Redegørelse om funktionsinspektion af IT-risikostyring i Velliv, Pension & Livsforsikring A/S

Finanstilsynet var februar 2024 på funktionsinspektion i Velliv, Pension & Livsforsikring A/S (Velliv eller selskabet). Inspektionen omhandlede selskabets IT-risikostyring. Inspektionen tog udgangspunkt i selskabets indsendte materiale og rapporteringer til Finanstilsynet.

Sammenfatning og risikovurdering

Velliv er et kommercielt livsforsikringsselskab med ca. 420.000 kunder. Selskabets forretningsmodel indebærer omfattende anvendelse af IT, hvilket medfører en række IT-risici. Selskabet har organiseret sig efter principperne med tre forsvarslinjer, hvor første forsvarslinje bl.a. udgøres af selskabets IT-sikkerhedschef (CISO). CISO har ansvaret for at foretage regelmæssige IT-risikovurderinger. Risikostyringsfunktionen i anden forsvarslinje overvåger risikostyringssystemet, herunder IT-risici.

IT-risikostyring

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

Finanstilsynet konstaterede, at selskabet har arbejdet med IT-risici og også foretager risikovurderinger på området, samt overordnet set har fastsat en metode for blandt andet IT-risikostyring. Det er dog Finanstilsynets vurdering, at området skal styrkes yderligere.

Finanstilsynet vurderede, at bestyrelsen ikke har fastsat tilstrækkelige risikotolerancegrænser for IT-risici. De fastsatte risikotolerancegrænser indeholder ikke objektive målepunkter. Mangelfulde risikotolerancegrænser medfører, at der ikke kan ske tilstrækkelig styring af IT-risici. Konkret betyder det, at selskabets faktiske risikoprofil ikke kan sammenholdes med den ønskede. Finanstilsynet har derfor påbudt bestyrelsen at fastsætte, hvilke og hvor store IT-risici selskabet må påtage sig, samt at specificere risikotolerancegrænser for IT-risici[1].

Derudover har bestyrelsen ikke i tilstrækkelig grad fastsat en metode for IT-risikostyring og måling af IT-risiko. Det gælder f.eks. metoden for at komme fra en vurdering af sandsynlighed og konsekvens til en samlet risikoscore. Det indebærer en risiko for, at risikoprofilen vurderes med usammenlignelige metoder fra år til år, og at bestyrelsen ikke opnår et retvisende billede af det aktuelle risikoniveau i forhold til bestyrelsens ønskede risikoappetit. Finanstilsynet har derfor påbudt bestyrelsen at fastsætte klare principper for opgørelse og måling af IT-risici[2].

[1] § 95, stk. 1, nr. 2 og 3, i lov om forsikringsvirksomhed samt § 8, stk. 1, nr. 1, og bilag 6, nr. 2, litra d, i bekendtgørelse om ledelse og styring af forsikringsselskaber m.v.

[2] § 95, stk. 2, nr. 2, i lov om forsikringsvirksomhed bilag 6, nr. 2, litra a, i bekendtgørelse om ledelse og styring af forsikringsselskaber m.v.