FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

LIVSFORSIKRINGSSELSKAPET NORDEA LIV NORGE AS
Postboks 7078
5020 BERGEN

VÅR REFERANSE	DERES REFERANSE		DATO
22/9373	6ea3e2addf2f		29.01.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Livsforsikringsselskapet Nordea Liv Norge AS (Nordea Liv) 13. og 14. desember 2022.

Hensikten med tilsynet var å gjøre en vurdering av hvordan styring og kontroll med IKT-området blir ivaretatt. Finanstilsynet hadde et særskilt fokus på hvordan Nordea Liv ivaretar risikostyring på IKT-området samt hvordan IKT-området håndteres i foretakets arbeid med beredskap og kontinuitet, utkontraktering av IKT-tjenester og IKT-sikkerhet. Videre ble styring og kontroll med prosjekt for utvikling av nytt kjernesystem (heretter benevnt kjernesystemprosjektet) vurdert.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport av 13. juli 2023 og styrets svar i brev av 28. september 2023.

Finanstilsynet har følgende merknader etter tilsynet:

1 Styring og kontroll innen IKT-området

Det framgår av finansforetaksloven § 8-6 første ledd, at styret skal sørge for forsvarlig organisering av virksomheten. Videre framgår det av § 8-11 tredje ledd, at daglig leder blant annet skal sikre at det finnes forsvarlige styrings- og kontrollsystemer. Kravene til forsvarlig virksomhetsstyring er nærmere regulert i § 13-5. Det følger også av § 8-11 tredje ledd, at daglig leder er ansvarlig for at det er etablert instrukser for de ansattes arbeidsoppgaver og ansvarsforhold, samt rapporterings- og saksbehandlingsregler. Ifølge IKT-forskriften § 2 skal foretaket utarbeide beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte. Ytterligere utdypinger om styring og kontroll framgår av delegert kommisjonsforordning (EU) 2015/35 (Solvens II) Artikkel 258. Videre angir EIOPA[1] Guidelines on information and communication technology security and governance (EIOPA-BoS-20/600) (heretter EIOPA GL on ICT) retningslinje 2, ytterligere utdypinger knyttet til styring og kontroll på IKT-området.

1.1 Systemeiers rolle og ansvar

I tilsynsmøtet ble resultater fra internrevisjonens (Group Internal Audit, heretter GIA) undersøkelse "General IT Controls" i 2021 referert. En av påpekningene i rapporten var at systemeier sin rolle og ansvar ikke var formelt definert i Nordea Liv, og at ansvaret som systemeier for flertallet av

[1] European Insurance and Occupational Pensions Authority (EIOPA)

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Jarleif Lødøen
Dir. tlf. 22 93 98 00

forretningsapplikasjoner var tildelt én enkeltperson. En viktig del av det definerte ansvaret for applikasjonseier er å ivareta kravene til informasjonssikkerhet og gjennomføre pålagte sikkerhetskontroller. Med utgangspunkt i dette vurderte GIA at Nordea Liv ikke har en betryggende styring og kontroll av sine systemer og IKT-infrastruktur. I foreløpig rapport oppfattet Finanstilsynet denne påpekningen som kritisk og viktig, og forutsatte at arbeidet med å lukke avviket så snart som mulig ble gitt høy prioritet.

Fra styrets svar framgår det at avviket var lukket på tidspunkt for det stedlige tilsynet, og at Nordea Liv i 2023 har foretatt en gjennomgang av interne rutiner og opprettet en ny koordineringsrolle, Application Management Coordinator (AMO). Den ansvarlige for denne rollen skal bistå applikasjonseierne i deres arbeid, avholde faste oppfølgingsmøter og sikre at aktivitetene som pålegges applikasjonseierne blir utført.

Finanstilsynet tar styrets svar til etterretning.

1.2 Fastsettelse av styrende dokumenter for Nordea Liv

I foreløpig rapport var det Finanstilsynets oppfatning at Nordea-konsernet sine gruppedirektiver, -instrukser, -protokoller og -retningslinjer blir etablert med utgangspunkt i EBAs retningslinjer og at Nordea Life & Pension Holding (heretter L&P Gruppen) ved behov etablerer tilsvarende styrende dokumenter med utgangspunkt i relevante retningslinjer fra EIOPA. Videre påpekte Finanstilsynet at Nordea Liv må sikre at egne retningslinjer er utarbeidet i henhold til gjeldende regelverk for livsforsikringsforetak, inkludert EIOPAs retningslinjer.

Styret har i sitt svar vist til at L&P Gruppen sin retningslinje for intern virksomhetsstyring krever at foretakene i L&P Gruppen har rutiner og prosesser som sikrer at etablerte interne retningslinjer ivaretar ekstern regulering. Retningslinjen er implementert i Nordea Liv. Videre er det vist til at Nordea-konsernets rutiner/retningslinjer vurderes i en arbeidsgruppe i L&P Gruppen og at arbeidsgruppen anbefaler hvilke rutiner/retningslinjer som bør implementeres i foretakene i L&P Gruppen. Når Nordea Liv mottar anbefalinger fra L&P Gruppen vurderer administrasjonen om rutinen/retningslinjen skal implementeres i foretaket og fremlegger en innstilling til styret. Styret tar deretter den endelige beslutningen om rutinen/retningslinjen skal implementeres. Fra styrets svar har Finanstilsynet notert seg at Nordea Liv ikke er pålagt å følge L&P Gruppens anbefalinger.

Finanstilsynet tar styrets svar til etterretning.

2 Styring og kontroll - årlig risikoanalyse

IKT-forskriften § 3 krever at det minst årlig skal gjennomføres risikoanalyse med utgangspunkt i en dokumentert prosess, som fastsetter klare ansvarsforhold for gjennomføring samt definerer hvordan eventuelle tiltak iverksatt som resultat av analysen skal følges opp. Den årlige risikoanalysen skal ta utgangspunkt i fastsatte kriterier for å vurdere akseptabel risiko, slik at man kontrollerer at IKT-risikoen styres innen akseptable grenser.

I foreløpig rapport var det Finanstilsynets vurdering at Nordea Liv ikke overholder IKT-forskriftens krav til risikoanalyse på IKT-området, ved at mitigerende tiltak ikke planlegges eller iverksettes i tide for å sikre at IKT-virksomheten drives innenfor foretakets risikoappetitt over tid (jf. punkt 3.4 Livssyklus for program- og maskinvare nedenfor). Forholdet ble påpekt med bakgrunn i risikoen

forbundet med teknisk gjeld i Nordea Liv sine IKT-systemer, der styring og kontroll med leverandørstøtte for foretakets maskin- og programvare etter Finanstilsynets syn ikke ble tilstrekkelig ivaretatt. Finanstilsynet ba i foreløpig rapport om en kort redegjørelse for om Nordea Liv gjennomfører helhetlige årlige risikovurderinger på IKT-området, basert på kriterier for akseptabel risiko med tiltaksplaner for å redusere risiko til akseptabelt nivå, jf. IKT-forskriften § 3.

Av styrets svar framgår det at foretaket har etablert en prosess som etter styrets vurdering overholder kravene til årlig risikovurdering, jf. IKT-forskriftens § 3. Det framgår videre fra styrets svar at risikovurderingen tar utgangspunkt i foretakets risikotaksonomi, og at denne inkluderer et eget sett med IKT-risikoer (fordelt på sikkerhetsrelaterte og teknologirelaterte risikoer). Dersom restrisiko er utenfor foretakets risikoappetitt, vil tiltak bli iverksatt.

Finanstilsynet understreker viktigheten av at tiltak iverksettes til rett tid for å sikre at IKT-virksomheten over tid ikke drives utenfor foretakets risikoappetitt.

3 IKT-sikkerhet

IKT-forskriften § 5 stiller krav til at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal det finnes retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Ytterligere utdypinger finnes i flere retningslinjer i EIOPA GL on ICT.

IKT-forskriften § 13 stiller krav til at det er etablert en oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Av forskriften framgår det videre at det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet og som dokumenterer at forskriftens krav er oppfylt. EIOPA GL on ICT utdyper i flere retningslinjer IKT-forskriftens bestemmelser vedrørende oversikt over IKT-utstyr. Det vises til retningslinjene om identifisering og utbedring av sårbarheter og håndtering av teknisk gjeld, herunder styring og kontroll med eventuelle sårbarheter knyttet til manglende leverandørstøtte. Av EIOPA GL on ICT retningslinje 14 framgår det at oversikten bør inneholde tilstrekkelige konfigurasjonsdata og angi avhengigheter mellom utstyr/komponenter. Videre at det bør være registrert tilstrekkelig informasjon for å kunne identifisere eiendelen, dens plassering, eiendelens sikkerhetsklassifisering og eier.

3.1 Oversikt over program- og maskinvare, samt sårbarheter knyttet til dette

I foreløpig rapport var det Finanstilsynets forventning at Nordea Liv har oversikt over sine systemer, tjenester og utstyr (program- og maskinvare, HW/SW), der utstyrsoversikten inkluderer avhengigheter mellom systemer/tjenester og utstyr på komponentnivå. Det var videre Finanstilsynet forventning at oversikten har navn på komponent, leverandør, bruksområdet/funksjonalitet, versjonen som er i bruk Nordea Liv, siste tilgjengelige versjon fra leverandør, status på støtte fra leverandør og eventuelt dato for opphør på støtte fra leverandør for komponenter som inngår i utstyrsoversikten. Det var videre Finanstilsynet forventning at Nordea Liv har oversikter med

tilstrekkelig informasjon over foretakets sårbarheter[2] knyttet til program- og maskinvare for å kunne vurdere, beslutte og iverksette risikoreduserende tiltak på kort og lang sikt.

Fra styrets redegjørelse framgår det at Nordea Liv mener å ha god oversikt over program- og maskinvare, samt deres status, med tanke på å ivareta kontroll med sårbarhetsrisiko og å iverksette nødvendige risikoreduserende tiltak. Det framgår videre at informasjonen om Nordea Liv sine IKT-systemer og komponenter er lagret i flere systemer, organisert ut fra informasjonsbehovet det enkelte området i Nordea Liv har for oppfølging av IKT-systemene. Finanstilsynet har notert seg at styret erkjenner at deler av informasjonen relatert til relasjoner mellom applikasjoner, komponenter og "lifecycle management" ikke er fullstendig oppdatert i systemet for virksomhetsarkitektur, men at det er igangsatt en revisjon og oppdatering av dette.

Det framgår videre av styrets svar at Nordea-konsernet i 2023 gjennomfører endringer i prosessen for Asset og Configuration Management der applikasjonseiere blant annet vil få bedre oversikt over, og varsling om, programvarekomponenter som nærmer seg utløp av leverandørstøtte. Styret oppfatter at dagens organisering gir et godt og tilpasset bilde for den daglige risikooppfølgingen.

Finanstilsynet tar styrets svar til etterretning.

3.2 Identifisering og utbedring av sårbarheter

3.2.1 Eierskap og ansvar for sårbarhetsprosessen

I foreløpig rapport viste Finanstilsynet til at Nordea-konsernets internrevisjon i 2021 mente at eierskapet og ansvaret for sårbarhetsprosessen i Nordea Liv var uklar.

Fra styrets svar har Finanstilsynet notert seg at det er den enkelte systemeiers ansvar å påse at identifiserte sårbarheter blir lukket og at det derfor ikke er grunnlag for å si at eierskapet/ansvaret for sårbarhetsprosessen er uklar. Sårbarheter i plattform og infrastruktur håndteres av dedikerte team sentralt i Nordea-konsernet. Sårbarheter i komponenter som benyttes i egenutviklede applikasjoner blir håndtert i de interne utviklingsteamene i henhold til styringsprosessen for foretakets smidige utviklingsløp. Sårbarheter som ikke er mulig å lukke i henhold til kravene blir risikovurdert og tilordnet en risikoeier.

Videre framgår det av styrets svar at et av ansvarsområdene for den nyopprettede rollen Application Management Coordinator (AMC) er å bistå "systemeierne og sikre at deres oppgaver blir fulgt opp på en effektiv måte".

Finanstilsynet forventer at AMC-rollen følger opp ansvaret den systemansvarlige har for å identifisere og lukke sårbarheter. Finanstilsynet forventer videre at Nordea Liv har tilstrekkelig oversikt og informasjon knyttet til sårbarheter, inkludert status på leverandørstøtte for maskin- og programvare, og at Nordea Liv løpende vurderer og iverksetter risikoreduserende tiltak på kort og

[2] Sårbarheter oppfattes som programfeil som kan utnyttes og manglende leverandørstøtte som utgjør risiko for at systemer/tjenester slutter å fungere som forventet. Dette omfatter sårbarheter som avdekkes i automatiske sårbarhetsskanninger (på maskiner/utstyr som har støtte for maskinell sårbarhetsskanning) og sårbarheter som identifiseres ved manuelle kontroller.

lang sikt for å hensynta dette. Videre forventer Finanstilsynet at sårbarhetsstatuser inngår i ledelses- og styrerapporteringen på IKT-området.

Finanstilsynet ber styret være særskilt oppmerksom på den IKT-risiko og konsekvens som ikke-utbedrede sårbarheter, og manglende leverandørstøtte, kan utgjøre for foretakets IKT-leveranser på kort og lang sikt.

3.2.2 Framdrift og status på sårbarhetshåndtering

Basert på mottatt dokumentasjon og informasjon som framkom i tilsynsmøtet oppfattet Finanstilsynet at Nordea Liv var tilfreds med framdriften knyttet til utbedring av identifiserte kritiske sårbarheter.

Finanstilsynet viste i foreløpig rapport til at utnyttelse av sårbarheter kan utgjøre en trussel mot det etablerte forsvarsverket mot ondsinnede angrep og vurderte det derfor som kritisk at Nordea Liv har oversikt over åpne sårbarheter, og at arbeidet med å lukke de kritiske sårbarhetene så raskt som mulig har høyeste prioritet. Finanstilsynet bad på denne bakgrunn om styrets kommentar, samt en status på sårbarheter pr. system med detaljinformasjon som angitt i punkt 3.1 Oversikt over program- og maskinvare.

Fra styrets svar har Finanstilsynet notert seg opplysningen om at foretaket gjennomfører "kontinuerlig og grundig sårbarhetsskanning" med oppfølging av identifiserte sårbarheter, og at det er tilsvarende fokus" på å sikre leverandørstøtte på viktige og kritiske systemer og komponenter". Finanstilsynet registrerer at styret opplyser at det finnes tilfeller der enkeltkomponenter har manglet leverandørstøtte, der regelmessig skanning ikke har identifisert sårbarheter, og at komponenten har kunnet fjernes uten signifikante konsekvenser for virksomheten.

Finanstilsynet ber styret være særskilt oppmerksom på den IKT-risiko som manglende leverandørstøtte vil kunne ha for foretakets IKT-systemer. Styret bør være særskilt oppmerksom på, og følge opp, IKT-systemer/-plattformer som ikke har støtte for automatisk skanning.

3.3 Håndtering av teknisk gjeld

I foreløpig rapport var det Finanstilsynets forståelse at Nordea Liv har teknisk gjeld og ikke-utbedrede sårbarheter knyttet til flere systemer, og at denne tekniske gjelden har bygget seg opp over mange år. Det var Finanstilsynets oppfatning at det var størst teknisk gjeld knyttet til Nordea Liv sine viktigste fag-/kjernesystemer. Av mottatt dokumentasjon oppfattet Finanstilsynet at fag-/kjernesystemer har blitt kjørt på programversjoner som har manglet støtte fra leverandørene, og at tilliggende program- og maskinvare også er kjørt uten at leverandøren har hatt støtte for de versjoner og det tekniske utstyr som er benyttet. Teknisk gjeld og manglende leverandørstøtte kan etter Finanstilsynets vurdering utgjøre en betydelig risiko for Nordea Liv sine tjenesteleveranser.

Fra styrets svar har Finanstilsynet notert seg at styret oppfatter at det ene kjernesystemet har hatt leverandørstøtte til enhver tid, og at de ulike forhold som Finanstilsynet pekte på i foreløpig rapport ligger noe tilbake i tid. Dokumentasjonen Finanstilsynet har mottatt viser blant annet at operativsystemet som det ene kjernesystemet kjørte på var uten leverandørstøtte i mer enn ett år, at systemets jobbstyringsverktøy var kjørt i "noen måneder" uten leverandørstøtte og at det var uklarhet rundt leverandørstøtte knyttet til lagringssystemet. Finanstilsynet vurderer på bakgrunn av dokumentasjonen at foretaket i perioder har hatt manglende leverandørstøtte.

Finanstilsynet påpeker foretakets ansvar for å ha oversikt over og følge opp status på leverandørstøtte samt iverksette mitigerende tiltak slik at IKT-området drives innen grensene for akseptabel risiko.

I foreløpig rapport ba Finanstilsynet om foretakets vurdering av hvordan eventuelle forsinkelser i kjernesystemprosjektet og den valgte konverteringsstrategien (jf. punkt 5.5 Konvertering og oppslag i historiske data nedenfor) vil kunne påvirke utviklingen i teknisk gjeld. I dette inngår utfordringer knyttet til manglende leverandørstøtte, og hvordan eventuelle endringer i leverandørstøtte kan ha konsekvenser for fremdriften.

Av styrets svar framgår det at faseinndelingen av migreringen for de tre kjernesystemene, samt planen for håndtering av teknisk gjeld og programvareoppdateringer er verktøyet for å fange opp konsekvenser av forsinkelser og iverksetting av tiltak. IT Drift og kjernesystemprosjektet vil samarbeide tett og koordinere linjens og prosjektets oppfølging for å sikre det ikke etableres ytterligere teknisk gjeld. I tillegg skal samarbeidet sørge for at kritiske tjenester og systemer til enhver tid kjører på versjoner og teknisk utstyr som er støttet av leverandører.

Finanstilsynet tar styrets svar til etterretning. Finanstilsynet understreker viktigheten av å følge opp status på leverandørstøtte for enkeltkomponentene av program- og maskinvare, inkludert driftsplattform og infrastruktur for kjernesystemene, og de omkringliggende systemene dersom ferdigstilling av kjernesystemprosjektet blir forsinket.

3.4 Livssyklus for program- og maskinvare

I foreløpig rapport var det Finanstilsynets vurdering at Nordea Liv manglet et bredt og helhetlig livssyklusfokus for håndtering av teknisk gjeld og sårbarheter knyttet til program- og maskinvare. Finanstilsynet vurderte dette som en forhøyet IKT-sikkerhetsrisiko.

Av styrets svar framgår det at foretaket overordnet er enig med Finanstilsynet i viktigheten av et bredt og helhetlig livssyklusfokus for håndtering av sårbarheter knyttet til program- og maskinvare. Det framgår videre fra styrets svar at utbedring av sårbarheter er et viktig satsningsområde på IKT-området og er forankret i ny IKT-strategi.

Teknisk gjeld knyttet til gamle kjernesystemer er vurdert som foretakets største systemmessige risiko. Styret mener foretaket har god oversikt over utestående feil og mangler, og har satt av kapasitet for å løse prioriterte oppgaver innenfor teknisk gjeld. Utbedringsarbeidet følges tett og parallelt med kjernesystemprosjektet.

Finanstilsynets forventer at Nordea Liv har et bredt og helhetlig livssyklusfokus for systemløsningene som håndterer sårbarheter knyttet til program- og maskinvare og teknisk gjeld, og iverksetter nødvendige risikoreduserende tiltak ved behov.

4 IKT-utkontraktering

Ifølge IKT-forskriftens § 2 annet ledd skal foretaket ha retningslinjer som skal sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette gjelder blant annet krav til skriftlig avtale, at avtalen sikrer foretakets rett til å kontrollere og revidere leverandørens aktiviteter samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av § 2 fjerde ledd at avtaler om utkontraktering av IKT-virksomhet og endring av slike avtaler skal behandles av styret. Styret skal presenteres en plan for utkontrakteringen, en risikovurdering av utkontrakteringsforholdet og en beskrivelse av hvordan foretaket skal sikre leveransen. EIOPA sine "Guidelines on system of governance" (EIOPA-BoS-14/253), EIOPA GL on ICT (EIOPA-BoS-20/600) og "Guidelines on outsourcing to cloud service providers" (EIOPA-BoS-20-002) inneholder ytterligere utdypninger for krav til styring og kontroll ved utkontraktering av IKT-virksomhet.

4.1 Tjenester levert Nordea Liv fra Finans Norge Forsikringsdrift (FNF)

I tilsynsmøtet framkom det at Nordea Liv ikke oppfattet å ha utkontraktert virksomhet til Finans Norge Forsikringsdrift (FNF). Fra Finanstilsynets gjennomgang av FNF sine tjenester innen livs- og pensjonsforsikring var det i foreløpig rapport Finanstilsynet vurdering at Nordea Liv har utkontraktert flere IKT-tjenester til FNF, og at Nordea Liv må følge opp disse tjenestene i henhold til kravene i IKT-forskriftens §12.

Finanstilsynet registrerer fra styrets svar at styret er enig i at Nordea Liv har utkontraktert virksomhet til Finans Norge Forsikringsdrift.

Finanstilsynet understreker styrets ansvar for å følge opp IKT-virksomheten som er utkontraktert til FNF i henhold til IKT-forskriftens bestemmelser.

4.2 Oppfølging av leverandører og tjenester ved utkontraktert IKT-virksomhet

Basert på informasjon som framkom i tilsynsmøtet gjennomfører Nordea Liv regelmessige vurderinger av leveransene fra utkontraktert IKT-virksomhet, men det foretas ikke en egen årlig vurdering av leverandør og leveransebildet. Nordea Liv mente dette delvis er dekket i etablerte prosesser, men informerte om at vurdering av leverandører kun gjøres ved vesentlige triggere eller forhold knyttet til leveransene.

Finanstilsynet vurderte at Nordea Liv bør etablere en modell for styring og kontroll av utkontraktert virksomhet der leverandørene og leveransene systematisk og regelmessig følges opp gjennom møteplasser på operasjonelt, taktisk og strategisk nivå. Oppfølgingen bør gjøres gjeldende både for intern og ekstern IKT-utkontraktering.

Finanstilsynet registrerer fra styrets svar at styret er enig i Finanstilsynets vurdering og at styret vurderer dette som overveiende hensiktsmessig for all kritisk utkontraktering. Styret er enig i at oppfølgingen kan gjøres enda mer systematisk for å sikre at alle viktige og kritiske utkontrakteringer følger samme minstefrekvens for strategisk oppfølging og helhetlig evaluering. Det framgår videre fra styrets svar at Nordea Livs Third Party Risk Management (TPRM) prosess for kritiske utkontrakteringsavtaler utenfor Nordea-konsernet fra og med 2023 nå gjøres årlig mot tidligere hvert tredje år. Leverandører (inkludert Nordea-konsernet) skal minimum følges opp kvartalsvis på strategisk nivå, der Chief Technology Officer (CTO) skal delta. På taktisk nivå skal

det avholdes minimum månedlige møter, hvor avdelingsledere skal delta. Møter på operativt nivå skal minimum avholdes ukentlig.

Finanstilsynet tar styrets svar til etterretning.

4.3 Utkontraktering til skyleverandør i forbindelse med nytt kjernesystem

I forbindelse med presentasjon av kjernesystemprosjektet i tilsynsmøtet oppfattet Finanstilsynet at systemet vil være basert på skyteknologi. Videre oppfattet Finanstilsynet at IKT-konsern (Nordea-konsernet) har etablert et rammeverk for styring og kontroll med leveranser fra skytjenesteleverandører. Styring og kontroll av tjenestekjøp i forbindelse med skyteknologi vil kreve ny kompetanse og tilpasning av roller og ansvar i Nordea Liv sin organisasjon, herunder til de nye og endrede kravene som gjelder sammenlignet med en tradisjonell utkontrakteringsmodell.

I foreløpig rapport var det Finanstilsynet vurdering at det var viktig at Nordea Liv operasjonaliserer Nordea-konsernets rammeverk for styring og kontroll med skytjenesteleverandører i foretaket i god tid før det nye kjernesystemet skal tas i bruk og slik at Nordea Liv gjennom dette sikrer at foretaket har nødvendig kompetanse for å styre og kontrollere bruken av skytjenester.

Av styrets svar framgår det at Nordea-konsernet har etablert et eget rammeverk for innkjøp, implementering, bruk og kontroll av skybaserte tjenester. Det framgår videre at selve anskaffelsen følger en fastsatt prosess som inkluderer ulike sjekkpunkter og kontroller, eksempelvis Third Party Risk Management (TPRM), Privacy Impact Analysis (PIA) samt godkjenningsrutiner for arkitektur og sikkerhet. Det framgår videre fra styrets svar at selv om anskaffelsesprosessen støttes av sentrale enheter i Nordea-konsernet, har Nordea Liv lagt stor vekt på å bygge egen kompetanse gjennom blant annet kursing og den praktiske gjennomføringen av innkjøpsprosessene.

Når det gjelder kjennskap til og oppfølging og etterlevelse av ulike lover og interne regelverk framgår det av styrets svar at Nordea Liv i prosessen med evaluering og anskaffelse av nytt kjernesystem har opparbeidet seg regulatorisk kompetanse ved analyser og gjennomganger av relevant regelverk, samt Nordea-konsernets direktiver og styringsdokumenter. Videre framgår det av styrets svar at Nordea Liv har gjennomført risikoanalyser for å identifisere risikoer og tiltak.

Det framgår av styrets svar at det i implementeringsprosjektet er tatt hensyn til at løsningen blir levert som Software as a service (SaaS), noe som krever utvidet kompetanse på flere områder. Opplæring er planlagt og allerede iverksatt. I tillegg til skyteknologi omfatter opplæringen temaer knyttet til operasjonell IKT-drift, tredjepartskontroll og -overvåkning, sikkerhet, etterlevelse og Nordea-konsernets interne rammeverk. Fra styrets svar har Finanstilsynet notert seg at Nordea Liv i forbindelse med overtagelse av ansvaret for IKT-driften vil foreta opplæring av de ulike rolleinnehavere med utgangspunkt i fastsatte rollebeskrivelser. Finanstilsynet registrerer at styret vurderer at dette vil sikre en styringsdyktig operasjonalisering av og kontroll over skytjenester.

Finanstilsynet tar styrets svar til etterretning.

5 Prosjektstyring – anskaffelse og utvikling

IKT-forskriften § 2 og § 6 stiller krav til prosjektstyring ved IKT-utvikling og -anskaffelser. Dette er ytterligere utdypet i EIOPA GL on ICT retningslinje 16, 17 og 18.

5.1 Prosjektstyring i kjernesystemprosjektet ved eventuelle forsinkelser

I tilsynsmøtet framkom det at Nordea Liv ikke har foretatt en nærmere vurdering av usikkerhet knyttet til utviklingsaktiviteter som kan ha stor konsekvens for framdriften i kjernesystemprosjektet.

Det er Finanstilsynets erfaring at forsinkelser i sentrale leveranser i IKT-prosjekter kan medføre omfattende konsekvenser for ferdigstilling av totalprosjektet. Når tre eksisterende kjernesystemer skal samles til ett, vil forsinkelser i utviklingen av felles funksjonalitet ha enda større konsekvenser.

I foreløpig rapport var det Finanstilsynet forventning at Nordea Liv har en aktiv oppfølging av utviklingsaktiviteter som kan skape forsinkelser, inkludert løpende konsekvens- og risikovurderinger og tiltaksplaner for å håndtere dette, slik at ledelse og styre til enhver tid har oversikt over framdrift og hvilke konsekvenser eventuelle forsinkelser medfører.

Av styrets svar framgår det at styret deler Finanstilsynets observasjon og at styret vurderer at kjernesystemprosjektet har ivaretatt Finanstilsynets forventninger. Fra styrets svar har Finanstilsynet notert seg at styret oppfatter kjernesystemprosjektet som omfattende, og at dette vil fordre en stram prosjektstyring der kravene til leveranser fra kjernesystemprosjektet kommer i tillegg til å sikre den løpende virksomheten. For styring av prosjektet benytter Nordea Liv seg av kjente rammeverk og verktøy, der det er etablert et veikart med tilhørende detaljerte planer for å ha oversikt over hovedutviklingsaktiviteter og avhengigheter. Fra styrets svar oppfatter Finanstilsynet at styret vurderer at veikartet med tilhørende detaljerte planer vil gi prosjektet oversikt ved eventuelle forsinkelser, konsekvenser av forsinkelser og at prosjektet på dette grunnlaget vil kunne iverksette nødvendige tiltak. Det framgår videre av styrets svar at det vil gjennomføres risikoanalyser for hele prosjektet og i de ulike fasene av prosjektet, der risiko for forsinkelser og tiltak vil følges opp løpende. I forbindelse med gjennomføringsfasen vil det, som del av den initielle analysen og faseplanleggingen, gjennomføres en nærmere vurdering av usikkerhet knyttet til utviklingsaktiviteter, noe som er i henhold til prosjektets overordnede framdrifts- og risikostyringsplaner.

Finanstilsynet tar styrets redegjørelse til etterretning.

5.2 Nøkkelpersonrisiko

I tilsynsmøtet og fra tilsendt dokumentasjon framkom det at Nordea Liv har nøkkelpersonrisiko knyttet til gammel teknologi, og at det er utfordrende å få ansatt kompetent personell. Nordea Liv har personell i organisasjonen med kjennskap til de gamle systemene som er ansatt i andre områder i organisasjonen.

I foreløpig rapport vurderte Finanstilsynet at utfordringene med nøkkelpersonrisiko kan søkes løst ved å inngå avtaler med allerede ansatte og gjennom dette sikre Nordea Liv nødvendig forutsigbarhet. Ved inngåelse av slike avtaler bør foretaket inkludere bestemmelser som håndterer eventuelle forsinkelser. Fra styrets svar har Finanstilsynet notert seg at styret anser det som hensiktsmessig å inngå slike avtaler. Videre framgår det av styrets svar at slike avtaler vil vurderes fortløpende for nøkkelroller og at Nordea Liv har iverksatt flere tiltak for å redusere risiko knyttet

til nøkkelpersonkompetanse, herunder dokumentering og kompetanseoverføring samt forenkling og automatisering av manuelle rutiner.

Finanstilsynet tar styrets kommentar til etterretning.

5.3 Lisenser og leverandørstøtte på eksisterende systemer ifm. ny kjerneløsning

I foreløpig rapport var det Finanstilsynet forventning at Nordea Liv vurderer konsekvensen av mulige forsinkelser i sin prosjektstyring, der eventuell IKT-risiko, økonomiske konsekvenser av kostnader til lisenser og utfordringer knyttet til IKT-drift blir klarlagt. I en slik avklaring vil forhold knyttet til eventuelt opphør av støtte fra system- og driftsleverandører inngå, da dette vil kunne påvirke gjennomføringen av kjernesystemprosjektet.

Fra styrets svar har Finanstilsynet notert seg at to av tre kjernesystemer er egenutviklet uten lisens. For det tredje kjernesystemet er det nylig inngått avtale om forlengelse av lisens, der Nordea Liv har leverandørstøtte på inntil 7 år. Det framgår videre fra styrets svar at økonomiske konsekvenser av forsinkelser knyttet til de tre eksisterende systemene er hensyntatt i de finansielle vurderingene.

Finanstilsynet forutsetter at Nordea Liv i sine vurderinger av behov for leverandørstøtte ved eventuelle forsinkelser også har vurdert sårbarheter i plattform og infrastruktur for kjernesystemene, inkludert de omkringliggende systemene som har avhengigheter til kjernesystemene. Eksempler på omkringliggende systemer er arbeidsflytverktøy, løsninger for elektronisk arkiv, integrasjon mot regnskapssystem, utbetalingssystem med flere.

Finanstilsynet tar styrets svar til etterretning.

5.4 Konsekvenser for drift av eksisterende systemer ifm. ny kjerneløsning

I foreløpig rapport påpekte Finanstilsynet at Nordea Liv må ta hensyn til konsekvensene som eventuelle forsinkelser i kjernesystemprosjektet vil kunne ha for avtaler om fortsatt IKT-drift for de tre eksisterende kjernesystemene.

Fra styrets svar framgår det at de tre eksisterende kjernesystemene driftes på intern infrastruktur i Nordea-konsernets datasenter og at relevant infrastruktur vil være tilgjengelig også ved eventuelle forsinkelser i prosjekt for nytt kjernesystem. Styret peker videre på at avtale om eksterne IKT-driftstjenester knyttet til applikasjonsdrift er fornyet for ett av systemene med mulighet for 7 års varighet, mens IKT-driftstjenester for de to andre kjernesystemene ivaretas av interne ressurser i Nordea Liv, med støtte fra innleide konsulenter fra en ekstern IKT-tjenesteleverandør. Fra styrets svar har Finanstilsynet notert seg at Nordea Liv har løpende fokus på å ha nødvendig kompetanse tilgjengelig på de tre eksisterende kjernesystemene.

Finanstilsynet tar styrets svar til etterretning.

5.5 Konvertering og oppslag i historiske data

I tilsynsmøtet framkom det at det foreløpig ikke foreligger en konverteringsstrategi. Basert på Finanstilsynets erfaring vil det være ulike strategier som er aktuelle for konvertering. Det kan eksempelvis være at deler av data/historikk velges å utelates for å redusere omfanget og kompleksiteten av konverteringen. Erfaringene er at det i de fleste tilfeller vil være behov for

oppslag i gamle data etter at konvertering er gjennomført, enten utfra kontroll-/revisjonsbehov eller for å se hvordan data var lagret for å kunne rydde opp i eventuelle feil som har skjedd i konverteringen.

I foreløpig rapport viste Finanstilsynets til erfaring om at oppslagsmulighet/historikk med utgangspunkt i eksisterende systemløsning vil kunne kreve lisens fra tidligere systemleverandør. Kostnaden for slik lisens vil kunne påvirke valg av konverteringsstrategi. Andre momenter som kan påvirke valg av konverteringsstrategi er systemleverandørens plan for videre støtte til systemet. Et annet alternativ er å utvikle en egen systemløsning med oppslag mot dataene slik de ligger lagret i de eksisterende systemene. Det var Finanstilsynets vurdering at fastsettelse av konverteringsstrategi bør skje tidlig i prosjektplanleggingen slik at Nordea Liv har kontroll med risikoen knyttet til løsning for tilgang til historiske data.

Fra styrets svar har Finanstilsynets notert seg at styret vurderer at risiko knyttet til løsning for tilgang til historiske data får tilstrekkelig fokus i prosjektarbeidet, da prosjektets tilnærming er å konvertere alle historiske data til nytt system, slik at tilgang til de gamle systemene ikke lenger vil være nødvendig for historiske oppslag. Videre har Finanstilsynet notert seg at konverteringstilnærming og -strategi vil bli besluttet individuelt for hvert av de tre kjernesystemene. Prosjektet vil følge både interne krav (Nordea Liv og Nordea-konsernet) og lovkrav for oppbevaring og oppslag av data.

Finanstilsynet tar styrets svar til etterretning.

6 IKT-tilgjengelighet og -kontinuitet (inkl. IKT-drift og beredskap)

Foretaket har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11. EIOPA GL on ICT utdyper IKT-forskriftens bestemmelse for hvordan foretak skal sikre forretningsmessig kontinuitet basert på forretningsmessige konsekvensanalyser (BIA[3]). Videre gir den anbefaling om utarbeidelse av kontinuitets-, respons-, kommunikasjons- og gjenopprettingslaner ved kriser samt hvordan testing skal foregå.

Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i en BIA for foretakets kritiske forretningsprosesser. En BIA skal sikre at Nordea Livs beredskaps- og kontinuitetsplaner blir fastsatt med utgangspunkt i forretningsmessige kritikalitet. En BIA gir også føringer for prioritering av rekkefølgen for gjenoppretting av IKT-systemer/tjenester. For å verifisere at det er etablert fungerende planer og løsninger må det foretas regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11 tredje ledd.

6.1 Årlig BIA og forretningsmessige kontinuitetsplan (BCP[4])

I foreløpig rapport var det Finanstilsynets vurdering at Nordea Liv sin BIA burde være mer detaljert. Finanstilsynet forventer at samtlige IKT-systemer/-tjenester som inngår i utførelsen av de enkelte kritiske forretningsprosessene er inkludert, slik at tilgjengelighets- og beskyttelseskravene hensyntar helheten.

[3] BIA – Business Impact Analysis
[4] BCP - Business Continuity Plan

Fra styrets svar har Finanstilsynet notert seg at Nordea Liv årlig gjennomfører BIA og oppdaterer BCP basert på dette. Det framgår videre fra styrets svar at siste oppdatering av den forretningsmessige kontinuitetsplanen ble gjennomført i 2. kvartal 2023, og at styret mener at de gjennomførte forretningsmessige konsekvensanalysene er tilfredsstillende.

Finanstilsynet forutsetter at avhengigheter til omkringliggende systemer, tjenester og komponenter, slik som eksempelvis arbeidsflytverktøy, elektronisk arkiv, integrasjon mot regnskapssystem, utbetalingssystem med flere er vurdert og hensyntatt i de forretningsmessige kontinuitetskravene når styret vurderer analysen som tilfredsstillende.

Finanstilsynet tar styrets svar til informasjon.

6.2 Test av BCP

I tilsynsmøtet var det Finanstilsynets forståelse at det ikke var fastsatt faste øvelser der Nordea Liv får testet samhandling og de etablerte kontinuitets- og beredskapsløsningene. I foreløpig rapport var det Finanstilsynets vurdering at testingen bør inkludere relevante scenarier knyttet til de kritiske og viktige forretningsprosessene, som definert i foretakets BIA, der også leverandører (og eventuelle underleverandører) av utkontraktert IKT-virksomhet inngår.

Av styrets svar framgår det at Nordea Livs BCP revideres og testes årlig. Det framgår videre fra styrets svar at det er fastsatt årlige øvelser der samhandling testes, basert på et eller flere av de obligatoriske scenarioene som er nedfelt i beredskapsplanen, og det er krav om at en eller flere av de kritiske forretningsprosessene identifisert i BIA skal testes. Det framgår videre fra styrets svar at det gjennomføres årlige krisegjenopprettingstester (Disaster Recovery test (DR)) med interne og eksterne leverandører. Siden alle de tre kjernesystemer fra og med år 2023 driftes av IKT-konsern så vil framtidig DR/failovertest foregå i samhandling med IKT-konsern. I 2024 er det planlagt å gjennomføre en simuleringstest for å teste nødløsningene basert på krav om at dette skal utføres hvert tredje år.

Fra styrets svar har Finanstilsynet notert seg at styret er enig med Finanstilsynet om at leverandører av utkontraktert virksomhet i større grad kan involveres i testing, og at Nordea Liv vil oppdatere sitt testregime tilsvarende. Det framgår videre at styret vurderer at Nordea Liv oppfyller kravene i IKT-forskriften for årlig testing av fastsatte beredskapsplaner.

Finanstilsynet tar styrets svar til etterretning.

7 Dataintegritet

IKT-forskriften § 4 stiller krav til at det skal fastsettes kvalitetsmål for de enkelte deler av IKT-virksomheten knyttet opp mot foretakets øvrige mål. Foretaket skal videre ha dokumenterte prosedyrer for oppfølging av de fastsatte kvalitetsmålene. Ytterligere utdypninger av temaet styring og kontroll med data (data governance) og dataintegritet framgår av EIOPA GL on ICT. Dataintegritet ses i sammenheng med konfidensialitet og tilgjengelighet i disse retningslinjene, og er omhandlet i retningslinje nummer 4, 6, 10, 11, 17, 21 og 22.

Basert på mottatt dokumentasjon og informasjon i tilsynsmøtet var det i foreløpig rapport Finanstilsynets oppfatning at Nordea Liv er i en tidlig fase i arbeidet med dataintegritet og styring

og kontroll av data. Det var videre Finanstilsynets oppfatning at utover at L&P Gruppen har fastsatt "Life & Pensjons Data Governance Operating Model", så er Nordea-konsernets gjeldende rammeverk for data governance i liten grad operasjonalisert i Nordea Liv. Videre var det Finanstilsynets vurdering at arbeidet med dataintegritet og datakvalitet utgjør et viktig fundament, som er særskilt viktig for IKT-løsninger og -systemer der automatisert beslutningsstøtte og detaljert rapportering inngår. Utfra Nordea Liv sin strategiske ambisjon om satsning på selvbetjening og automatisering vurderte Finanstilsynet i foreløpig rapport at arbeidet med dataintegritet og styring og kontroll med data bør intensiveres.

Av styrets svar har Finanstilsynet notert seg at det er enig i at arbeidet med dataintegritet samt styring og kontroll med data, bør intensiveres. Fra styrets svar har Finanstilsynet videre notert seg at temaet dataintegritet samt styring og kontroll av data allerede er identifisert som et risikoområde i forbindelse med Nordea Liv sin årlige IKT-risikovurdering, og at det er iverksatt tiltak. Blant tiltakene inngår en strategisk forankring av arbeidet med styring og kontroll av data i IKT-strategien, da Nordea Liv skal bli et mer datadrevet foretak. Videre framgår det at Nordea Liv høsten 2023 også har iverksatt tiltak for å etablere tydeligere prinsipper for styring og kontroll med data. Finanstilsynet registrerer at disse prinsippene skal definere kravene til de ulike involverte rollene og hvordan etterlevelse skal sikres. Dette vil komme i form av lokale instruksjoner som tar Nordea-konsernets overordnede rammeverk ned til en effektiv lokal implementering i Nordea Liv. Frist for ferdigstillelse er første halvår 2024. Styret opplyser at når prinsippene er etablert vil rollene bemannes og nødvendig opplæring vil bli gitt.

Finanstilsynet tar styrets svar til etterretning.

***

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet. Kopi av tilsynsrapporten bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Jarleif Lødøen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.