Redegørelse om funktionsinspektion af IT-risikostyring i Lærernes Pension, forsikringsaktieselskab

Finanstilsynet var i februar 2023 på funktionsinspektion i Lærernes Pension, forsikringsaktieselskab (herefter selskabet eller Lærernes Pension).

Inspektionen omhandlede selskabets IT-risikostyring. Undersøgelsen tog udgangspunkt i selskabets indsendte materiale og rapporteringer til Finanstilsynet.

Sammenfatning og risikovurdering

Lærernes Pension administrerer pensionsordninger for ca. 158.000 lærere. Selskabet outsourcer en stor del af sin IT til Forca.

Selskabets forretningsmodel indebærer omfattende anvendelse af IT, hvilket medfører en række iboende IT-risici.

Selskabets IT-ansvarlige i 1. forsvarslinje er selskabets økonomidirektør. Herudover har selskabet etableret en risikostyringsfunktion, som er forankret i risikostyringsafdelingen. og placeret i 2. forsvarslinje

IT-risikostyring
Generelt vurderer Finanstilsynet, at IT-risici er et væsentligt risikoområde for Lærernes Pension Bestyrelsen skal derfor fastsætte, hvilke og hvor store IT-risici selskabet må påtage sig samt aktivt tage stilling til strategiske mål for IT-risici.

Samlet set vurderer Finanstilsynet, at der er en risiko for, at selskabet påtager sig IT-risici, som ikke er i overensstemmelse med bestyrelsens risikoappetit.

Finanstilsynet konstaterede, at bestyrelsen ikke har fastsat tilstrækkelige risikotolerancegrænser for IT-risici. Finanstilsynet har derfor påbudt selskabet at sikre, at bestyrelsen fastsætter, hvilke og hvor store IT-risici selskabet må påtage sig, og specificere risikotolerancegrænser for IT-risici, som udgør kontrollerbare grænser for størrelsen af acceptable IT-risici.

Finanstilsynet vurderer, at forsikringsselskaber løbende bør sammenholde deres faktiske risikoprofil med den ønskede risikoprofil, udtrykt ved bestyrelsens risikotolerancegrænser, med henblik på at give bestyrelsen et billede af, hvor selskabet eventuelt ligger udenfor bestyrelsens ønskede niveau for IT-risici. Finanstilsynet konstaterede, at selskabet ikke havde fastlagt den faktiske risikoprofil, hvorfor selskabet er blevet påbudt at fastlægge selskabets risikoprofil for IT-risici.

Selskabet havde ikke fastsat en klar metode for IT-risikostyring eller for hvordan IT-risici, som selskabet er eller kan blive udsat for, skal vurderes. Finanstilsynet forventer, at selskaber sikrer en egen identifikation og vurdering af risici, når de anvender outsourcing. Vurderingen skal blandt andet indeholde stillingtagen til risikoen for ufuldstændig eller mangelfuld vurdering af IT-risici hos outsourcingleverandører. Selskabet er blevet påbudt at fastsætte principper for opgørelsen og måling af IT-risici samt at have effektive procedurer, der kan sikre tilstrækkelig identifikation og vurdering af IT-risici.

Endeligt vurderede Finanstilsynet, at der ikke var tilstrækkelig fokus på IT-risici i risikostyringsfunktionen. Risikostyringsfunktionen har en vigtig opgave i at understøtte risikostyringssystemet ved bl.a. at sikre, at alle væsentlige risici bliver identificeret, målt, overvåget, styret og rapporteret korrekt. Finanstilsynet har derfor påbudt selskabet at sikre, at risikostyringsfunktionen i tilstrækkeligt omfang inddrager og vurderer IT-risikostyring i funktionens opgavevaretagelse og rapportering.