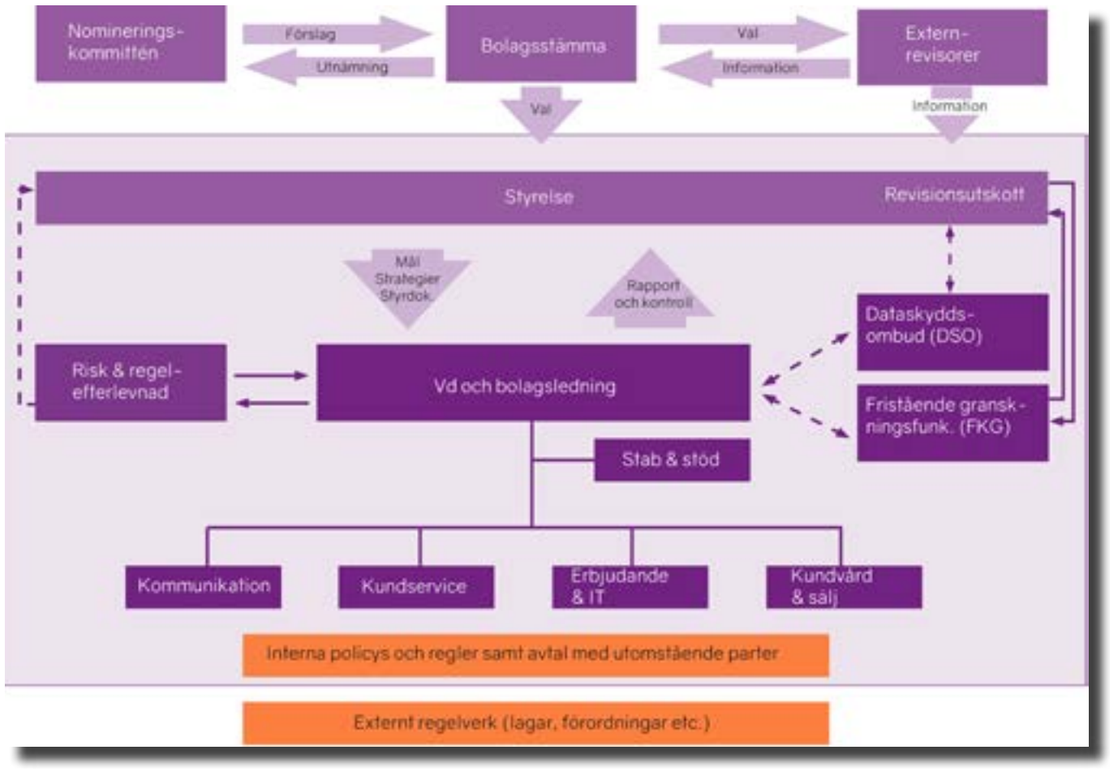
minPension

Förenklad bolagsstyrningsrapport för 2021

Innehåll

minPension

minPensions bolagsstyrningsstruktur



1 Inledning

Sedan 2004 bedrivs ett framgångsrikt samarbete mellan staten och försäkringsbranschen (privat-offentlig samverkan) kring individernas pensionsinformation[1] inom ramen för Min Pension i Sverige AB (minPension). minPension utvecklar och förvaltar webbplatsen minPension.se. Till skillnad från de flesta andra leverantörer av pensionsinformationstjänster är minPension en oberoende och neutral aktör[2]. De tjänster som tillhandahålls av minPension är dessutom kostnadsfria för pensionsspararna att använda.

Bolagets övergripande mål är att så många pensionssparare som möjligt ska använda tjänsterna på minPension.se med lämplig regelbundenhet för att få en samlad bild av sin intjänade/insparade pension och för att göra pensionsprognoser. På så sätt kan de bilda sig en uppfattning om vad de kan förvänta sig i pension och vad som påverkar pensionens storlek. Därutöver ska merparten av de individer som går i pension ha använt tjänsten Uttagsplaneraren och uppleva att det är tryggt och enkelt att planera uttag av sin pension med hjälp av tjänsten.

minPension har anslutningsavtal med de pensionsaktörer som levererar pensionsinformationen till tjänsterna (anslutna aktörer) och användarvillkor med de pensionssparare som har registrerat sig på minPension.se (användare) samt tillhörande dokumentation om hur minPension behandlar personuppgifter. Anslutningsavtal och användarvillkor i kombination fungerar som fullmakter för inhämtning och behandling av pensionsinformationen.

1.1 Rapporten

minPension förelägger årligen en s.k. förenklad bolagsstyrningsrapport för styrelsen i samband med årsredovisningen. Rapporten har utarbetats enligt de principer som gäller för svensk kod för bolagsstyrning utgiven av Kollegiet för svensk bolagsstyrning och minPension ska följa koden i tillämpliga delar. Rapporten ingår inte i årsredovisningen och har därför

1 Se antologin ”Min Pension – ett exempel på privat-offentlig samverkan” av Katrin Westling Palm och Christina Lindenius (2017)

2 minPension är en neutral och oberoende aktör med huvudfokus på pensionsspararnas behov. minPension bygger på ett frivilligt samarbete mellan staten och branschen och agerar därför inte på uppdrag av enskilda aktörer och har heller inget vinstintresse. Finansieringen av verksamheten sker gemensamt av staten och branschen.

minPension

inte granskats av externrevisionen. Rapporten har däremot delats till revisorerna för synpunkter. De synpunkter som har framförts har beaktats.

2 minPensions bolagsstyrning

minPension är ett helägt dotterbolag till SFS-Svensk Försäkring Service AB, som är ett helägt dotterbolag till försäkringsföretagens branschorganisation Svensk Försäkring. Verksamheten bedrivs i ett samarbete mellan staten och försäkringsbranschen vilket regleras genom ett konsortialavtal (nedan ”samverkansavtal”). Enligt villkoren i detta avtal svarar staten via Pensionsmyndigheten och Statens tjänstepensionsverk (SPV) för finansieringen av den ena halvan av de årliga driftskostnaderna för minPension. För finansieringen av den andra halvan svarar dels de medlemsbolag hos Svensk Försäkring som bedriver verksamhet inom liv- och pensionsområdet, dels vissa övriga anslutna pensionsaktörer som levererar pensionsinformation till minPension[3]. Utöver detta har minPension bedrivit två sidofinansierade projekt under 2021, nämligen ”pensionssäsongssatsningen” motsv. 218 tusen kronor samt Elektroniska flyttblad motsv. 425 tusen kronor[4].

2.1 Bolagsstämman

Bolagsstämman är minPensions högsta beslutande organ. Bolagets årliga ordinarie bolagsstämma hålls vanligtvis i april. Vid bolagsstämman lägger styrelsen fram årsredovisningen som enligt årsredovisningslagen (1995:1554) ska innehålla balans- och resultaträkning, noter och förvaltningsberättelse samt en revisionsberättelse. Stämman beslutar om fastställelse av resultat- och balansräkning, resultatdisposition och ansvarsfrihet gentemot bolaget för styrelseledamöter och den verkställande direktören. Bolagsstämman beslutar också arvode till styrelsen och revisorer.

3 Länk till förteckning över de ca 30 aktörer som är anslutna till minPension https://www.minpension.se/kontakta-pensionsbolag

4 Pensionssäsongssatsningen regleras i ett särskilt avtal mellan minPension och Pensionsmyndigheten. Beträffande finansiering m.m. beslutas det av Svensk Försäkrings styrelse.

2.2 Styrelsen

minPensions styrelse ansvarar för bolagets organisation och förvaltningen av bolagets angelägenheter. Styrelsen ska tillse att den har erforderlig kännedom om bolagets angelägenheter, ställning samt övriga förhållanden av betydelse för verksamheten. Styrelsens arbete regleras i en särskild arbetsordning. Arbetsfördelningen mellan å ena sidan styrelsen och å andra sidan den verkställande direktören finns dokumenterad i en vd-instruktion.

Styrelsen består av tre ledamöter från pensionsbranschen, två ledamöter från Pensionsmyndigheten och en ledamot från SPV. Detta framgår av det samverkansavtal som träffades 2005 mellan pensionsbranschen och staten om inrättandet av Min Pension i Sverige AB[5]. minPensions styrelseordförande är Svensk Försäkrings verkställande direktör. Sedan Pensionsmyndigheten bildades 2010 är myndighetens generaldirektör ordinarie ledamot i styrelsen. Även SPV:s generaldirektör är ordinarie ledamot. Varje ledamot har en suppleant. Styrelsens ledamöter och suppleanter ingår inte i minPensions bolagsledning.

Förfarandet när det gäller tillsättandet av ordförande samt ledamöter från pensionsbranschen går till på följande sätt. Svensk Försäkrings styrelse har för ändamålet tillsatt en nomineringskommitté. I arbetet tillämpas en rotationsprincip genom att en ordinarie ledamot lämnar styrelsen varje år. Kontinuiteten uppnås genom att en suppleant i stället väljs in som ordinarie ledamot. Det innebär normalt en sammanlagd mandatperiod om fyra år.

Nomineringskommittén har i sitt arbete att utgå från ett principdokument fastställt av Svensk Försäkrings styrelse där det framgår att bolagets styrelse ska ha en god sammantagen kompetens, mångfald och branschrepresentation samt att varje ledamot ska ha en tillräckligt hög nivå för att självständigt kunna fatta beslut av strategisk vikt för minPension. Nomineringskommittén föreslår även ett val av ordförande. För att säkerställa en tydlig koppling mellan behandlingen av frågor rörande minPension i Svensk Försäkrings styrelse och styrningen av bolaget har det bedömts som lämpligt att det är den verkställande direktören för Svensk Försäkring som innehar ordförandeposten i minPensions styrelse. Bolagsstämman beslutar därefter om val av ledamöter till styrelsen.

5 Detta avtal har reviderats tre gånger, nämligen 2010, 2020 samt 2021.

minPension

Den 15 april 2021 valdes följande styrelse

Ordförande: Christina Lindenius (Svensk Försäkring)

Ordinarie ledamöter: Daniel Barr (Pensionsmyndigheten), Maria Humla (SPV), Anna-Karin Laurell (Folksam), Carl-Magnus Löfström (Pensionsmyndigheten) samt Katarina Thorslund (Alecta).

Suppleanter: Elin Berglöf (Pensionsmyndigheten), Johan Bergsten (SPV), Mats Galvenius (Svensk Försäkring), Pär Hedén (Pensionsmyndigheten), Peter Salomon-Sörensen (Swedbank) samt Anna-Carin Söderblom Agius (Skandia).

En extra bolagsstämma genomfördes den 21 juni 2021 då stämman beslutade ett förslag till reviderad bolagsordning (se nedan).

Styrelsen håller ett konstituerande sammanträde i nära anslutning till bolagsstämman. Vid det konstituerande styrelsemötet väljs styrelseordförande till nästkommande konstituerande styrelsesammanträde.

Därutöver ska styrelsen hålla minst fyra sammanträden per år, lämpligt fördelade över året enligt styrelsens arbetsordning. Vid behov hålls extra sammanträden. Styrelsen har under 2021 hållit sex sammanträden.

Styrelsen har sedan några år tillbaka ett ökat fokus på den strategiska styrningen av minPensions långsiktiga inriktning och utveckling. Ett exempel på detta är den årligt återkommande strategidagen som genomförs på hösten med styrelsen. Strategidagen syftar till att ge styrelsen tillräckligt med tid för att kunna föra fördjupade strategiska diskussioner som normalt inte ryms vid de ordinarie styrelsesammanträdena.

Ett annat exempel är de gemensamma seminarier med ledamöter från Svensk Försäkrings styrelse (livbolagen) och branschrepresentanterna i minPensions styrelse som genomfördes för några år sedan. Ett viktigt syfte med seminarierna har varit att uppnå en bred samsyn om minPensions framtida inriktning och utveckling samt att så konkret som möjligt formulera rekommendationer till minPensions styrelse som sedan kunnat utgöra ett viktigt underlag i bolagets verksamhetsplanering m.m. Syftet och målet med seminarierna har uppnåtts på ett bra sätt och resultaten från seminarierna finns tydligt dokumenterade i s.k. slutdokument.

Nedan sammanfattas viktiga ärenden och frågeställningar som minPensions styrelse har arbetat med under 2021.

Inom utvecklingsområdet har styrelsens fokus legat på det fortsatta arbetet med att vidareutveckla den strategiska tjänsten Uttagsplaneraren som har varit i drift sedan hösten 2019. Uttagsplaneraren är en av de viktigaste tjänsterna som minPension tillhandahåller pensionsspararna. Avsevärda resurser har hittills lagts ner och kommer även fortsättningsvis att läggas ner på vidareutveckling och förvaltning av tjänsten under de närmaste åren. Av detta skäl har styrelsen bl.a. beslutat en plan för de kommande årens (2022–2024) utvecklingsarbete med Uttagsplaneraren (främst med fokus på tillkommande funktionalitet ur ett användarperspektiv) samt en uppdaterad anslutningsplan avseende MisLife 2.0, Pensioner under utbetalning samt tilläggstjänsterna Överföra plan, Beräkningsmodell 2 och Beräkningsmodell 3.

Ytterligare berednings- och utredningsarbete har varit nödvändigt under året när det gäller projektet som arbetar med att införa tjänsten Elektroniska flyttblad, vars driftsättning har blivit försenad till följd av detta. Planen är nu att driftsättning ska ske under andra halvan av 2022.

Styrelsen är strategisk styrgrupp för såväl Uttagsplaneraren som Elektroniska flyttblad.

Under året har styrelsen behandlat frågan om hur minPension bättre ska kunna nå ut till pensionssparare med lågt intresse och låg kunskap om sin framtida pension och få dem att använda tjänsterna på minPension i högre utsträckning. Ett problem som har uppmärksammats är att individer i denna grupp, som trots allt loggar in på minPension, alltför ofta inte fullföljer hela processen med att skapa prognoser/uttagsplaner.

Styrelsen har arbetat vidare med den komplicerade frågan om förutsättningar och möjligheter att tillskapa funktionalitet för att ge användarna möjlighet att se hur pass hållbart deras pensionstillgångar är placerade på minPension.se. Ur ett bolagsstyrningsperspektiv kan det dessutom konstateras att införandet av en tjänst som redovisar pensionstillgångarna ur ett hållbarhetsperspektiv för användarna även förutsätter att minPensions uppdrag utökas formellt till att omfatta detta.

För minPension har länge funnits en tydligt kommunicerad beskrivning av bolaget som ett ”icke vinstdrivande företag”, vilket indikerar att bolaget också är ett icke vinstutdelande aktiebolag. Något uttryckligt förbud mot

minPension

vinstutdelning eller särreglering kring hantering av överskott har dock inte funnits i vare sig bolagsordningen eller samverkansavtalet. Av detta skäl tog minPensions styrelse initiativ till en översyn för att skapa ökad tydlighet kring hanteringen av överskott och vinstutdelningsbegränsningar. Översynen har bl.a. resulterat i en justering av bolagsordningen så att det har tagits in uttryckliga vinstutdelningsbegränsningar. Den reviderade bolagsordningen beslutades på en extra bolagsstämma den 21 juni. Styrelsen har även låtit genomföra en översyn av bolagets finansieringsmodell. Det framkom även ett behov av att göra vissa förtydliganden i den reglering kring finansieringsmodellen som finns i det anslutningsavtal som reglerar samverkan kring tjänsterna på minPension med de anslutna aktörerna. Det reviderade anslutningsavtalet beslutades av styrelsen i juni 2021. Med anledning av justeringarna i såväl bolagsordning som finansieringsmodell beslutades i juni 2021 även korresponderande justeringar i samverkansavtalet.

Verksamheten vid minPension växer snabbt och befinner sig i en intensiv utvecklingsfas. För att kunna möta denna utveckling på ett effektivt och säkert sätt har styrelsen, genom revisionsutskottet, beslutat att minPension ska implementera en ny och vidareutvecklad IT-sourcingstrategi. Ett relativt omfattande och genomgripande implementeringsarbete har därför genomförts under året. Den nya strategin ska vara implementerad före utgången av 2025.

Därutöver har styrelsen omnämnt betydelsen av att vidareutveckla modeller och arbetssätt genom s.k. dimensionerande antaganden som stärker den långsiktiga planeringen och uppskattningarna av den långsiktiga kostnadsutvecklingen. Dessa sträcker sig ca fem år framåt i tiden och omfattar sådana parametrar som har betydande påverkan när det gäller personal- och kompetensbehovet samt organisationens dimensionering (även utlagd verksamhet), IT-systemens prestanda etc. Denna typ av underlag och analyser är centrala för styrelsen i arbetet med verksamhetsplanering och budget och har börjat tillämpas sedan ett par år tillbaka.

Styrelsens arbete utvärderas regelbundet och utgör grunden för bedömning av styrelsens och verkställande direktörens prestationer när det gäller bolagets resultat och utveckling. Utvärderingen sker enligt en process som bygger på underlag från Styrelseakademien och Styrelsekollegiet.

Inga arvoden utgår till styrelsen.

2.3 Revisionsutskottet

Våren 2019 beslutade styrelsen att inrätta ett revisionsutskott. Formellt regleras detta i styrelsens arbetsordning. Revisionsutskottets uppgifter består enligt aktiebolagslagen bl.a. av att övervaka bolagets finansiella rapportering samt att övervaka effektiviteten i arbetet med bolagets interna styrning och kontroll som riskhantering, regelefterlevnad (t.ex. dataskyddsfrågornas hantering samt informationssäkerhet m.m.). Vid minPension är avsikten att utskottet även ska bidra till att bereda styrelsens beslut inom kontroll- och granskningsområdet. Ett viktigt skäl till inrättandet av revisionsutskottet är den ökade aktiviteten inom kontroll- och granskningsområdet som är ett resultat av att bolagets verksamhet successivt blir allt mer omfattande och komplex samt de ökade krav som följer av detta, t.ex. gällande dataskyddsfrågor och informationssäkerhet.

Styrelsen har beslutat en arbetsordning för revisionsutskottet samt en granskningsplan för det kommande verksamhetsåret. Revisionsutskottet består av Mats Galvenius (ordförande), Maria Humla och Katarina Thorslund. Utskottet har genomfört nio sammanträden (varav två per capsulam) under 2021.

2.4 Organisation

minPension hade vid årsskiftet 2021/2022 en verkställande direktör och en vice verkställande direktör samt därutöver 14 anställda medarbetare. Organisationen består av en enhet som har ett tvärorganisatoriskt funktionellt ansvar (Stab & stöd) och fyra enheter med ett ansvar för kärnverksamhetens centrala leveransprocesser (Erbjudande & IT, Kommunikation, Kundservice samt Kundvård & sälj).

Bolagets organisation, personal- och ledningsansvar finns dokumenterat i ett särskilt beslut som har fattats av ordföranden och vd.

Som framgått ovan pågår ett intensivt arbete med att vidareutveckla minPensions verksamhet, organisation samt arbetsformer/arbetssätt. Detta är nödvändigt för att bolaget ska kunna klara en tillväxt av antalet användare parallellt med att befintliga tjänster vidareutvecklas och att nya tjänster utvecklas, samtidigt som fler typer av pensionsprodukter ska visas för användarna på minPension.se. En viktig del i detta arbete handlar om att vidareutveckla effektiviteten och tydligheten i centrala processer m.m. såvitt avser både verksamheten och IT. Mot denna

minPension

bakgrund har ett mer processorienterat arbetssätt börjat införas. Inledningsvis innefattar detta endast några av alla de processer, system, objekt och tjänster som finns vid minPension. Dessa kommer successivt att utökas i takt med att arbetet fortskrider. För att få en ökad tydlighet har även ansvariga kopplats till processerna, systemen, objekten och tjänsterna[6].

En betydande del av bolagets verksamhet är utkontrakterad till externa uppdragstagare. Denna verksamhet utgörs av IT-drift och support, övervakning av IT-driften, applikationsförvaltning, IT-utveckling, kundservice samt tjänster inom shared servicecenter (ekonomi, HR, kontors-IT, administration, kontorslokaler etc)[7].

Vid bolaget finns en ledningsgrupp. Ledningsgruppens uppgifter, roll och verksamhet finns reglerad i en särskild arbetsordning.

Utveckling, och framför allt IT-utveckling, utgör en betydande del av minPensions verksamhet. Av detta skäl inrättades för några år sedan ett s.k. projektkontor. Kontorets roll är att vara navet mellan ledningen och projekten och verkar för att projekten koordineras samt arbetar mot de gemensamma verksamhetsmålen. Projektkontoret har en central funktion för att stödja ledningsgruppen med att säkerställa en god styrning, kontroll och uppföljning av de viktigaste projekten som bolaget driver. Ungefär en gång per månad genomförs ett särskilt ledningsgruppsmöte som i stort sett helt fokuserar på förvaltnings- och utvecklingsprojekten. Projektkontoret bistår även projekten och projektledarna på olika sätt.

Utgångspunkten för bolaget har varit att utarbeta en organisation som är anpassad för att kunna möta de nya och förändrade krav som kommer att ställas på bolaget i en nära framtid. En viktig del i detta arbete är t.ex. att hitta en lämplig avvägning mellan att bedriva verksamheten med egen personal eller genom användning av externa uppdragstagare. Frågeställning utgör en central del i den nya IT-sourcingstrategin.

3 Intern kontroll och riskhantering

Styrelsen arbetar löpande med att vidareutveckla och stärka bolagsstyrningen. Detta ska uppnås genom fortsatt arbete med frågor som rör bolagets ”inre arbete”, t.ex. bolagets processer för styrning/ledning,

6 Detta regleras i beslutet ”Beslut om processer, system, objekt och tjänster vid minPension samt ansvariga för dessa”.

7 Denna verksamhet regleras i ”Riktlinjer för utkontraktering av verksamhet vid minPension”.

planering, uppföljning och kontroll samt förvaltning/utveckling. Viktiga områden som arbetet med intern styrning och kontroll fokuseras på inom minPension är

- dataskydds- samt informationssäkerhetsfrågorna,
- de viktigaste arbetsprocesserna inom bolaget, främst inom IT-området samt incidenthantering/rapportering,
- de största och viktigaste projekten, främst inom IT-området,
- ekonomistyrning, ekonomisk rapportering och kostnadseffektivitet, samt
- de mest kritiska leverantörsavtalen avseende utkontrakterad verksamhet.

3.1 Kontrollmiljö

I likhet med föregående år läggs kraft på att vidareutveckla och stärka bolagets förmåga att nå de mål och verkställa de strategier som har beslutats av styrelsen.

Styrelsen och den verkställande direktören ansvarar för fastställande av minPensions styrdokument i form av riktlinjer, planer samt strategidokument. Styrelsen avgör vilka styrdokument som ska fastställas av styrelsen[8].

I en miljö med snäva tidplaner, starka beroenden mellan olika aktiviteter samt med begränsade personella resurser måste bolaget ha en effektiv och väl fungerande bolagsstyrning som säkerställer att bolaget framgångsrikt kan hantera den löpande verksamheten samtidigt som stora och strategiska projekt, aktiviteter, förstudier och utredningar genomförs.

Bolagets arbete med den interna styrningen och kontrollen har successivt vidareutvecklats. Bolaget har en särskild policy för intern styrning och kontroll som styrelsen har beslutat och som revideras årligen. Av denna framgår bl.a. att bolaget ska följa Finansinspektionens allmänna råd om styrning och kontroll av finansiella företag (FFFS 2005:1) i tillämpliga delar. Därutöver har ett arbete genomförts med att implementera en process med tillhörande styrdokument, planer, bemanning etc för intern styrning och kontroll, dvs. uppbyggnad av funktioner för hantering av risker, regelefterlevnad, incidenter och kriser.

8 Detta regleras i styrdokumentet ”Riktlinjer för styrande dokument vid minPension”.

minPension

I samband med att styrelsen ska besluta årsredovisningen inbjuds externrevisionen att redogöra för sina iakttagelser och slutsatser från granskningsarbetet. I det sammanhanget kommenterar även externrevisionen arbetet med den interna styrningen och kontrollen vid bolaget.

3.2 Riskhantering

minPensions riskhantering bygger på tydliga mål, policyer och riktlinjer samt en effektiv operativ struktur och transparent rapportering. minPensions riskhantering följer roll- och ansvarsfördelningen enligt den traditionella modellen med en indelning i tre s.k. ”försvarslinjer”.

1:a försvarslinjen: Styrelsen, bolagsledningen och samtliga medarbetare. Linje- resp. processorganisationen (inkl. system-, objekt-, tjänste- och informationsägare) har det fulla ansvaret för de risker som uppstår i den dagliga verksamheten. Den första försvarslinjen är ansvarig för förvaltningen av minPensions risker och för att följa policyer och regler.

2:a försvarslinjen: Funktionerna för riskhantering resp. regelefterlevnad vid enheten Stab & stöd som rapporterar till bolagsledningen och styrelsen. Andra försvarslinjen ansvarar för att bistå med metodkunskap när det gäller att identifiera, kvantifiera, analysera, hantera och rapportera bolagets risker. Den ansvarar också för att göra vissa kontroller och uppföljningar av risker.

3:e försvarslinjen: För några år sedan beslutade styrelsen att en fristående kontroll- och granskningsfunktion (FKG) skulle inrättas inom bolaget. Funktionen har befogenhet att på egen hand besluta om att genomföra kontroller och granskningar efter samråd med revisionsutskottet eller ordföranden. Funktionen ska således ges full insyn i all verksamhet vid bolaget. Funktionen rapporterar direkt till ordföranden/styrelsen/revisionsutskottet. Rapporteringen sker i normalfallet i samband med styrelsesammanträden och på revisionsutskottets sammanträden.

De övergripande och mest väsentliga risker som bedöms kunna påverka bolagets möjligheter att nå sina mål på ett kostnadseffektivt och säkert sätt är i allt väsentligt kopplade till den komplexa situation som råder och som kommer att råda under de närmaste åren. Ett flertal större projekt, aktiviteter, förstudier och utredningar ska genomföras parallellt med att

den löpande verksamheten och driften ska bedrivas med hög kvalitet, vilket även innefattar att uppfylla författningskrav och andra regelverk. I många fall finns även ett inbördes beroende mellan projekten. Riskerna är ofta relaterade till beroenden av andra aktörer, resursfrågor (främst egen personal, men även personal hos de mest centrala leverantörerna), driftsäkerheten i IT-systemen samt parallella utvecklingsspår och förändringar på minPension.se. Vissa av riskerna är dessutom relaterade till och påverkar varandra. Vidare ska bolaget anpassas för att klara en tillväxt av antalet användare parallellt med att befintliga tjänster vidareutvecklas och nya tjänster utvecklas samtidigt som fler typer av pensionsprodukter ska visas för användarna.

minPension upprättar årligen ett särskilt dokument som innehåller väsentliga risker i bolagets verksamhet. De risker som redovisas i detta dokument följs regelbundet upp av bolagsledningen och resultaten av dessa uppföljningar föreläggs för styrelsen minst två gånger per år, dvs. hur riskerna hanteras (accepteras, begränsas, delas eller elimineras) och utvecklas. Med väsentliga risker avses risker som är så allvarliga att de kan äventyra bolagets måluppfyllelse. I dokumentet beskrivs, kategoriseras och värderas riskerna. Därutöver redovisas vilka åtgärder som har vidtagits eller ska vidtas samt tidplaner för detta arbete. En redogörelse lämnas också för hur riskerna har utvecklats sedan styrelsens föregående uppföljning. Styrelsen har tidigare beslutat ett ”tak” för det högsta tillåtna riskvärdet utan att extraordinära åtgärder omedelbart måste vidtas. I riskdokumentet redovisas även en samlad bedömning av den aggregerade risknivån i verksamheten.

Förutom den hantering av de övergripande och mest väsentliga riskerna som har redogjorts för ovan sker det också en systematisk riskhantering när det gäller risker i projektverksamheten. Detta innebär t.ex. att riskanalyser görs regelmässigt för alla större och strategiska projekt, men även för mindre projekt som är av principiell betydelse, när så bedöms lämpligt. Även på enhetsnivå genomförs en systematisk riskhantering under verksamhetsåret. Riskanalyser genomförs för bolagets olika informationstillgångar inom ramen för informationssäkerhetsarbetet. Varje informationstillgång har en informationsägare. Det är i normalfallet den enhetschef som har ansvaret för den verksamhet som bedrivs där informationen skapas eller inkommer[9].

minPensions verksamhet innebär en exponering mot olika typer av risker, särskilt viktiga är verksamhetsrisker avseende IT-verksamheten och driftsäkerheten i denna, informationssäkerheten, dataskyddsfrågorna och

9 Detta regleras i beslutet ”Beslut om informationstillgångar, informationsägare och deras ansvar vid minPension”.

minPension

användarnas personliga integritet samt risker i anslutning till utkontraktering av verksamhet till leverantörer[10]. Dessa verksamhetsrisker följs noga av bolaget.

3.3 Dataskyddsarbetet

Under 2021 har arbetet främst fokuserats på förvaltning och efterlevnad av GDPR-regelverket. Vid minPension sker förvaltningen av GDPR-regelverket genom en kombination av administrativa, organisatoriska och tekniska åtgärder. För detta ändamål har en särskild förvaltningsorganisation införts[11]. En särskild riktlinje har även utarbetats vars syfte är att ge en överblick över vilka kontroller, uppföljningar m.m. som behöver göras under ett verksamhetsår vid minPension för att skapa och påvisa efterlevnad av GDPR-regelverket[12]. Riktlinjen ligger således till grund för linjeorganisationens löpande dataskyddsarbete.

minPension har under hösten fortsatt arbetet med att säkerställa att bolaget uppfyller de krav som följer av den s.k. Schrems II-domen när det gäller de mest centrala leverantörerna (personuppgiftsbiträden) samt de olika stödsystem som kan vara baserade på s.k. molntjänster. Avsikten är att förvissa sig om att minPensions åtgärder (avtalsmässiga, organisatoriska samt tekniska) är tillräckliga för att kunna påvisa regelefterlevnad. Arbetet har kvalitetssäkrats med stöd av en advokatbyrå, som gjort en genomgång av de åtgärder som minPension har vidtagit baserat på Europeiska Dataskyddsstyrelsens 6-stegsmodell. Resultaten av detta arbete har dokumenterats i en rapport. I anslutning till detta har även en uppföljning gjorts av Cookies-hanteringen, som även den har dokumenterats.

För att få använda tjänsterna på minPension måste pensionsspararna dels godkänna minPensions användarvillkor, dels bekräfta att man har tagit del av hur minPension behandlar personuppgifter. Användaren möter båda dessa dokument på minPensions webbplats. Båda dokumenten har reviderats under året. Skälet är bl.a. att en ny typ av aktörer som tillhandahåller individuellt pensionssparande (IPS) har getts möjlighet att träffa avtal med minPension om att kunna lämna uppgifter om sina kunders IPS-innehav till minPension (s.k. fristående IPS-leverantörer). Vidare kan sedan juni 2021 pensionssparare med statlig pension få en s.k. förenklad

10 Utkontraktering regleras i ”Riktlinjer för utkontraktering av verksamhet vid minPension”.
11 Detta regleras i beslutet ”Beslut om förvaltningsorganisation avseende GDPR-regelverket”.
12 Riktlinje för årliga kontroller och uppföljningar av GDPR-regelverket för att säkerställa efterlevnad

prognos (genom den s.k. API-lösningen) från minPension vid inloggning på Mina sidor hos SPV.

För att undvika risken för eventuella intressekonflikter i dataskydds-arbetet har ett externt dataskyddsombud (DSO) engagerats på uppdragsbasis. Den nya ordningen trädde ikraft i mitten av februari 2021.

Av vd-instruktionen framgår att vd årligen ska lämna en samlad rapport till styrelsen om bolagets arbete med dataskyddsfrågorna. Detta gäller även för övriga organisationer som ingår i Svensk Försäkring i Samverkan (SFIS). På det konstituerande styrelsesammanträdet redovisades således Årlig statusrapport om dataskyddsarbetet vid minPension som styrelsen beslutade. Syftet med rapporten är att redovisa hur minPension arbetar med skyddet av personuppgifter inom sin verksamhet i förhållande till GDPR-regelverket inklusive svensk följdlagstiftning.

3.4 Informationssäkerhetsarbetet

Via minPension.se bearbetas, lagras och överförs stora mängder person-uppgifter och annan integritetskänslig information. Såväl individer, som myndigheter och anslutna aktörer, har krav och förväntningar på att utveckling, drift och förvaltning av minPension.se sker på ett säkert sätt och med ett riskbaserat och systematiskt informationssäkerhetsarbete som grund.

I takt med att minPensions verksamhet successivt ökar i omfattning, vilket bl.a. innebär alltmer komplexa IT-lösningar m.m., samtidigt som bolagets verksamhet blir allt mer betydelsefull och hårdare länkad till de anslutna aktörernas, blir frågor rörande driftsäkerhet, regelefterlevnad och informationssäkerhet allt viktigare. En central fråga i anslutning till detta är även efterlevnaden och förvaltningen av GDPR-regelverket.

minPension har bl.a. som ett långsiktigt mål (ca 3 års sikt) att ett ledningssystem för informationssäkerhet (LIS) enligt standarden ISO 27001 ska implementeras i tillämpliga delar för att minimera bolagets säkerhetsrisker. Arbetet ska bidra till att uppfylla informationssäkerhets-dimensionerna konfidentialitet, riktighet, tillgänglighet och spårbarhet. På några års sikt kan målet vara en certifiering enligt ISO 27001 resp. ISO 27552 (som även täcker in och hanterar GDPR-kraven), om det bedöms som ändamålsenligt.

minPension

I informationssäkerhetsarbetet ingår bl.a. att ta fram ett ramverk med nödvändiga policyer och riktlinjer som ska stödja informations-säkerhetsarbetet. Bolaget har en särskild informationssäkerhetspolicy som har beslutats av styrelsen och som revideras årligen. Bolagets informationssäkerhetspolicy står i överensstämmelse med den infor-mationssäkerhetspolicy som gäller för verksamheter ingående i Svensk Försäkring i Samverkan.

Under året har arbetet med att vidareutveckla informationssäkerheten vid bolaget fortsatt. Arbetet har främst varit inriktat på att fastställa minPensions informationstillgångar och göra riskanalyser kring dessa som en grund för informationsklassning. Ett omfattande arbete har även genomförts med att utarbeta målgruppsanpassade riktlinjer[13] som följer av kraven i standarden ISO 27001 som ska ligga till grund för utform-ningen av styrning/ledning, roller/ansvarsfördelning, processer samt förvaltningsorganisation.

I organisationer med ett högt säkerhetsmedvetande är det brukligt att styrelsen beslutar om vad som är maximal acceptabel avbrottstid i verksamheten. Med stöd av ett säkerhetskonsultföretag har minPen-sion analyserat frågan om vad som är en rimlig maximal acceptabel avbrottstid i minPensions verksamhet med beaktande av kostnader och tekniska begränsningar. Analysen har dokumenterats i ett beslut som har fastställts av styrelsen, vilket kommer att prövas regelbundet inom ramen för minPensions verksamhetsutveckling samt bolagets arbete med informationssäkerhet och kontinuitetshantering.

Den alltmer utbredda s.k. ”Overlay-tekniken”, eller ”skärmskrapning” utgör en risk som har aktualiserats och som har blivit allt påtagligare under de senaste åren. minPension har därför vidtagit en rad olika skyddsåtgärder, bl.a. tekniska, i syfte att försvåra för oseriösa aktörer att missbruka minPension på detta sätt. Det är sannolikt att frågan om missbruk av minPension.se kommer att få än mer aktualitet till följd av den utvidgade flytträtten av fond- och depåförsäkringar. Av detta skäl bedriver minPension ett arbete där den strategi som har utarbetats mot aktörers missbruk av minPension.se vidareutvecklats. Styrelsen har fastslagit att man ser allvarligt på denna typ av missbruk, bl.a. ur ett

13 De målgruppsanpassade informationssäkerhetsriktlinjerna som beslutades i april 2021 är
- Styrning och ledning av informationssäkerhet,
- Informationssäkerhet för chefer,
- Informationssäkerhet för medarbetare, samt
- Säker it.

Riktlinjerna kommer att kompletteras med underliggande styrdokument, exempelvis i form av anvisningar och/eller instruktioner.

kundskydds- och informationssäkerhetsperspektiv, och att arbetet med att bekämpa det därför ska ges hög prioritet.

Under våren 2021 uppdrog minPension åt ett säkerhetskonsultbolag att bistå i arbetet med att klarlägga huruvida minPensions verksamhet och den information som lagras av minPension omfattas av Säkerhetsskyddslagen (2018:585) eller ej. I ett första steg genomförs en förstudie (s.k. skyddsvärdesutredning) som kommer att färdigställas under våren 2022 och föreläggas för styrelsen.

3.5 Kontrollaktiviteter

De generella kontrollaktiviteterna är primärt knutna till den struktur som anges i IT-driftmodell med tillhörande delprocesser. Delprocesserna utgörs av systemövervakning, behörighet, incidenthantering, problemhantering samt förändringshantering.

Modellen stöds av riktlinjer, instruktioner, avtal och andra operativa dokument som reglerar hur IT-driften ska genomföras. Genom delprocesserna beskrivs hur olika kontrollmål uppfylls. Vissa kontrollmål är övergripande och inte knutna till en viss delprocess.

3.6 FKG-granskningar

På uppdrag av styrelsen och revisionsutskottet har den fristående kontroll- och granskningsfunktion (FKG) under verksamhetsåret 2021 slutfört och redovisat två granskningar och påbörjat en. Dessa återfinns i den granskningsplan som styrelsen har beslutat. Granskningarna har fokuserat på olika aspekter av dataskydds- och informationssäkerhetsfrågor samt avtalsefterlevnad.

Granskningsarbetet har genomförts av oberoende konsulter och resultaten från granskningarna har dokumenterats i rapporter. Dessa har i sin tur resulterat i olika åtgärdsplaner, vilka beslutas och följs upp av revisionsutskottet[14].

14 Ett exempel på detta är ”RU:s gemensamma åtgärdsplan avseende dataskydd och informationssäkerhet” avseende de nämnda FKG-granskningarna. Syftet med åtgärdsplanen, som utarbetats av vd och bolagsledningen på uppdrag av revisionsutskottet, är att stödja arbetet med att genomföra önskad ”förflyttning” inom de förbättringsområden som redovisas i granskningsrapporterna. Därutöver har beslutats att utskottet löpande ska följa upp arbetet i förhållande till åtgärdsplanen och vid lämpliga tillfällen återrapportera uppnådda resultat till styrelsen.

minPension

3.7 Information och kommunikation

Policyn för intern styrning och kontroll anger att minPension ska ha för verksamheten ändamålsenliga informations- och kommunikationssystem samt rutiner för spridande av intern information.

I det operativa ansvaret för den verkställande direktören och övriga chefer ingår att upprätta samt fortlöpande revidera minPensions styrdokument samt att hålla medarbetare vid var tid informerade om styrdokumenten. Samtliga styrdokument finns lätt tillgängliga för personalen på minPensions gemensamma server.

3.8 Uppföljning

Uppföljning (avvikelserapportering) av måluppfyllelse, budget och riskhantering sker halvårsvis och redovisas för styrelsen[15].

I den årliga verksamhetsplanen redovisas långsiktiga mål (på ca tre års sikt) som anger vilken ”förflyttning” som ska göras från nuläget samt kortsiktiga (ca ett års sikt) verksamhetsmål. De kortsiktiga målen fungerar som delmål för att uppnå de långsiktiga målen. De lång- och kortsiktiga målen bidrar sammantaget till att nå det övergripande målet. För målen redovisas nuläge och i vissa fall hur måluppfyllelsen ska mätas. Vidare anges vilka större projekt och aktiviteter av strategisk natur som behöver genomföras för att nå målen.

Uppföljningen avseende första halvåret dokumenteras och omfattar
- revidering av Verksamhetsplan och budget för innevarande år,
- halvårsuppföljning av mål och risker, samt
- halvårsuppföljning av budget och prognos.

Uppföljningen avseende ett helt verksamhetsår dokumenteras och omfattar
- årsuppföljning av Verksamhetsplan och budget för innevarande år,
- årsuppföljning av mål och risker,
- årsuppföljning av budget,
- styrelsens årliga strategidag, samt
- beslut om verksamhetsplan och budget samt risker för kommande år.

15 Detta regleras i styrdokumentet ”Anvisningar för uppföljning av mål, projekt/aktiviteter, budget och väsentliga risker”.

Uppföljning avseende de åtgärdsplaner som har blivit ett resultat av de FKG-granskningarna som har genomförts följs löpande upp av revisionsutskottet.

4 Hållbar verksamhet

Sedan några år tillbaka är det obligatoriskt för stora bolag att årligen avge en hållbarhetsrapport. Hållbarhetsrapporten ska innehålla de icke-finansiella upplysningar som behövs för förståelsen av företagets utveckling, ställning, resultat och konsekvenserna av dess verksamhet, däribland upplysningar i frågor som rör miljö, personal och sociala förhållanden, respekt för mänskliga rättigheter och motverkande av korruption.

minPension omfattas inte av lagkravet men arbetar med hållbarhetsfrågorna på ett verksamhetsanpassat sätt. Målet är att bidra till såväl en hållbar samhällsutveckling som en hållbarhetsanpassad verksamhet.

Arbetet operationaliseras bl.a. genom att minPension förvissar sig om att de mest centrala leverantörerna arbetar systematiskt med hållbarhetsfrågor i sin verksamhet. Det handlar t.ex. om analys av risker och möjligheter förknippade med etik, miljö och andra hållbarhetsfrågor. En redogörelse från dessa begärs årligen in för att ingå i ett årligt dokument som redovisas för styrelsen.

5 Revisorer

Vid årsstämman 2019 beslutades att utse revisionsbolaget Deloitte till minPensions revisor, med auktoriserade revisorn Henrik Nilsson som huvudansvarig, för en tid av fyra år från och med räkenskapsåret 2019. Revisorns uppgift är att granska bolagets finansiella rapportering samt styrelsen och verkställande direktörens förvaltning av bolaget.