av, eller kontroll med, tilganger til IT-systemer som gis til Foretakets leverandører. Finanstilsynet påpekte i foreløpig rapport svakheter ved Foretakets rutiner for tildeling av rettigheter til leverandører og var kritisk til at tredjeparter på tilsynstidspunktet hadde tilgang til Foretakets kjernesystemer uten at rutiner for oppfølging eller kontroll av tilganger var tilstrekkelig etablert. Videre påpekte Finanstilsynet svakheter ved foretakets kontroll med tilganger mhp. overvåkingen av data som blir aksessert i Foretakets kjernesystemer. Av foreløpig rapport fremgikk det at Finanstilsynet forventer at Foretaket har kontroll med hvilke av leverandørens brukere som har tilgang til sensitive data, og kan dokumentere dette.

I sitt tilsvar erkjenner styret at rutiner for sporing, kontroll og tilgangsstyring må formaliseres og forsterkes. Finanstilsynet merker seg fra styrets tilsvar at Foretaket har besluttet å utarbeide rutiner for tilgangsstyring, sporing og kontrollaktiviteter, inkl. kontroll med aksesserte data, og at disse gjennomføres og dokumenteres minimum kvartalsvis.

Finanstilsynet tar styrets tilsvar til etterretning og ber om å motta dokumentasjon på at tiltakene er gjennomført innen 31. januar 2022.

Rapportering av hendelser

Rettslig utgangspunkt:

IKT-forskriftens § 9. Avviks- og endringshåndtering.

Finanstilsynets vurdering i foreløpig rapport var at Foretaket ikke rapporterer hendelser i samsvar med IKT-forskriften § 9. Ved gjennomgang av Foretakets hendelser to siste kalenderårene fremkom det at Foretaket, etter Finanstilsynets vurdering, har hatt hendelser som er rapporteringspliktige etter IKT-forskriftens bestemmelse uten at rapportering til Finanstilsynet var gjennomført.

Rapporteringen skal normalt omfatte hendelser som Foretaket selv kategoriserer som alvorlighetsgrad svært alvorlig eller kritisk, men kan også omfatte andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk.

Styret opplyser i tilsvaret at de konkrete hendelsene ikke har vært vurdert som svært alvorlige eller av kritisk karakter. Styret noterer seg at Finanstilsynet mener det bør være en lavere terskel for innrapportering av hendelser på IT-området enn hva Foretaket hittil har lagt til grunn.
Det fremkommer også av styrets svar at Finanstilsynets vurdering tas til etterretning og at Foretaket vil følge Finanstilsynets oppfordring ved eventuelle fremtidige hendelser.

Finanstilsynet tar styrets tilsvar til etterretning.

Retningslinjer for bruk av eksterne sikkerhetstestere

Rettslig utgangspunkt:

IKT-forskriften § 5. Sikkerhet.

Finanstilsynet påpekte i foreløpig rapport at Foretaket på tilsynstidspunktet ikke hadde etablert retningslinjer for bruk av eksterne leverandører av etiske innbruddstjenester.

Styret skriver i sitt tilsvar at det tar Finanstilsynets merknader til etterretning og Foretaket vil utarbeide retningslinjer basert på allment aksepterte standarder.

Finanstilsynet tar styrets tilsvar til etterretning, og ber om å motta kopi av Foretakets retningslinjer for etiske innbruddstjenester innen 31. januar 2022.

Revisjoner og kvalitetskontroll

Rettslig utgangspunkt:

IKT-forskriften § 8. andre ledd.

Finanstilsynet påpekte i foreløpig rapport svakheter i Foretakets tredjelinjeforsvar for IT-området og etterlyste helhetlige revisjoner av området.

Styret tar i sitt tilsvar Finanstilsynets merknader til etterretning, og Foretaket vil sørge for at dette legges inn som en fast del av internrevisjonens årshjul.

Finanstilsynet tar styrets tilsvar til etterretning.

Utkontraktering

Rettslig utgangspunkt:

IKT-forskriftens § 12. Utkontraktering.

Finanstilsynet påpekte i foreløpig rapport at Foretakets avtale med leverandør av kundeinformasjonssystem anses som en utkontraktering ettersom systemet driftes på leverandørens løsninger. Avtalen med leverandøren er en databehandleravtale. Finanstilsynet anser ikke en

databehandleravtale til å være dekkende som utkontrakteringsavtale iht. IKT-forskriften, blant annet når det gjelder rett til innsyn og tilsyn med alle elementer hos leverandøren som kan påvirke systemleveransen.

Styret tar i sitt tilsvar til etterretning at avtalen ikke i tilstrekkelig grad tilfredsstiller IKT-forskriftens krav, og informerte om at de vil ta i bruk statens standardavtale med nødvendige tilpasninger for å sikre at avtalen dekker forskriftens krav til innhold i avtale om utkontraktering.

Finanstilsynet tar styrets tilsvar til etterretning, og ber om å motta en kopi av ny avtale med leverandøren innen 31. januar 2022.

Klassifisering av sensitiv informasjon:

Rettslig utgangspunkt:

IKT-forskriftens § 2. Planlegging og organisering.

I foreløpig rapport påpekte Finanstilsynet svakheter ved Foretakets retningslinjer og rutiner for klassifisering av sensitiv informasjon. Videre påpekte Finanstilsynet at dette kan medføre at informasjon med kritikalitet og sensitivitet ikke blir tilstrekkelig sikret. Finanstilsynet anser det er spesielt viktig at Foretak med systemer som kan inneholde kurssensitiv informasjon har tilfredsstillende kvalitet i nevnte rutiner.

Styret skriver i sitt tilsvar at det tar Finanstilsynets merknad til etterretning og det vil sørge for at Foretaks rutiner forsterkes, og at Foretaket vil implementere systemer for håndtering av slik informasjon.

Finanstilsynet tar styrets tilsvar til etterretning, og ber om å motta en kopi av Foretakets retningslinjer for klassifisering av sensitiv informasjon innen 31. januar 2022.

Kopi av dette brevet bes sendt til ekstern og intern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Arild Tømmerås
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.