FINANSTILSYNET

Finanstilsynet

28. juni 2024

Redegørelse om funktionsinspektion af IT-risikostyring i AkademikerPension

Finanstilsynet var i januar og februar 2024 på funktionsinspektion i AkademikerPension.

Inspektionen omhandlede virksomhedens IT-risikostyring samt overgang til nyt kernesystem. Undersøgelsen tog udgangspunkt i virksomhedens indsendte materiale og rapporteringer til Finanstilsynet.

Sammenfatning og risikovurdering

AkademikerPension er en medlemsejet pensionskasse, der administrerer pensionsordninger for ca. 170.000 akademikere.

Virksomhedens forretningsmodel indebærer omfattende anvendelse af IT, hvilket medfører en række iboende IT-risici. Virksomheden har organiseret sig efter principperne med tre forsvarslinjer, hvor første forsvarslinje er afdelingscheferne, f.eks. under Investering og Økonomi, mens anden forsvarslinje udgøres af risikostyringsfunktionen.

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

Finanstilsynet konstaterede, at pensionskassen 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 konstaterede, at pensionskassen ikke har sikret tilstrækkelig forankring af de anvendte risikotolerancegrænser for IT-risici i bestyrelsen. Risikotolerancegrænser er et vigtigt element i forhold til at sikre, at admini-

strationens håndtering af IT-risici sker i overensstemmelse med bestyrelsens anvisninger. Finanstilsynet har derfor påbudt bestyrelsen at fastsætte, hvilke og hvor store IT-risici pensionskassen må påtage sig, samt at specificere risikotolerancegrænser for IT-risici[1].

Finanstilsynet konstaterede desuden, at politik eller retningslinjer ikke i tilstrækkelig grad angiver principperne for opgørelse eller måling af IT-risici, og at principperne derfor ikke er tilstrækkelig forankret i bestyrelsen. Der er dermed risiko for, at pensionskassen ikke styrer og måler sine IT-risici i tilstrækkelig grad i overensstemmelse med bestyrelsens beslutninger. Finanstilsynet har derfor påbudt bestyrelsen at fastsætte klare principper for opgørelse og måling af IT-risici[2].

Derudover konstaterede Finanstilsynet, at pensionskassen i forbindelse med skift af kernesystem har oplevet og fortsat oplever en række forskelligartede drifts- og dataudfordringer, der indebærer og nødvendiggør manuelle processer og kontroller. Finanstilsynet vurderer, at omfanget af de manuelle processer og kontroller på de konkrete områder, herunder aktuarområdet, udgør en forhøjet risiko i forhold til at sikre en effektiv understøttelse af virksomhedens drift, herunder aktuardrift, med en deraf afledt forhøjet risiko for virksomhedens varetagelse af sine forpligtelser. Det har givet anledning til en risikooplysning.

[1] § 95 i lov om forsikringsvirksomhed samt § 5, stk. 1, § 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. 72, i lov om forsikringsvirksomhed samt § 7, stk. 3, nr. 5, § 8, stk. 1, nr. 2, og bilag 6, nr. 2, litra a, i bekendtgørelse om ledelse og styring af forsikringsselskaber m.v.