ARBETSORDNING FÖR STYRELSEN I S:T ERIK FÖRSÄKRINGS AB JÄMTE INSTRUKTION FÖR ARBETSFÖRDELNING MELLAN STYRELSEN OCH VD M.FL

FASTSTÄLLD AV STYRELSEN 2022-05-23

A ARBETSORDNING FÖR STYRELSEN

A.1 Allmänt

Denna arbetsordning med tillhörande instruktioner har upprättats i enlighet med 8 kap 46a och b §§ ABL samt 10 kap 6 och 14§§ Försäkringsrörelselagen (riskhantering och intern kontroll) och ska revideras årligen och vid behov.

Arbetsordningen ska skickas till varje styrelseledamot, styrelsesuppleant, VD och revisorerna med suppleanter.

A.2 Styrelsesammanträden

A.2.1 Tid och plats för styrelsesammanträden

Tid och plats för styrelsesammanträden fastställs av styrelsen.

Styrelsen ska normalt hålla fem ordinarie sammanträden per arbetsår.

Utgångspunkten för de ordinarie styrelsesammanträdena är att dessa hålls i en lokal där alla ledamöter och suppleanter som kan deltar på plats. Distansdeltagande enligt nedan är endast avsett att vara ett komplement till fysisk närvaro.

Vid ordinarie styrelsesammanträde får ordförande i samråd med vice ordförande, om särskilda skäl föreligger, i kallelsens föreslå att styrelseledamot, suppleant, arbetstagarrepresentant och annan får närvara på distans. Om ordinarie styrelseledamöter inte samtycker till att så sker ska de i svar på kallelsen ange detta. För att deltagande på distans ska vara möjligt krävs att ingen av ordinarie styrelseledamöter motsätter sig detta senast tre arbetsdagar innan mötet. Om någon motsätter sig distansdeltagande på möte meddelas detta per mail via styrelsesekreterare.

Ledamot, suppleant, arbetstagarrepresentant eller annan som önskar delta på distans ska anmäla detta till ordföranden senast två arbetsdagar innan styrelsesammanträdet.

Om känsliga och/eller sekretessbelagda uppgifter kommer att avhandlas vid sammanträdet måste lämpliga tekniska och organisatoriska åtgärder vidtas för att sekretessen ska upprätthållas.

En förutsättning för deltagande på distans är bland annat att sekretessen kan upprätthållas, att distansdeltagande ledamot, suppleant och arbetstagarrepresentant har möjlighet att ta del av handlingar som delas ut vid mötet och att skyddet för personuppgifter kan upprätthållas. Ärenden som hanteras på styrelsesammanträdet kan vara sådana att det inte är lämpligt att hantera dessa annat än på ett fysiskt möte utan deltagande på distans.

Beslut fattade med deltagare på distans ska protokollföras på vanligt sätt enligt punkt A.2.7 nedan.

A.2.2 Återkommande ärenden

Vid varje ordinarie styrelsesammanträde ska följande ärenden behandlas:

- Utseende av protokolljusterare
- Föregående protokoll
- Beslutspunkter
- Ekonomisk rapportering
- Skaderapportering
- Regelefterlevnadsrapport
- Anmälan om klagomål
- Sammanfattande riskrapport
- Revision
- Annan rapportering
- Övrigt
- Ärendebalans

A.2.3 Särskilda ärenden

Utöver de återkommande ärenden som angetts ovan ska följande ärenden behandlas som beslutspunkter vid sammanträde nedan angivna tidpunkter.

Tidpunkt	Ärende som ska behandlas
Årets första ordinarie sammanträde	Årsbokslut Budget och inriktning för de kommande tre åren. Kontroll av intressekonflikter Revisionsrapport ORSA, SFCR, RSR, Årlig QRT Uppföljning internkontrollplan Antagande av Finanspolicy för Stockholms Kommunkoncern och Stockholms Stadshus AB.
Första ordinarie sammanträde efter bolagsstämman	Ändrad firmateckningsrätt (vid behov); Antagande av arbetsordning, VD-instruktion samt övriga instruktioner och policys.
Sista ordinarie sammanträde före sommaren	Tertialbokslut 1 jämte prognos.
Första ordinarie sammanträde efter sommaren	Strategimöte. Tertialbokslut 2 jämte prognos
Årets sista ordinarie sammanträde	Budget. Återförsäkring Sammanträdestider för nästkommande år. Riskinventering Riskkontrollplan

Årlig rapport från regelefterlevnads-funktionen.
Regelefterlevnadsplan
Internkontrollplan

Därutöver ska behandlas sådana ärenden som anges nedan under B.1.3

A.2.4 Extra styrelsesammanträde

För överläggning och beslut i ärenden som inte kan hänskjutas till ett ordinarie styrelsesammanträde, kan sammanträde hållas vid andra tillfällen. Detta kan begäras av styrelseledamot eller VD genom framställning till styrelsens ordförande.

Extra styrelsesammanträde får hållas per telefon, genom videokonferens eller motsvarande digitalt media (se A.2.1 avseende säkerhet). Beslut fattade i sådan ordning ska protokollföras på vanligt sätt enligt punkt A.2.7 nedan.

Extra styrelsesammanträde kan också avhållas per capsulam, varvid protokoll med förslag till beslut upprättas och därefter cirkuleras eller utsänds till var och en av ledamöterna.. Styrelsesammanträde i denna ordning får hållas endast om samtliga ordinarie styrelseledamöter biträder besluten d.v.s. att inga avvikande meningar lämnas. De ordinarie styrelseledamöterna anses ha bistått beslutet i och med undertecknande av protokollet alternativt efter att de har lämnat sitt godkännande till förslaget via e-postmeddelanden och undertecknande skett i enlighet med punkten A2.7 nedan.

A.2.5 Kallelse och underlag

Till styrelsesammanträdena, ordinarie och extra, ska samtliga styrelseledamöter och suppleanter kallas. Kallelse med dagordning och skriftlig dokumentation i form av underlag, rapporter och, vad gäller beslutspunkter, förslag till beslut, ska om inte särskilda skäl föreligger sändas ut eller finnas publicerad på anvisad e-tjänst för styrelsehandlingar senast sju dagar före styrelsesammanträdet. Om särskilda skäl föreligger får en eller flera av handlingarna eller justerade versioner av redan tillgängliggjorda handlingar inklusive justerad dagordning göras tillgängliga i anvisad e-tjänst senast två veckodagar före sammanträdet eller, om oundvikligt, lämnas direkt vid sammanträdet.

Utöver vad som ovan angivits ska kopia av kallelse sändas ut per e-post till bolagets revisorer och Stockholms Stadshus AB. Tillhörande handlingar ska finnas att tillgå elektroniskt för dessa om inte annat framgår nedan.

Handlingarna i den anvisade e-tjänsten för styrelsehandlingar publiceras internt för styrelsen, vilket innebär att inloggning krävs för att få tillgång till handlingarna i anvisad e-tjänst. Samtliga styrelseledamöter och suppleanter förutsätts ha tillförsäkrat sig tillgång till anvisad e-tjänst för styrelsehandlingar genom egen personlig inloggningDe handlingar som finns att tillgå elektroniskt anses vara ledamöter och suppleanter tillhanda samma dag som publicering sker. De handlingar som sänds via post anses vara tillhanda dagen efter avsändandet. Handlingar där uppgifter med sekretess föreligger publiceras inte i den anvisade e-tjänsten och tillhandahålls enligt vad som närmare framgår av respektive kallelse.

Styrelsesammanträden ska hållas med utgångspunkt från att utsänt material är inläst.

A.2.6 Beslut

Styrelsen fattar beslut genom att en majoritet biträder beslutet enligt 8 kap 22§ ABL, förutom vad som anges i punkt A.2.4 angående extra sammanträde per capsulam.

A.2.7 Protokoll

Styrelsens ordförande ansvarar för att protokoll förs vid varje styrelsesammanträde. Protokollet ska föras av sekreteraren eller av annan av styrelsen särskilt utsedd person. Protokollet ska vara kortfattat, dock med iakttagande av de krav som föreligger enligt 8 kap 24§ ABL. Protokollet ska ange fattade beslut och det underlag, muntligt och/eller skriftligt redovisat, som besluten grundats på. Vidare ska av protokollet framgå avvikande mening (reservation) eller särskilt uttalande som styrelseledamot eller VD begärt att få antecknat.

Protokollen ska undertecknas av sekreteraren, eller den ovan annan av styrelsen särskilt utsedd person, och justeras av ordföranden vid sammanträdet jämte en särskilt vid sammanträdet därtill utsedd person. Vid styrelsesammanträden per capsulam justeras protokollet av ordförande och vice ordförande.

Styrelsens sekreterare ska se till att kopior av protokollen, efter justering, skickas till, eller publiceras på anvisad e-tjänst för styrelsehandlingar, till samtliga styrelseledamöter, revisorer och Stockholms Stadshus AB.

Protokollen ska - för kalenderår - numreras och ges löpande paginering. VD svarar för att protokollen jämte beslutsunderlag förvaras på ett betryggande sätt i enlighet med 8 kap 26§ ABL.

A.2.8 Ordförande vid styrelsesammanträdena

Styrelsens ordförande, eller vid dennes förhinder vice ordföranden, är ordförande vid styrelsesammanträden. Om varken ordföranden eller vice ordföranden kan närvara utser styrelsen annan ledamot att för tillfället leda styrelsens arbete. Tills valet har förrättats fullgörs ordförandens uppgifter av den som varit ledamot i styrelsen längst tid. Om flera ledamöter har lika lång tjänstgöringstid fullgörs detta temporära ordförandeskap av den äldste av dem.

A.3 Arbetsfördelningen inom styrelsen

Styrelsen ska ha en ordförande och en vice ordförande (valda av Kommunfullmäktige enligt Bolagsordningen). Ordföranden, eller i dennes ställe vice ordföranden, ska leda styrelsens arbete och bevaka att styrelsen fullgör sina uppgifter samt se till att styrelsen sammanträder i den omfattning och på det sätt som anges i denna arbetsordning eller som följer av lag. Ordföranden ska upprätthålla en nära och fortlöpande kontakt med VD angående bolagets utveckling.

Stockholms Stadshus AB samordnar rekrytering av VD till dotterbolagen i samarbete med dotterbolagets ordförande, dotterbolagets vice ordförande och koncernstyrelsens ordförande/vice ordförande. Beslutet om anställning av VD fattas av dotterbolagets styrelse. Dotterbolagets ordförande och vice ordförande beslutar gemensamt, efter samråd med Stockholms Stadshus AB och koncernstyrelsens ordförande/vice ordförande, VD:s förmåner vid nyanställning. Detsamma gäller vid förändringar av villkoren i anställningsavtalet. . Styrelsen ska informera om VD:s anställningsförmåner. Stockholm Stadshus AB samordnar, på motsva-

rande sätt, villkoren vid avslut av VD:s anställning i bolaget. Arbetet sker i samråd med bolagets ordförande och vice ordförande samt koncernstyrelsens ordförande/vice ordförande. Bolagets ordförande, efter samråd med vice ordförande, äger ingå avtal om avslut av anställning VD. Beslutet om entledigande av VD fattas av bolagets styrelse.

Till ordföranden, eller i dennes ställe vice ordföranden, delegeras beslutanderätten att utse och befullmäktiga ersättare för VD vid dennes frånvaro. Fullmakten får som längst avse tiden fram till och med nästa styrelsemöte och kan därefter förlängas av styrelsen.

Stockholm Stadshus AB samordnar den årliga lönerevisionen för VD, vilket bland annat innebär att ta fram underlag och förslag till ny lön. Bolagets ordförande ansvarar, efter samråd med moderbolaget och koncernstyrelsens ordförande/vice ordförande, för att träffa överenskommelse med VD om lönerevision. Styrelsen ska informeras om VD:s lönerevision.

Bolagets ordförande och vice ordförande beslutar gemensamt om eventuellt avsteg från principen att VD inte äger bedriva verksamhet (inneha bisyssla) vid sidan av sin anställning i bolaget (jfr bland annat 8 kap 34§ ABL).

Det förekommer därutöver inte någon särskild arbetsfördelning inom styrelsen. Styrelsen får dock uppdra åt en eller flera av styrelsens ledamöter att vidta vissa åtgärder eller vara ansvarig för vissa ärenden. Styrelsen ska ha en särskilt utsedd sekreterare.

Bolaget är personuppgiftsansvarigt enligt bestämmelserna i GDPR, vilket innebär att i första hand bolagets styrelse ansvarar för de åligganden som bestäms i denna förordning och tillhörande nationell lagstiftning.

A.4 Övrigt

A.4.1 Kommunens ledningsfunktion

Bolagets styrelse och VD har att följa av bolagsstämman eller av kommunfullmäktige utfärdade ägardirektiv, såvida dessa inte strider mot bolagsordning, lag eller bolagets intresse.

Som framgår av bolagsordningen har kommunstyrelsen, om inte sekretess föreligger, rätt att ta del av bolagets handlingar och räkenskaper, samt i övrigt inspektera bolaget och dess verksamhet. Bolaget ska därför, om inte sekretess föreligger, lämna kommunstyrelsen den information om verksamheten som den begär. Bolagets styrelse eller VD ska, vid behov, se till att detta görs.

Beslut om bildande eller avveckling av bolag eller verksamhetsgren, liksom andra strategiskt eller principiellt viktiga frågor ska underställas kommunfullmäktige för prövning (jfr bolagsordningen).

A.4.2 Investeringar

- Investeringsplan fastställs i budget.
- Inriktningsbeslut och genomförandebeslut om investeringar överstigande 300 mnkr ska föreläggas kommunfullmäktige för godkännande.
- Uppföljning och återredovisning sker fortlöpande i koncernstyrelsen i tertialrapporter, samt i årsredovisningen.

Enligt 10 kap. 3 § kommunallagen ska det i bolagsordningen framgå att kommunfullmäktige ska få ta ställning innan sådana beslut i bolagets verksamhet som är av principiell beskaffenhet eller annars av större vikt fattas. Ärenden som ligger utanför bolagets reguljära verksamhet eller är av särskilt känslig natur bör därför, oavsett belopp, behandlas som frågor av principiell beskaffenhet eller annars av större vikt och kräver godkännande av kommunfullmäktige. Förvärv av bolag ska, liksom bildande av bolag, också betraktas som ärenden av principiell beskaffenhet eller annars av större vikt och kräver godkännande av kommunfullmäktige.

A.4.2 Gåva

Gåva till allmännyttigt eller därmed jämförligt ändamål beslutas av ägaren/bolagsstämman. Styrelsen kan dock fatta beslut att lämna gåva för allmännyttigt eller därmed jämförligt ändamål om det med hänsyn till bolagets ställning är av ringa värde och det rymmer inom den kommunala kompetensen. (jfr 17 kap 5 § ABL).

A.4.3 Sekretess

All information som lämnas till styrelsens ledamöter, suppleanter och revisorer och som ej är offentliggjord ska, med beaktande av vad som gäller enligt tryckfrihetsförordningens samt offentlighets- och sekretesslagens bestämmelser, behandlas så att bolaget inte skadas. Handling eller information som är sekretesskyddad får ej lämnas vidare till eller röjas för annan.

B. INSTRUKTION FÖR ARBETSFÖRDELNINGEN MELLAN STYRELSEN OCH VD M.FL.

B.1 Styrelsen

B.1.1 Allmänt

Enligt 8 kap 29 och 36 §§ äger VD, eller i dennes ställe utsedd ersättare, generellt att företräda bolaget utåt och teckna dess firma i vad avser all löpande förvaltning såvida inte styrelsen genom riktlinjer eller anvisningar gjort särskilda begränsningar.

Styrelsen har det yttersta ansvaret för bolagets organisation och förvaltning av dess angelägenheter.

Styrelsen ska se till att bolagets organisation är så utformad att bokföringen, medelsförvaltningen och bolagets ekonomiska förhållanden i övrigt kontrolleras på ett betryggande sätt.

Styrelsen ska fastställa målsättningar, policys och strategiska planer som är av väsentlig betydelse för bolaget. Styrelsen ska vid behov se till att de blir föremål för uppdateringar och översyner.

Styrelsen svarar för den årliga fastställelsen av denna instruktion.

B.1.2 Utlämnande av allmän handling

Till VD, dennes ersättare och bolagsjurist är delegerat beslutanderätten om utlämnande av allmänna handlingar (jfr 6 kap 2 och 3 §§ offentlighets- och sekretesslagen).

B.1.3 Frågor som ska beslutas av styrelsen m.m.

VD ska förelägga styrelsen nedan angivna frågor för beslut. Beloppen är angivna exklusive mervärdesskatt.

a)	Ingående av avtal som ej ingår i den löpande verksamheten	> 100.000 kr
b)	Teckning, förvärv eller avyttring av aktier	Oberoende av belopp
c)	Upptagande eller lämnande av lån, refinansiering, garantier, panter eller borgen.	Oberoende av belopp
d)	Beslut om löner eller andra anställningsvillkor för ledande befattningshavare på annat än för branschen sedvanliga villkor	Oberoende av belopp
e)	Förändring av affärsplan	
f)	Avsteg från stadens policies om representation m.m.	Oberoende av belopp
g)	Avsteg från försäkringstekniska riktlinjer	
h)	Andra frågor som är av större principiell betydelse	

Beslut i ovan angivna frågor, dock inte fråga avseende 8 kap 34 § ABL, får för särskilt tillfälle genom beslut av styrelsen delegeras till VD. Beslut om sådan delegering ska antecknas i protokoll.

Avtal som ej avser löpande förvaltningsåtgärder ska alltid tecknas av två firmatecknare i förening.

VDs kostnader godkänns av ordföranden. Ordförandens kostnader godkänns av vice ordförande tillsammans med VD. Styrelseledamots-/ersättares kostnader godkänns av ordförande tillsammans med vice ordförande och VD

B.1.4 Information och rapportering till styrelsen

Beslut som har fattats av VD i den löpande förvaltningen men som är av större betydelse för bolagets eller koncernens verksamhet och ekonomiska situation ska rapporteras till styrelsen vid närmast följande sammanträde.

Denna rapportering ska innefatta resultat, finansieringsförhållanden, likviditet och andra betydelsefulla ekonomiska förhållanden samt information om viktiga händelser, såsom exempelvis uppkomna tvister av betydelse, uppsägning av för bolaget viktigare avtal, etc.

I brådskande fall, samt när behov i övrigt föreligger mellan ordinarie styrelsemöten, ska rapportering ske direkt till styrelsens ordförande. Rapporteringen ska vara av sådan beskaffenhet att styrelsen tillåts göra en välgrundad bedömning.

Till moderbolaget ska rapportering baseras på det koncernrapporteringssystem som anges av Stockholms Stadshus AB

B.1.5 Kontroll - Attest - Utanordning

VD ska upprätta förslag till fullständig instruktion som reglerar attesträtten m.m. inom bolaget. I instruktionen ska anges vem som ska utföra underliggande kontroll och vilka befattningshavare som har attest- respektive utanordningsrätt. Instruktionen fastställs av bolagets styrelse och ska i tillämpliga delar utgå från av Staden centralt beslutade principer.

Attestberättigad äger rätt att skriftligt delegera utförandet av nödvändiga kontrollåtgärder.

B.2 VD

B.2.1 Allmänt

VD är skyldig att i sitt handlande för bolaget främja dess intressen. VD ska iaktta lojalitetsplikt som följer av anställningen vilket bl.a. innebär att denne, med beaktande av vad som gäller enligt tryckfrihetsförordningens och sekretesslagens bestämmelser, behandlar all information till utomstående så att bolaget inte skadas och att denne har upplysningsplikt gentemot styrelsen rörande angelägenheter och förhållanden som har betydelse för bolaget.

VD får inte handlägga fråga:

- rörande mellanhavande mellan sig och bolaget,
- mellan bolaget och tredje man om VD i fråga har ett väsentligt intresse som kan strida mot bolagets,
- mellan bolaget och tredje man som VD ensam eller tillsammans med annan får företräda.

Vad som sägs om VD gäller även den som satts i VD:s ställe, såvida styrelsen inte genom riktlinjer eller anvisningar gjort särskilda begränsningar.

B.2.2 Föredragande m.m.

VD ska upprätta förslag till dagordning inför styrelsesammanträdena och inhämta styrelsens ordförandes godkännande innan det skickas ut. VD ska också ta fram erforderligt informations- och beslutsunderlag inför sammanträdena samt i övrigt uppfylla sina åligganden enligt denna arbetsordning.

VD ska vidare vara föredragande vid styrelsens sammanträden och därvid avge motiverade förslag till beslut. VD får, där så är lämpligt, delegera uppgiften som föredragande i särskilt ärende till annan person som är underställd. För särskilt fall kan extern föredragande (t.ex. anlitad konsult för visst projekt) komma i fråga.

B.2.3 Övrigt

VD ansvarar för att bolagets bokföring fullgörs i överensstämmelse med lag och annan författning och att medelsförvaltningen sköts på ett betryggande sätt.

Som framgår av bolagsordningen har kommunstyrelsen, om inte sekretess föreligger, rätt att ta del av bolagets handlingar och räkenskaper, samt i övrigt inspektera bolaget och dess verksamhet. Bolaget ska därför, om inte sekretess föreligger, lämna kommunstyrelsen den information om verksamheten som den begär. Bolagets styrelse eller VD ska, vid behov, se till att detta görs.

ERSÄTTNINGSPOLICY FÖR S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

Innehåll

1 Allmänt

Denna policy har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Syftet med policyn är att ersättningar inte ska hota företagets förmåga att upprätthålla en lämplig kapitalbas samt är i linje med företagets riskprofil.

Dokumentet ska prövas årligen av styrelsen och revideras vid behov.

2 Ersättningsprinciper

Rörlig ersättning ska inte utgå till någon befattningshavare hos S:t Erik Försäkring.

Uppgifter om VD:s ersättning, i form av lön, andra förmåner och pension, ska redovisas öppet i årsredovisningen.

Lönesättande kriterier framgår av bolagets Lönepolicy.

ETISK POLICY FÖR S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

Innehåll

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna ska prövas årligen av styrelsen och revideras vid behov.

2 Bolagets etiska värdegrund

S:t Erik Försäkrings uppdrag är att svara för att kommunkoncernen har ett adekvat försäkringsskydd utifrån kostnads- och nyttoaspekten. Bolaget ska verka för att kunder och ägare har ett starkt förtroende för bolagets verksamhet. Det är viktigt att bolagets styrelse, ledning och medarbetare har en samsyn kring bolagets värdegrund och hur den efterlevs i den dagliga verksamheten. Bolaget följer stadens riktlinjer som anges i stöd- och styrdokument.

3 Policy

Kunder, ägare och övriga intressenter hos S:t Erik Försäkring ska känna trygghet och förtroende genom de höga krav bolaget ställer på sig självt såväl externt som internt. Verksamheten ska präglas av hederlighet, professionalism, integritet, vänlighet, lojalitet och långsiktighet.

Hög etik går längre och ställer större krav än att endast avstå från det otillåtna. S:t Erik Försäkring håller sig därför på ett betryggande respektavstånd från det otillåtna.

4 Grundläggande etiska principer

I alla möten med kunder, leverantörer, samarbetsparters, övriga intressenter och medarbetare emellan ska S:t Erik Försäkring vara bärare av följande grundläggande värderingar och principer:

Hederlighet. Vi är öppna, ärliga och rättvisa. Vi håller vad vi lovar vad gäller service, handläggningstider, tillgänglighet, m.m. Om något hakar upp sig på vägen informerar vi om det så fort vi kan. Det är ett minimum att leva upp till lagar och förordningar, god branschsed och interna regler. Hederlighet innebär att vi rakryggad står för allt vi gör. Vi ska tåla genomlysning utan att skämmas.

Professionalism och respekt. Vi är ytterst professionella och har tillgång till ledande kompetens inom vårt ansvarsområde. Inom bolaget råder ömsesidig professionell respekt oavsett vilka arbetsuppgifter vi har. Ömsesidig professionalism och respekt ska prägla våra relationer med kunder, leverantörer och övriga intressenter. Vi kommer alltid väl förberedda och i tid till möten, av respekt mot alla vi möter liksom mot oss själva. Till professionalismen hör kreativitet och strävan efter ständiga förbättringar.

Integritet. Genom vårt agerande kan vi sakligt och engagerat argumentera för våra synpunkter när vi ger råd eller inför ett beslut. Vårt handlande präglas av tydlighet och rättvisa och påverkas vare sig av risk för obehag eller av möjliga fördelar. Integritet visar vi i vår förmåga att stå emot otillbörliga påtryckningar, oavsett varifrån de kommer. Vår opartiskhet får aldrig kunna ifrågasättas.

Lojalitet. Vår verksamhet är av stor betydelse för våra kunder. Verksamheten kan därför ibland bli föremål för särskilda meningsyttringar. På jobbet är vi ärliga och uppriktiga i vår kommunikation och i vårt handlande. Vi talar till varandra och inte om varandra. Det är lojalt och vittnar om integritet att tala till bolagets ledning liksom till medarbetare när något är fel och bör rättas till i stället för att tiga. Alla påpekanden om fel och brister ska tas på allvar av både ledning och styrelse.

Vänlighet. Vi bemöter varje kund, samarbetspartner eller kollega på ett sätt som motsvarar dennes positiva förväntan på vårt agerande. Vi visar respekt för individen och vi har initiativkraft och förmåga till inlevelse i den andres situation.

Långsiktighet. Vårt uppdrag är att finnas vid kundens sida i ur och skur långsiktigt. Vi ska svara för trygghet, uthållighet och långsiktighet. Vi ska söka nya vägar men eftersträvar i slutändan tillförlitliga, robusta och förtroendegivande lösningar.

Efterlevnad. S:t Erik Försäkrings styrelse, ledning och medarbetare ska följa lagar och övriga bestämmelser som styr bolagets verksamhet, inte bara i bokstavlig mening utan med insikt om det bakomliggande syftet. Förtroendet för bolaget ska vara starkt och orubbat.

Alla situationer kan inte tydliggöras genom etiska regler och riktlinjer – var och en måste med utgångspunkt i sitt eget goda omdöme och sunda förnuft ta ansvar för att i varje enskilt fall handla på ett etiskt korrekt sätt. Internt ska S:t Erik Försäkring präglas av ett öppet diskussionsklimat där vi talar med varandra om vad som är lämpligt uppträdande, så att vi utvecklar tydliga gemensamma värderingar i frågor av etisk natur som rör arbetet.

5 Kundrelationen

S:t Erik Försäkring ska lämna aktiv service och alla uppdrag ska ske så skyndsamt som möjligt. Beslut ska alltid motiveras.

Kunden ska på ett enkelt och lättfattligt sätt informeras om sina rättigheter och skyldigheter samt om bolagets åtgärder och beslut.

Blir ett ärende fördröjt ska kunden skyndsamt upplysas om anledningen. Beror dröjsmålet på kunden ska kunden informeras om att den fortsatta handläggningen är beroende av dennes åtgärder.

Handläggningen av kundärenden ska ske smidigt med lyhördhet för kundens individuella förhållanden.

6 Leverantörer

S:t Erik Försäkring effektiviserar verksamheten genom att lägga ansvar för vissa delar av verksamheten på externa leverantörer/samarbetspartner. Då brister i deras verksamhet kan skada förtroendet för S:t Erik Försäkring är det viktigt vid val av kritiska leverantörer att de kan tydliggöra att de egna etiska riktlinjerna är i paritet med S:t Erik Försäkrings.

7 Övriga föreskrifter

Så som dotterbolag till Stockholms Stadshus AB ska S:t Erik Försäkring och bolagets medarbetare i övrigt agera efter moderbolagets policys och riktlinjer inom det etiska området.

Dokument finns på Stockholms stads intranät: intranat.stockholm.se.

FÖRSÄKRINGSPLAN

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Föreliggande försäkringsplan är antagen av styrelsen för S:t Erik Försäkring och ska revideras årligen.

Inom Stockholms kommunkoncern ska de i denna försäkringsplan angivna självriskerna och försäkringsomfattningarna normalt gälla hos respektive enhet. Avsteg får endast göras efter samråd med S:t Erik Försäkring. Bolaget beslutar om försäkring ska tillhandahållas direkt, indirekt eller placeras hos annat bolag.

2 Bakgrund

Stockholms kommunfullmäktige beslöt godkänna en försäkringspolicy för Stockholms stad i enlighet med kommunstyrelsens utlåtande 2004:22. Av försäkringspolicyn framgår bland annat att styrelsen för S:t Erik Försäkring årligen ska fastställa en försäkringsplan. ”Försäkringsplanen ska ange uppgifter om kommunkoncernens aktuella försäkringstyper, såsom ansvars-, egendoms-, förmögenhetsbrottsförsäkring, etc, med tillhörande ramar för självrisker och försäkringsomfattning.

Stockholms stads förvaltningar och bolag har skyldighet att teckna försäkringar i syfte att skydda stadens egendom och verksamhet, så att egendomens långsiktiga värde bibehålls”.

Vidare anges i försäkringspolicyn att det är respektive nämnd och styrelse som fattar beslut om försäkring, dock efter samråd med S:t Erik Försäkring.

3 Försäkringstyper

I försäkringspolicyn anges att styrelsen ska besluta om ramar för självrisker och försäkringsomfattning. Med föreliggande försäkringsplan lämnar styrelsen för S:t Erik Försäkring anvisningar enligt nedan. VD äger rätt vidta mindre avvikelser.

Följande försäkringar ska vid behov finnas inom Stockholms stads förvaltningar och bolag samt stiftelser. Ytterligare försäkringsbehov kan finnas för vissa enheter. Redovisade självrisknivåer, försäkringsomfattning och försäkringsbelopp ska normalt gälla.

3.1 Övergripande begränsade försäkringsbelopp

Försäkringsbeloppet för kommunkoncernen som helhet, eller för enskilda försäkringsmoment, ska begränsas med beaktande av risk, återförsäkring och branschpraxis.

Följande begränsade försäkringsbelopp är gemensamma för samtliga förvaltningar, stiftelser och bolag som har försäkring i S:t Erik Försäkrings AB:

<u>Egendomsförsäkring</u>

- Totalt försäkringsbelopp (loss limit) 3 200 000 KSEK per skada och år
- Inom det totala försäkringsbeloppet gäller följande begränsningar (sublimiter):

- Storm, översvämning och jordskalv 500 000 KSEK per skada och försäkringsår

- Krav som inte ingår i traditionell brand-, inbrott-, vatten- eller maskinförsäkring (allrisk) 500 000 KSEK per skada och försäkringsår

- Inventarier per försäkringsställe 350 000 KSEK per skada och försäkringsår

Terrorism försäkring

- Första risk 2 000 000 000 SEK per skada och år, dock max det belopp som anges i underliggande försäkringsbrev.
-
- Inom det totala försäkringsbeloppet gäller följande begränsningar (sublimiter):

    - Extrakostnader 10 000 000 SEK per skada .

    - Stockholmsmässan 500 000 000 SEK per skada

Ansvarsförsäkring

- Totalt försäkringsbelopp (loss limit) 500 000 KSEK per skada och år

- Försäkringen gäller inte för skador som enheter - bolag, förvaltningar och stiftelser inom Stockholms kommunkoncern - med ansvarsförsäkring hos S:t Erik Försäkring orsakar varandra.

3.2 Förvaltningssektorn

Försäkring	***Försäkringsgivare***	***Självrisk***	***Omfattning***	***Försäkrings-belopp***
Allmänt ansvar	S:t Erik Försäkring	1 basbelopp	Enl. villkor	500 mnkr
Ansvar, ren förmögenhetsskada	S:t Erik Försäkring	10 basbelopp	Enl. villkor	10 mnkr
Byggherreansvar	S:t Erik Försäkring	3 basbelopp	Enl. villkor	10 mnkr
Byggherreansvar över 10 mnkr	Upphandlas vid behov	Varierande	Enl. villkor	Efter behov
Byggfel	Upphandlas vid behov	Varierande	Enl. villkor	Efter behov
Egendom, byggnad	S:t Erik Försäkring	3 eller 10 basbelopp	Allrisk	Fullvärde. alt. Första risk
Egendom, inventarier	S:t Erik Försäkring	1 basbelopp	Allrisk	Max 350 mnkr per försäkrings-ställe
Entreprenad (CAR)	S:t Erik Försäkring	3 basbelopp	Allrisk	Enl. förs.brev.

Extrakostnader/ Hyresförlust	S:t Erik Försäkring	Se egendom	24 månader	Varierande -
Förmögenhetsbrott	Länsförsäkringar	1 mnkr	Enl. villkor	200 mnkr
Motorfordon	Protector	Varierande	Helförsäkring	-
Tjänsteresa	Gouda	-	Enl. villkor	Varierande
Utländska besökare	Gouda	-	Enl. villkor	Varierande
Olycksfallsförsäkring	S:t Erik Försäkring	-	Enl. villkor	Enl. villkor
Reseförsäkring, elev	ERV	-	Enl. villkor	Enl. villkor
Patientförsäkring	Moderna försäkringar	Enligt villkor	Enl. villkor	Enl. villkor
Utställning	S:t Erik Försäkring	5 000 kr	Allrisk	Enl. förs.brev
VD/ Styrelseansvar	Protector	-	Enl. villkor	100 mnkr
Terrorism	S:t Erik Försäkring	-	Enl. villkor	2000 mnkr

(CAR = contractors all risks insurance)

3.3 Bolagssektorn

Försäkring	***Försäkringsgivare***	***Självrisk***	***Omfattning***	***Försäkrings-belopp***
Allmänt ansvar	S:t Erik Försäkring	1 basbelopp	Enl. villkor	10 mnkr
Allmänt ansvar	S:t Erik Försäkring	10 mnkr	Enl. villkor	500 mnkr
Ansvar, ren förmögenhetsskada	S:t Erik Försäkring	10 basbelopp	Enl. villkor	10 mnkr
Byggherreansvar	S:t Erik Försäkring	3 basbelopp	Enl. villkor	10 mnkr
Byggherreansvar över 10 mnkr	Upphandlas vid behov	Varierande	Enl. villkor	Efter behov
Byggfel	Upphandlas vid behov	Varierande	Enl. villkor	Efter behov
Egendom, byggnad	S:t Erik Försäkring	3, 10 eller 30 bas-belopp	Allrisk	Fullvärde alt. Första risk
Egendom, inventarier	S:t Erik Försäkring	1 basbelopp	Allrisk	Efter behov, dock max 350 mnkr per försäkrings-ställe
Extrakostnader/ Hyresförlust	S:t Erik Försäkring	Se egendom	24 månader	Varierande -
Förmögenhetsbrott	Länsförsäkringar	1 mnkr	Enl. villkor	200 mnkr
Konsultansvar	S:t Erik Försäkring	Enl. ABK	Enl. ABK	Enl. ABK
Motorfordon	Protector	Varierande	Helförsäkring	-
Volontärförsäkring	S:t Erik Försäkring	-	Enl. villkor	Enl. villkor
Tjänsteresa	Gouda	-	Enl. villkor	Varierande
Utländska besökare	Gouda	-	Enl. villkor	Varierande
Patientförsäkring	Moderna försäkringar	Enl. villkor	Enl. villkor	Enl. villkor
VD/styrelseansvar	Protector	-	Enl. villkor	100 mnkr

Terrorism	S:t Erik Försäkring	-	Enl. villkor	2000 mnkr
Avbrott	S:t Erik Försäkring	-	Enl. villkor	5 - 400 mnkr

Stockholms Hamn AB:s hamnförsäkring tecknas externt.

4 Försäkringsbelopp

Med försäkringsbelopp i egendomsförsäkringen menas de i försäkringsbrevet angivna beloppen till vilka egendomen är försäkrad. För byggnad ska försäkringsbeloppet motsvara byggnadens nyanskaffningsvärde.

Försäkringstagaren ansvarar för att i respektive försäkringsbrev angivna försäkringsställen, försäkringsvärden och omfattning är korrekta.

5 Försäkringsform

För ***byggnad*** tillämpas någon av följande försäkringsformer:

Fullvärdeförsäkring ska normalt gälla om inte annat anges i försäkringsbrevet. I försäkringsbrevet ska anges aktuellt försäkringsbelopp.

Första riskförsäkring med angivet begränsad maximal ersättning ska gälla för vissa byggnader som inte ska återuppföras eller där det är svårt att ange ett korrekt försäkringsbelopp som motsvarar nyanskaffningsvärdet.

Helvärde kan gälla vid behov och anges då i försäkringsbrevet.

Vid behov ska försäkringen omfatta merkostnad för kulturvärde och myndighetskrav med upp till 20 MSEK i försäkringsbelopp.

Ansvarsförsäkringen gäller inte för skador som de försäkrade orsakar varandra.

För **m*askinerier/inventarier och varor*** tillämpas följande:

Helvärde ska normalt gälla om inte annat anges i försäkringsbrevet. I försäkringsbrevet ska anges aktuellt försäkringsbelopp.

IKT-RIKTLINJER I S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

Innehållsförteckning

1 Inledning

För att konkretisera strategin för informations- och kommunikationsteknik, nedan IKT, och riktlinjer som är styrande för IKT har S:t Erik Försäkrings AB, nedan Bolaget, antagit dessa riktlinjer.

Riktlinjerna är framtagna i enlighet med Eiopas riktlinjer (20/600) för säkerhet och företagsstyrning avseende IKT, nedan Eiopas IKT-riktlinjer. Cybersäkerhet inkluderas i IKT och ska därmed hanteras som en del av Bolagets allmänna hantering av IKT-risker och säkerhetsrisker.

Dessa riktlinjer omfattar samtliga anställda samt Bolagets ledning. Riktlinjerna ska kommuniceras med samtliga anställda. När det bedöms relevant ska hela eller delar av dessa riktlinjer kommuniceras till och gälla för Bolagets tjänsteleverantörer.

Bolaget tillämpar, utöver de definitioner som nämns nedan, de definitioner som anges i Eiopas IKT-riktlinjer.

Dessa riktlinjer ska ses över och revideras löpande, minst årligen.

2 Syftet med riktlinjerna

Riktlinjerna syftar till att minska de IKT-risker och säkerhetsrisker som Bolaget är exponerade för samt för att säkerställa god förberedelse för att hantera eventuella IKT- och säkerhetsincidenter.

3 Definitioner

Cyberattack	Alla former av hackande som leder till ett offensivt/skadligt försök att förstöra, exponera, ändra, deaktivera, stjäla eller få obehörig åtkomst till eller på ett obehörigt sätt använda en informationstillgång som riktar sig mot IKT-system.
Cybersäkerhet	Bevarande av konfidentialitet, integritet och tillgänglighet vad gäller information och/eller informationssystem via ett cybermedium.
IKT-tillgång	En programvaru- eller maskinvarutillgång som finns i affärsmiljön.
IKT- och säkerhetsrisk	Som en delkomponent i operativ risk; risk för förlust som beror på brott mot konfidentialiteten, på att integriteten hos system och data inte fungerar, på att system och data är olämpliga eller otillgängliga, eller på oförmåga att ändra på IKT:n inom rimlig tid och till rimliga kostnader när miljö eller verksamhetskraven förändras (dvs. flexibilitet). Detta inkluderar cyberrisker och informationssäkerhetsrisker till följd av otillräckliga eller icke-

	funktionella interna processer eller externa händelser, däribland cyberattacker eller otillräcklig fysisk säkerhet.
Informationssäkerhet	Bevarande av konfidentialitet, integritet och tillgänglighet vad gäller information och/eller informationssystem. Därtill kan även andra egenskaper vara aktuella, såsom autenticitet, ansvar, oavvislighet och tillförlitlighet.
IKT-tjänster	Tjänster som tillhandahålls via IKT-system och tjänsteleverantörer till en eller flera interna eller externa användare.
IKT-system	Uppsättning program, tjänster, it-tillgångar, IKT-tillgångar eller andra komponenter som hanterar information, vilket inkluderar driftsmiljön.
Informationstillgång	En samling uppgifter, antingen materiella eller immateriella, som är värda att skyddas.

4 Riktlinjer som behandlar IKT

Bolaget har en rad interna policyer och riktlinjer som på ett eller annat sätt berör IKT.

Bolaget är anslutna till flera tjänster och IKT-tillgångar som upphandlats genom Stockholm Stad. Därvid finns flertalet riktlinjer som behandlar olika typer av frågor rörande IKT och informationssäkerhet som är producerade av Stockholm Stad vilka också ska efterlevas av Bolaget. Dessa kan i sin tur ha påverkan på Bolagets arbete kring informationssäkerhet och IKT-strategi.

4.1 Bolagets interna riktlinjer

a) Styrelsens arbetsordning
b) Riktlinjer för intern styrning och kontroll
c) Riktlinjer för riskhantering
d) Instruktion för funktionen för riskhantering
e) Riktlinjer för internrevision
f) Riktlinjer för rapportering av händelser av väsentlig betydelse
g) Riktlinjer för hantering av personuppgifter
h) Katastrofplan
i) IT-avbrottsplan med tillhörande bilagor

4.2 Riktlinjer som delas med Stockholms stad

a) Riktlinjer för incidentrapportering
b) Policy för skyddande av personuppgifter
c) Ramverk vid anskaffning av molntjänster
d) Kryptorekommendationer
e) Handbok för informationsklassning
f) Riktlinjer för infrastruktur
g) E-strategi
h) Riktlinjer för stadens IT-infrastruktur
i) Riktlinje informationssäkerhet
j) Stockholms stads IT-program

5 Roller och ansvarsområden

5.1 Styrelsen

Bolagets styrelse har det övergripande ansvaret att fastställa och godkänna Bolagets skriftliga IKT-strategi som en del av och i överensstämmelse med Bolagets övergripande affärsstrategi. Styrelsen ansvarar också för att Bolaget har ett effektivt system för hantering av IKT-risker och säkerhetsrisker som en del av Bolagets allmänna riskhanteringssystem.

5.2 VD

Bolagets vd ansvarar för att Bolagets kartläggning och identifiering av risker utförs i enlighet med Bolagets riktlinjer för riskhantering samt där relevant, dessa riktlinjer. Vd ansvarar därutöver för den fortsatta processen med att analysera och/eller minimera identifierade IKT-risker. Arbete enligt ovan kan delegeras till annan anställd.

Bolagets vd ska säkerställa att samtliga anställda erhåller relevant information och utbildning om IKT-risker och säkerhetsrisker.

5.3 Anställda

Samtliga anställda ansvarar för att utföra sitt arbete i enlighet med fastställda riktlinjer, instruktioner och befattningsbeskrivningar. Bolagets anställda ansvarar för att rapportera eventuella incidenter i enlighet med Stockholm Stads riktlinjer för incidentrapportering.

5.4 Informationssäkerhetssamordnare

Bolaget ska ha en intern informationssäkerhetssamordnare som utgör ett stöd till Bolagets ledning i IKT-relaterade frågor och rapporterar även direkt till Bolagets styrelse och vd.

Samordnaren är ansvarig för vart och ett av Bolagens system. Denne ska löpande se över risken för avbrott eller andra störningar ur IKT-synpunkt och sköter Bolagets kontakt i dessa frågor med Stockholm Stad.

Ansvar vid eventuella avbrott framgår av Bolagets IT-avbrottsplan.

5.5 Dataskyddsombud

Bolaget ska ha ett Dataskyddsombud som löpande ska se över potentiella brister i Bolagets informationssäkerhet som kan påverka hanteringen av personuppgifter i verksamheten. Eventuella brister ska rapporteras till Bolagets vd och styrelse.

5.6 Riskhanteringsfunktionen

Bolagets funktion för riskhantering utför bl.a. sådant arbete som faller på funktion för informationssäkerhet i enlighet med EIOPA:s IKT-riktlinjer. Funktionen för riskhantering ska mot den bakgrunden bl.a.:

- utgöra ett stöd till Bolagets ledning i samband med fastställande och upprätthållande av Bolagets IKT-riktlinjer,
- regelbundet rapportera och ge vägledning om informationssäkerhetens status och utveckling,
- övervaka och granska genomförandet av informationssäkerhetsåtgärder,

- följa upp hur informationssäkerhetskrav följs upp av tjänsteleverantörer,

- följa upp anställda och ledningens kunskap och kännedom om Bolagets IKT-riktlinjer, och
- samordna granskningar av operativa incidenter eller säkerhetsincidenter och rapportera granskningar till Bolagets ledning och vd.

Det arbete som utförs inom ramen för funktion för informationssäkerhet rapporteras till Bolagets styrelse och vd.

5.7 Katastrofgrupp IT

Bolaget ska ha en katastrofgrupp med i förväg utsedda medlemmar och ersättare. De personer som ska vara med och ta beslut om alternativa rutiner, återgång till normalläge och eventuella korrigerande åtgärder ska finnas med i gruppen. Katastrofgruppens medlemmar och ansvar vid avbrott framgår i Bolagets IT-avbrottsplan.

Bolaget har även en krisledningsorganisation som består av en krisledning- och kommunikationsansvarig, administrativ funktion, samverkansfunktion samt analysfunktion. Dessa funktioners ansvar finns beskrivna i Bolagets katastrofplan.

5.8 Övriga nyckelfunktioner

I Bolagets organisation utgör vd, samtliga anställda samt vissa outsourcade verksamheter nyckelfunktioner. Bolaget har två kundansvariga, en riskhanteringsansvarig, en skadeansvarig, en bolagsjurist, en IA ansvarig och en ekonomiansvarig. Dessa samt deras ersättare anges närmare i Bolagets katastrofplan. För de aktuella tjänsterna gäller att ersättaren kanske inte fullt ut kan ta över samtliga arbetsuppgifter. Emellertid finns kompetens hos konsulter, närstående bolag och förvaltningar i staden som kan utnyttjas.

Roller och ansvarsområden inom Stockholms stad finns angivna i Stockholms stads riktlinjer för informationssäkerhet. Till stöd för stadens säkerhetsarbete och för kommunfullmäktiges mål om en trygg och säker stad finns ett strategiskt riskhanteringsråd, som bland annat hanterar frågor som rör informationssäkerhet. Informationssäkerhetschefen, som är placerad på stadsledningskontoret, samordnar aktiviteter inom informationssäkerhet över hela staden och är rådgivare för förvaltningar och bolag.

Utöver ovan har Bolaget centrala funktioner som bevakar IKT-risker ur olika perspektiv. Respektive funktions uppdrag och ansvar finns beskrivna i separat riktlinjer och varje funktion rapporterar direkt till Bolagets styrelse och vd.

6 IKT-strategi

Bolaget ska regelbundet analysera arbetet för att upprätthålla god informationssäkerhet samt ha en IKT-strategi. Strategi och analys finns dokumenterat i bilaga 1.

7 Utkontraktering m.m.

7.1 Upphandling och utkontraktering

Bolaget ska inför nya upphandlingar och utläggning av verksamhet ta eventuella IKT-risker i beaktande. Bolaget ska identifiera och ställa de krav som Bolaget anser nödvändiga för att Bolagets information ska hanteras säkert hos den externa leverantören.

Bolagets styrelse har antagit separata riktlinjer för dels upphandling, dels utlagd verksamhet. Vid kravställande ska Bolaget beakta vilken möjlighet som ges till olika former av granskningar av leverantörens säkerhetskrav. Detta kan avse exempelvis rätten till revision, krav på åtkomst till resultat av leverantörens egenkontroller eller externa granskningar initierade av leverantören själv, stöd från leverantören vid granskningar, Finansinspektionens rätt till insyn etc.

7.2 Beroende gentemot tjänsteleverantörer

När IKT-tjänster och IKT-system utkontrakteras ska Bolaget se till att relevanta krav för sådana tjänster och system uppfylls, utan att det påverkar tillämpningen av dessa interna IKT-riktlinjer samt EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer.

I de fall kritiska eller viktiga funktioner utkontrakteras ska Bolaget se till att tjänste-leverantörens avtalsförpliktelser omfattar krav på innehåll i sådana avtal enligt EIOPA:s IKT-riktlinjer samt EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantörer.

Vid hantering av tredjepartsleverantörer ska Bolaget även beakta Stockholms stads riktlinjer för informationssäkerhet.

Vid utkontraktering till en molntjänstleverantör ska Bolaget även beakta Stockholms stads ramverk vid anskaffning av molntjänster.

8 Riskhanteringsprocess

Bolaget ska regelbundet genomföra en kartläggning över Bolagets affärsprocesser och affärsverksamheter, affärsfunktioner, roller och tillgångar (t.ex. informationstillgångar och IKT-tillgångar). Syftet med kartläggningen är att identifiera deras betydelse och ömsesidiga beroendeförhållanden beträffande IKT-risker och säkerhetsrisker.

Hantering av IKT-risker och säkerhetsrisker ska vara en del av Bolagets allmänna riskhanteringssystem och riskhanteringsprocess som finns beskrivet i Bolagets interna riktlinjer för riskhantering. Detta inbegriper att, i enlighet med Bolagets riskstrategi, fastställa risktolerans för IKT-risker och säkerhetsrisker. IKT-risker ska inkluderas i Bolagets riskregister som tas fram Bolaget tillsammans med funktionen för riskhantering.

9 Logisk säkerhet

9.1 Behörighetstilldelning och åtkomsträttigheter

Bolaget ska hantera åtkomsträttigheter, däribland fjärråtkomst till informationstillgångar och deras stödsystem utifrån behovsenlig behörighet. Bolaget tillämpar principen om begränsad behörighet innebärande att anställda och tredjepartsleverantörer endast beviljas de åtkomsträttigheter som är nödvändiga för att utföra arbetsuppgifterna.

Ansvar för behörighetstilldelning och åtkomsträttigheter ligger på Bolagets vd. Beviljad behörighet och åtkomsträttigheter ska dokumenteras. Behörighet och åtkomsträttigheter bör ses över regelbundet för att säkerställa att anställda och tredjepartsleverantörer inte har för omfattande rättigheter och att åtkomsträttigheter upphävs/tas bort om de inte längre behövs.

9.2 Fjärråtkomst och autentiseringsmetoder

Fjärradministratörsåtkomst till kritiska IKT-system ska endast beviljas utifrån behovsenlig behörighet och förutsatt att starka autentiseringslösningar används. Bolaget tillämpar för närvarande dubbel autentiseringslösning genom att fjärråtkomst endast ges genom användande av säkerhetskort i kombination med en lösenordskod eller annan motsvarande säkerhetslösning.

9.3 Loggning

Möjlighet för Bolaget att logga all användaraktivitet kravställs inför att Bolaget tar in nya system. I dagsläget tillämpas rutiner för loggning av användaraktivitet i samtliga av Bolagets system.

10 Fysisk säkerhet

Bolaget ska skydda lokaler, IT-utrustning och känsliga områden från obehörigt tillträde och från miljöfaror. För detta ändamål har Bolaget vidtagit säkerhetsåtgärder i form av skalskydd, branschnormer för stöldskydd och brand, lås och larm, lösenordsskydd och tillträdeskontroll. Utrustning, särskilt stöldbegärlig, ska vara märkt så att den kan identifieras.

Stöldskyddsmärkningen ska utformas så att den är svår att avlägsna. Vidare ställer Bolaget fysiska säkerhetskrav vid upphandlingar. Fysisk och miljörelaterad säkerhet återges i sin helhet i Stockholms stads riktlinjer för informationssäkerhet.

Fysisk åtkomst till IKT-system ska endast beviljas behöriga personer i enlighet med avsnitt 9.1 ovan. Behörighet ska tilldelas i enlighet med personens uppgifter och ansvarsområden och begränsas till personer som har lämplig utbildning och som övervakas på ett lämpligt sätt. Fysisk åtkomst bör ses över regelbundet för att säkerställa att onödiga åtkomsträttigheter snabbt tas bort om de inte längre behövs.

11 IKT-säkerhet

Genom vad som nämns ovan i dessa riktlinjer samt genom redan befintliga riktlinjer nämnda i avsnitt 4 har Bolaget infört rutiner för att säkerställa konfidentialitet, integritet och tillgänglighet.

Bolaget har därtill processer för att förhindra säkerhetsincidenter i IKT-system och IKT-tjänster, samt att om de inträffar minimera effekten på IKT-leveransen.

Då hela Bolagets IT-infrastruktur är placerad i Stadens struktur, är det stadens riktlinjer och åtgärder som gäller för Bolaget.

Mot bakgrund av att Bolaget är en del av Stockholms stad ingår Bolaget i Stockholms stads avtal med Leverantör avseende systemdrift och systemförvaltning av stadens centrala verksamhetssystem. Genom detta avtal tillgodoses för verksamhetssystemen hög grad av tillgänglighet, driftssäkerhet, tillförlitlighet och säkerhet. Inom ramen för detta avtal finns specifika och omfattande riktlinjer för informationssäkerhet som Leverantören är bunden av. Till avtalet hör också beskrivning av säkerhetskrav och därav ingående aktiviteter i IT-säkerhetsarbetet, hur sekretessbelagda handlingar ska hanteras samt krav på kommunikationslösningar och krisberedskap. Verksamheten kontrolleras regelbundet av Bolaget i enlighet med avsnitt 7 ovan.

Avseende Bolagets verksamhetssystem ansvarar Bolaget för att uppdatera systemens tekniska och säkerhetsmässiga plattform, och genomföra nödvändiga uppgraderingar. När det emellertid gäller uppgradering av servrar där Bolagets system huserar, är det stadens ansvar att implementera relevanta säkerhetsuppdateringar och tillse att nödvändiga uppgraderingar sker. Bolaget ska regelbundet säkerställa att sådana uppdateringar utförs på ett korrekt sätt.

Gällande informationsklassning tillämpar Bolaget stadens handbok för informationsklassning.

12 Granskning, bedömning och testning

Bolagets centrala funktioner ska regelbundet och ur olika synvinklar granska och bedöma Bolagets arbete med IKT. Vid behov ska Bolaget utföra stresstester som validerar tillförlitligheten och effektiviteten hos Bolagets informationssäkerhetsåtgärder och säkerställer att Bolaget tar hänsyn till de hot och sårbarheter som har identifierats genom hotövervakning samt riskbedömningsprocessen för IKT-risker och säkerhetsrisker. Testerna ska vidare identifiera eventuella svagheter, överträdelser och incidenter vad gäller säkerheten. Sådana tester ska utföras av oberoende personer med ändamålsenlig kunskap och kompetens.

System tillhandahållna genom Stockholm Stad testas regelbundet i egen regi. Bolaget avser att regelbundet kontrollera att sådana tester utförs samt efterfråga information om incidenter, skador eller annat som kan påverka Bolagets informationssäkerhetsarbete.

13 Revision

Bolagets styrning, system och processer för IKT-risker och säkerhetsrisker ska vid behov genomgå revision. Är systemet kritiskt ska revision utföras minst årligen. Sådan revision ska utföras av revisorer eller motsvarande med tillräcklig kunskap, kompetens och expertis inom IKT-risker och säkerhetsrisker för att kunna lämna en oberoende försäkran om deras effektivitet till Bolagets styrelse och vd.

Bolaget ska vidare säkerställa löpande att nödvändig revision av system tillhandahållna genom Stockholms stad utförs.

14 Hantering av incidenter och IT-avbrott

Bolaget har i befintliga interna riktlinjer samt genom Stockholms stads riktlinjer, rutiner för bl.a. spårning, loggning, klassificering och analys av incidenter och IT-avbrott.

15 Utbildning

Bolaget ska regelbundet utbilda all personal och ledning om informationssäkerhet och IKT-risker. Bolaget ska eftersträva en hög medvetenhet kring informationssäkerhet, IKT-risker och säkerhetsrisker i syfte att minska antalet fel som beror på den mänskliga faktorn, stölder, bedrägerier, felaktig användning och förluster.

Bilaga 1

1 Informations- och kommunikationsstrategi

Informations- och kommunikationsteknologi, nedan IKT, är en viktig och integrerad del av S:t Erik Försäkrings AB:s, nedan Bolaget, verksamhet. Informations- och kommunikationsflödet inom Bolaget sker övervägande digitalt och är ständigt accelererande. Med detta ökar komplexiteten inom IKT och det följer större krav på att säkerställa ändamålsenlig säkerhet och företagsstyrning avseende IKT.

Informationssäkerhet handlar om styrning av skydd till lämplig nivå för varje informationsmängd, inklusive styrning av utformningen av fysiskt skydd. Bolaget eftersträvar ett systematiskt IKT- och informationssäkerhetsarbete som bygger på att säkerhetsåtgärder ska vidtas utifrån de risker verksamhetens IKT- och informationshantering är utsatta för. Bolagets fysiska skydd motsvarar därmed de krav som kommer fram i Bolagets riskanalys och informationsklassningar. Sammanfattningsvis är det Bolagets behov som ska styra skyddsnivån.

Mot bakgrund av ovan och som en del i Bolagets IKT-strategi har Bolagets styrelse antagit interna riktlinjer för IKT. I dessa riktlinjer finns bl.a. beskrivet hur Bolaget är organiserat, vilka IKT-system Bolaget använder och hur nyckelberoenden gentemot Bolagets tjänsteleverantörer ska hanteras.

Som en del i IKT-strategin avser Bolaget att kontinuerligt utbilda Bolagets anställda och ledning i IKT-relaterade frågor och att upprätthålla en god medvetenhet kring IKT-risker. Detta syftar till att minimera risken för att potentiella incidenter, cyberattacker och intrång inträffar samt för att minimera eventuella skador.

Utöver ovan är en viktig del i Bolagets IKT-strategi är att kartlägga och identifiera IKT-risker inom ramen för riskhanteringsprocessen i syfte att kunna möta riskerna med ändamålsenligt skydd och förhindra att incidenter inträffar. Inom ramen för riskhanteringsprocessen ska Bolaget regelbundet analysera IKT- och säkerhetsrisker samt de åtgärder Bolaget vidtar för att säkerställa god hantering av IKT. Sådana analys ses över löpande och följer nedan.

2 Analys

Bolaget ska minst årligen genomföra och uppdatera verksamhetsanalys, omvärldsanalys och riskanalys hänförlig till informationssäkerhet och där tillhörande risker.

2.1 Verksamhetsanalys

Bolaget har den 1 oktober 2021 hållit en workshop för att närmare analysera verksamheten ur informationssäkerhetssynpunkt och därvid kartlagt Bolagets och andra intressenters behov, förväntningar och förutsättningar vilka behöver beaktas vid utformning av informations-säkerhetsarbetet och dess styrning. Bolaget har utarbetat såväl kontinuitets- som beredskaps-planer för att i största möjliga mån säkerställa driften av viktiga system i verksamheten. Det kan dock konstateras att verksamheten utan större problem skulle kunna fungera trots att vitala system under viss tid ligger nere, såsom exempelvis skadereglering kan dokumenteras manuellt och en okulär besiktning kräver inte nödvändigtvis digitala hjälpmedel. Sådant arbete fordrar emellertid visst efterarbete i form av att registrera dokumentation i Bolagets olika system.

Vidare utvisar verksamhetsanalysen att Bolaget är beroende av andra verksamhetsutövare i form av såväl tjänsteleverantörer som leverantörer av utkontrakterade tjänster. Mot bakgrund av att Bolaget är tillståndspliktigt ställs redan en mängd krav på Bolaget avseende uppföljning av utlagd verksamhet. Således gör Bolaget bedömningen att uppföljningsarbetet inte nämnvärt kommer förändras eller behöva förstärkas, dock avser Bolaget att utöka kravställandet i så måtto att Bolaget även fångar upp leverantörers hantering och beredskap rörande frågor om informationssäkerhet.

Bolagets styrelse har konstaterat att ett avbrott i något av Bolagets kritiska system, inte får föreligga i mer än maximalt en vecka. För mer information om hanteringen vid eventuella avbrott, se Bolagets kontinuitetsplan.

Samtliga Bolagets identifierade IKT-tillgångar återfinns i bilaga 2.

2.2 Omvärldsanalys

Vid workshopen identifierade vidare Bolaget vilka rättsliga krav som stipuleras för verksamheten och hur dessa påverkar Bolagets informationssäkerhetsarbete. Vid tillfället för analysen kunde det konstateras att Bolaget, utöver Dataskyddsförordningen, träffas av en mängd näringsrättsliga regler såsom försäkringsrörelselagen och lagen om försäkrings-distribution. Därtill ska i sammanhanget särskilt nämnas EIOPA:s riktlinjer för säkerhet och företagsstyrning avseende informations- och kommunikationsteknik samt EIOPA:s riktlinjer för uppdragsavtal med molntjänstleverantörer.

Bolaget kunde vid omvärldsanalysen konstatera att det finns mycket god beredskap för att hantera de rättsliga krav som ställs och kommer att ställas även i framtiden. I denna del har Bolaget stöd av Bolagets funktion för regelefterlevnad som utför löpande omvärldsbevakning och rapporterar direkt till Bolagets styrelse och vd om relevanta regelverk.

De rättsliga kraven omfattar vidare uppföljning av tjänsteleverantörer och leverantörer av utlagd verksamhet, vilket omnämns under avsnitt 2.1 ovan.

2.3 Riskanalys

Riskanalysen ska löpande identifiera IKT-risker och utförs verksamhetsövergripande.

Riskerna avseende informationssäkerheten tas fram genom en systematisk och kreativ process, där riskerna och potentiella händelser som kan leda till negativa konsekvenser ska beskrivs. Dessa bedöms sedan med avseende på sannolikheten att de inträffar samt konsekvensens allvar ifall de skulle inträffa. Riskhanteringsprocessen beskrivs närmare i Bolagets riktlinje för riskhantering. Bolaget har i denna del stöd av Bolagets funktion för riskhantering som rapporterar direkt till Bolagets styrelse och vd.

Närmare information för hur ovan nämnda risker hanteras samt Bolagets riskaptit för IKT-risker, återfinns i Bolagets riktlinje för riskhantering.

Bilaga 2

IKT-tillgångar

Med IKT-tillgångar avses en programvaru- eller maskinvarutillgång som finns i Bolagets affärsmiljö. De verksamhetssystem som Bolaget använder är:

a) IA (incidentrapporteringssystem)
b) INSMAN (försäkringssystem)
c) Outlook (E-post)
d) Microsoft Office (kontorssystem)
e) Telefonväxel/mobil
f) Agresso (ekonomisystem)
g) VISMA Agda (lönesystem)
h) www.sterikforsakring.se - Ombraco
i) Tieto
j) Primona
k) eDok

Affärsprocesser

- Försäkringsprocess
- Skadehanteringsprocess
- Återförsäkringsprocess
- Kapitalförvaltningsprocess

Affärsverksamhet

- Försäkring

INSTRUKTION FÖR S:T ERIK FÖRSÄKRINGS AB:S FUNKTION FÖR RISKHANTERING

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Inledning och syfte

Denna instruktion har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Instruktionen är föremål för revidering och skall fastställas årligen av styrelsen för S:t Erik Försäkrings AB.

Instruktionens syfte är att säkerställa att riskhanteringsfunktionens ansvar, uppgifter och befogenheter är tydliga och att funktionen därmed kan säkerställa att ett effektivt riskhanteringssystem införts inom bolaget.

2 Riskhanteringsfunktionens roll

Riskhanteringsfunktionen övervakar bolagets samlade riskexponering (riskprofil) och verkar för att effektivisera riskhanteringssystemet. Riskhanteringsfunktionen ska informera bolagets styrelse och ledning om bolagets risker i en samlad form.

Riskhanteringsfunktionen är operativt underställd VD men ska verka självständigt, utan inverkan från VD eller verksamhet i sina bedömningar av de risker som hanteras och övervakas i funktionens arbete. Styrelsen fastställer funktionens övergripande arbetsplan.

Riskhanteringsfunktionen har rätt att närvara vid styrelsens möten för att avlägga rapporter. Riskhanteringsfunktionen har rätt att få tillgång till all information som är nödvändig för att fullgöra arbetet.

Riskhanteringsfunktionen ska ge en samlad, allsidig och saklig bild av bolagets väsentliga risker och ska analysera och övervaka riskutvecklingen, särskilt ska funktionen bevaka och rapportera framväxande risker. Funktionen ska i analysen väga in och bedöma all information eller rapporter som är relevanta för utvärderingen av riskprofil och riskhanteringssystem. Det innefattar information även från ekonomi-, aktuarie- och regelefterlevnadsfunktionerna. Riskhanteringsfunktionen ska särskilt samarbeta nära med aktuarien.

Riskhanteringsfunktionens uppgifter inbegriper:

1. Assistera styrelse, VD och övrig verksamhet i utformningen av riskhanteringssystemet

2. Övervaka och utvärdera riskhanteringssystemet samt föreslå förändringar när så anses erforderligt

3. Övervaka riskprofilen

4. Avlägga detaljerade rapporter om bolagets riskexponeringar till styrelse och VD

5. Lämna råd till styrelse, VD och övrig verksamhet i riskhanteringsfrågor, exempelvis vid utformning strategi, förändringar i verksamhetens inriktning och vid beslut om större projekt eller investeringar.

6. Identifiera och bedöma framväxande risker

7. Driva ORSA-processen och sammanställa ORSA-rapport enligt Policy för ORSA

3 Särskilda uppgifter

3.1 Riskregister

Riskhanteringsfunktionen ska föra det riskregister som anges i Riktlinjer för riskhantering i S:t Erik Försäkrings AB, och tillse att det uppdateras minst årligen.

3.2 Incidenter

Verksamheten ska rapportera incidenter i Stockholms stads incidentrapporteringssystem. Riskhanteringsfunktionen ska stödja verksamhetens arbete att utarbeta förbättringsåtgärder utifrån inträffade incidenter. Funktionen ska minst årligen följa upp att åtgärder vidtagits.

3.3 Aktivitetsplan

Riskhanteringsfunktionen skall till årets sista styrelsemöte föreslå en aktivitetsplan för nästkommande år att fastställas av styrelsen.

3.4 Rapporter

Riskhanteringsfunktionen ansvarar för att

- omedelbart rapportera identifierade akuta risker och incidenter till ledning och styrelse,
- avlägga regelbundna rapporter enligt nedan

3.4.1 Sammanfattande riskrapport

Riskhanteringsfunktionen ska, med av styrelsen i årsplanen beslutat intervall samt vid behov, sammanställa en skriftlig sammanfattande riskrapport. Rapporten ska ge en detaljerad, allsidig och saklig bild av bolagets samtliga väsentliga risker inklusive deras förändring och eventuella framväxande risker.

Riskrapporten ska väga in information från aktuariefunktionen och funktionen för regelefterlevnad, riskhanteringsfunktionens egna bedömningar av denna information samt övrig relevant information.

Riskrapporten ska tillställas styrelse och VD.

3.4.2 Årsrapport

Riskhanteringsfunktionen ska årligen sammanställa en skriftlig rapport som beskriver arbetet under året och redogör för hur den av styrelsen fastställda årsplanen samt övriga uppgifter enligt denna instruktion, särskilt kontrollerna enligt avsnitt 3.5 nedan, genomförts.

Årsrapporten ska tillställas styrelse och VD och även föredras muntligen för styrelsen.

3.4.3 Incidentrapport

Riskhanteringsfunktionen skall till årets sista styrelsemöte sammanställa en skriftlig incidentrapport med en samlad analys av inträffade incidenter, uppföljning av vidtagna åtgärder och förslag till ytterligare förbättringar. Rapporten skall tillställas styrelse och VD.

3.5 Kontroller

Riskhanteringsfunktionen ska löpande kontrollera att riskanalyser utförts tillfredsställande inför outsourcing respektive affärsbeslut. Verksamheten ansvarar för att genomföra och tillhandahålla riskanalys för uppdragsavtal respektive affärsbeslut.

Riskhanteringsfunktionen ska årligen kontrollera riskregistret har uppdaterats under året och att det uppfyller kraven enligt Riktlinjer för riskhantering i S:t Erik Försäkrings AB.

Riskhanteringsfunktionen ska löpande kontrollera att incidenter rapporteras på ett korrekt vis och årligen kontrollera att beslutade åtgärder relaterade till incidenter har vidtagits.

INSTRUKTION FÖR FÖRANDE AV FÖRMÅNSRÄTTSREGISTER

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Instruktionen ska fastställas årligen av styrelsen och revideras vid större förändringar av S:t Erik Försäkrings AB:s förutsättningar.

Syftet med policyn är att ange hur arbetet med förande av förmånsrättsregister ska ske så det vid varje tidpunkt kan användas för att fastställa den särskilda förmånsrätt som följer av 6 kap. 13§ Försäkringsrörelselagen.

2 Registeransvarig

VD ansvarar för att det förs ett förmånsrättsregister, att det hålls löpande uppdaterat och att rapportering sker i enlighet med denna instruktion.

VD kan delegera det faktiska förandet av förmånsrättsregister till annan för uppgiften lämpad person, men ansvarar även då enligt ovan.

3 Förmånsrättsregister

3.1 Allmänt

Då S:t Erik Försäkring inte tillhandahåller tjänstepension finns endast ett förmånsrättsregister. Registret innehåller de tillgångar som täcker skulden för de garanterade försäkringstekniska avsättningarna för egen räkning och innehåller information enligt nedan.

3.2 Innehåll i förmånsrättsregistret – tillgångar

Förmånsrättsregistret ska innehålla information om tillgångar som motsvarar följande avsättningar:

- Garanterad återbäring och garanterade försäkringsåtaganden
- Villkorad återbäring och försäkringsåtaganden där försäkringstagaren står risken
- Försäkringstekniska avsättningar

Följande information ska finnas avseende varje individuell tillgång:

- ISIN-kod
- Eventuell annan identifikationskod
- Antal/nominellt belopp
- Var förvaring av värdepapper sker (depå, värdepapperskonto eller dylikt)
- Emittent/utfärdare
- Aktuellt verkligt värde i SEK
- Datum för värde
- Notering om pantsättning till förmån för annan än försäkringstagaren
- Vilken valuta innehavet är noterat i
- Valutakurs (om valutan ej är i SEK) använt för värdering
- Klassificering av innehavet – geografiskt

- Klassificering av innehavet – tillgångsslag

3.3 Innehåll i förmånsrättsregistret – försäkringstekniska avsättningar

S:t Erik Försäkrings aktuarie lämnar uppgift om värdet på de garanterade försäkringstekniska avsättningarna för egen räkning med tillägg av värdet av en reservdeposition. Normalt lämnas dessa uppgifter månadsvis. Vid behov kan S:t Erik Försäkring begära uppgift om detta vid andra tidpunkter exempelvis vid inträffade skador av större omfattning eller av annan anledning. Aktuarien gör löpande en översyn över lämplig fördelning av de försäkringstekniska avsättningarna i rapporteringen. Utdrag ur registret kan vid behov göras vid var tidpunkt.

3.4 Förvaring av förmånsrättsregister

Förmånsrättsregistret förvaras i elektronisk form på S.t Erik Försäkrings server. Back-up tas löpande på registret. Registret tillhandahålls på lämpligast möjliga sätt, elektroniskt eller i pappersform, till Finansinspektionen vid begäran.

3.5 Avstämning av förmånsrättsregister

Registret ska månadsvis stämmas av mot uppgifter om tillgångar hos det förvaringsinstitut för värdepapper respektive bankkonto för likvida medel, som S:t Erik Försäkring använder för att förvara tillgångarna.

4 Rapportering

S:t Erik Försäkring upprättar månadsvis en registerrapport. Rapporten visar värdet på tillgångarna i förmånsrättsregistret och värdet på den skuld som ska täckas. Ansvarig för denna rapportering är registeransvarig. Vid exempelvis större förändringar i marknadsräntor som påverkar tillgångarna eller vid inträffade skador av större omfattning eller vid annan förändring som föranleder misstanke om att tillgångarna påverkats i större omfattning, ska sakbolaget omgående upprätta en rapport för att kontrollera att tillgångarna är tillräckliga för att täcka skulden.

Om värdet på tillgångarna beräknas att inte uppgå till minst 110% av skulden ska detta omedelbart rapporteras till VD, styrelsen, samt funktionerna för regelefterlevnad och riskhantering. Åtgärder ska då vidtas för att förhindra att tillgångarna kommer att understiga skulden.

Om tillgångarna beräknas understiga 100 % av skulden ska den registersansvarige omedelbart rapportera detta till (VD och) styrelsen som ansvarar för att omedelbart informera Finansinspektionen. Detsamma gäller om förmånsrättsregistret inte längre förs eller kan föras på kvalitétssäkert sätt. Regelefterlevnads- och riskhanteringsfunktionen ska informeras samtidigt.

4.1 Principer för värdering av förmånsrättstillgångar

Värdering av förmånsrättstillgångarna sker i enlighet med verkligt värde enligt 5 kap. 2§ FRL. Med detta avses det värde som utgör en marknadsanpassad värdering (det belopp till vilket det kan överlåtas till annan oberoende part) vid realiseringstillfället.

Principerna för värdering framgår i övrigt av ”Riktlinje för värdering av tillgångar och skulder, kapitalbas och finansieringsplan på medellång sikt”

4.2 Principer för beräkning av försäkringstekniska avsättningar

Principerna för beräkning och värdering av de försäkringstekniska avsättningarna framgår av bolagets ”Processbeskrivning – Beräkning av försäkringstekniska avsättningar”.

INSTRUKTION FÖR HANTERING AV S:T ERIK FÖRSÄKRINGS AB:s RAPPORTERING TILL FINANSINSPEKTIONEN

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Denna instruktion har upprättats mot bakgrund av de rapporteringsregler som S:t Erik Försäkrings AB, nedan benämnt Bolaget, och som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna revideras löpande av ekonomifunktionen och skall fastställas minst årligen av styrelsen. VD beslutar om och uppdaterar löpande de underliggande dokumenten för ansvar och validering.

Syftet med instruktionen är att klargöra vilka rapporteringar som ska ske, ansvaret för dessa samt hur de beslutas.

Bolaget ska inge rapporter till Finansinspektionen med uppgifter innehållande bl.a. uppgifter om Bolagets ekonomiska ställning. Den regelbundna tillsynsrapporteringen består av en kvalitativ årsrapport som benämns redogörelse för verksamheten, nedan benämnd RSR, samt kvantitativa mallar för års- och kvartalsrapporter, nedan benämnd QRT. Den publika solvens- och verksamhetsrapporten, nedan benämnd SFCR), består också av en kvalitativ och en kvantitativ del.
En övergripande rutinbeskrivning av den kvantitativa rapporteringen framgår av ”Rutinbeskrivning vid kvantitativ Solvens II-rapportering”[1].

2 Årsvis information

2.1 Regelbunden tillsynsrapport - RSR

Bolaget ska årligen lämna en rapport till Finansinspektionen som redogör för verksamheten, så kallad RSR-rapport.

2.1.1 Periodicitet

Årligen enligt Kommissionens delegerade förordning EU (2015:35), FFFS 2015:21 och 2016:5.

Ingående del-QRT ska valideras senast 2 veckor innan styrelsens beslut och rapporten som helhet vara validerad och klar för utskick till styrelsen senast 1 vecka innan styrelsens beslut.

2.1.2 Innehåll

Innehållet i RSR-rapporten framgår av rättsreglerna under p1 samt av ”Projektplan S2”[2] Vart tredje år ska denna vara fullständig medan den mellanliggande år endast ska belysa materiella förändringar inom de områden som rapporten ska beskriva.

2.1.3 Ansvarig

Ansvarig för att rapportering sker är ekonomifunktionen. Ansvarig för ingående delar framgår av ”Projektplan S2”[2].

2.1.4 Kontroll

VD kontrollerar att rapporten upprättats och är korrekt samt att den rapporteras.

[1] G/1.4/Arbetsområden/ Styrdokument/Instruktion FI rapportering
[2] G/i.4/Arbetsområden/Rapportering

2.1.5 Beslut

Rapporten ska tillställas styrelsen för beslut innan den rapporteras. Av underlaget ska utförda kontroller framgå.

2.2 Solvens- och verksamhetsrapport - SFCR

Bolaget ska årligen offentliggöra en solvens- och verksamhetsrapport, så kallad SFCR-rapport. Om vissa betydande utvecklingar inträffat ska den uppdateras och återigen offentliggöras. SFCR-rapporten innehåller kvalitativa och kvantitativa upplysningar, varav vissa kvantitativa upplysningar ska lämnas enligt fördefinierade format.. Denna rapport ska rapporteras in till Finansinspektionen när företaget publicerar den på sin hemsida.

2.2.1 Periodicitet

Årligen samt vid behov av uppdatering enligt Kommissionens delegerade förordning EU (2015:35), FFFS 2015:21 och 2016:5.

Ingående del-QRT ska valideras senast 2 veckor innan styrelsens beslut och rapporten som helhet vara validerad och klar för utskick till styrelsen senast 1 vecka innan styrelsens beslut.

2.2.2 Innehåll

Innehållet i SFCR-rapporten framgår av rättsreglerna under p1, Kommissionens genomförandeförordning (EU) 2015/2452, samt av ”Projektplan S2”[3]

2.2.3 Ansvarig

Ansvarig för att rapportering sker och att den offentliggörs är ekonomifunktionen. Ansvarig för ingående delar framgår av ”Projektplan S2”[3].

2.2.4 Kontroll

VD kontrollerar att rapporten upprättats, offentliggjorts och är korrekt samt att den rapporteras.

2.2.5 Beslut

Rapporten ska tillställas styrelsen för beslut innan den rapporteras. Av underlaget ska utförda kontroller framgå.

2.3 Årsrapport – QRT

En kvantitativ rapport – uppgifter i siffror. Tillhör den EU-gemensamma rapporteringen..

2.3.1 Periodicitet

Årligen enligt Kommissionens genomförandeförordning (EU) (2015/2450), FFFS 2015:21 och 2016:5.

Ingående del-QRT ska valideras senast 2 veckor innan styrelsens beslut och rapporten som helhet vara validerad och klar för utskick till styrelsen senast 1 vecka innan styrelsens beslut.

[3] G/i.4/Arbetsområden/Rapportering

2.3.2 Innehåll

Innehållet i den årliga QRT-rapporten framgår av rättsreglerna under p1samt av ”Validering årsrapportering”[4].

2.3.3 Ansvarig

Ansvarig för att rapportering sker är ekonomifunktionen. QRT-ansvariga framgår av ”Validering årsrapportering”[4].

2.3.4 Kontroll

VD kontrollerar att rapporten upprättats och är korrekt samt att den rapporteras. Validering av ingående del-QRT framgår av ”Validering årsrapportering”[4].

2.3.5 Beslut

Rapporten ska tillställas styrelsen för beslut innan den rapporteras. Av underlaget ska utförda kontroller framgå.

2.4 Risk- och solvvensbedömning – ORSA

Bolaget ska i enlighet med 10 kap. 13 § försäkringsrörelselagen rapportera resultatet av egen risk- och solvensbedömning, så kallad ORSA, till Finansinspektionen. ORSA ska vara en integrerad del i affärsstrategin och ska beaktas vid varje strategiskt beslut. Rapportering sker genom en tillsynsrapport som beskriver ORSA.

2.4.1 Periodicitet

2 veckor efter att styrelsen fastställt ORSA enligt Kommissionens delegerade förordning EU (2015:35), FFFS 2015:21 och 2016:5.

2.4.2 Innehåll

ORSA:s innehåll framgår av den ORSA-policy som bolaget fattat beslut om samt 10 kap. 13§ Försäkringsrörelselagen, Kommissionens delegerade förordning (EU) 2015/35 samt Guidelines från EIOPA 14/259.

2.4.3 Ansvarig

VD ansvarar för att utarbetande av och rapportering av ORSA sker.

2.4.4 Kontroll

Kontroller sker enligt ORSA-policy.

2.4.5 Beslut

Rapporten ska tillställas styrelsen för beslut innan den rapporteras. Av underlaget ska utförda kontroller framgå.

2.5 Ägares kvalificerade innehav och ägarintressen

Bolaget ska lämna uppgifter till Finansinspektionen om ägares kvalificerade innehav samt uppgifter om regelansvarig och klagomålsansvarig.

[4] G/2.3.3.13/Årsrapportering/QRT

2.5.1 Periodicitet
Årligen, senast den 30 juni, samt så snart registrerade förhållanden har ändrats, se FFFS 2011:14.

2.5.2 Innehåll
Innehållet framgår av FFFS 2011:14.

2.5.3 Ansvarig
Ansvarig för att rapportering sker är ekonomifunktionen.

2.5.4 Kontroll
VD kontrollerar att rapporten upprättas och är korrekt samt att den rapporteras.

2.5.5 Beslut
VD fattar beslut om rapportering.

2.6 Rapportering av betydande transaktioner inom en grupp
S:t Erik Försäkrings AB ägs av Stockholms Stadshus AB som är ett försäkringsholdingföretag med blandad verksamhet.

I enlighet med 19 kap. 2 §fjärde stycket försäkringsrörelselagen (201 0:2043), FRL, ska grupptillsyn enligt 19 kap. 41 § FRL utövas över försäkringsföretag vars moderföretag är ett försäkringsholdingföretag med blandad verksamhet. Sådana försäkringsföretag ska enligt 19 kap. 41 § FRL ha en god kontroll över transaktioner med försäkringsholdingföretaget med blandad verksamhet och dess andra anknutna företag. Vid Finansinspektionens tillsyn över detta krav gäller 19 kap. 37 § FRL i tillämpliga delar.

Finansinspektionen ska för varje enskild grupp besluta vilka slag av transaktioner som är betydande respektive mycket betydande. Finansinspektionen ska också besluta om lämpliga tröskelvärden.

2.6.1 Periodicitet
Betydande transaktioner av vissa slag inom gruppen ska minst årligen rapporteras till Finansinspektionen. Transaktioner som har en mycket betydande omfattning ska rapporteras snarast möjligt.

2.6.2 Innehåll
Enligt årligt beslut från Finansinspektionen.

2.6.3 Ansvarig
Ansvarig för att rapportering sker är ekonomifunktionen.

2.6.4 Kontroll
VD kontrollerar att rapporten upprättas och är korrekt samt att den rapporteras.

2.6.5 Beslut
VD fattar beslut om rapportering.

3 Kvartalsvis information

3.1 Kvartalsrapport – QRT

Kvantitativ rapport.

3.1.1 Periodicitet

Kvartalsvis enligt Kommissionens genomförandeförordning (EU) 2015/2450, FFFS 2015:21 och 2016:5.

Ingående del-QRT ska valideras senast 2 veckor innan VD:s beslut och rapporten som helhet vara validerad och klar för utskick till VD senast 1 vecka innan VD:s beslut.

3.1.2 Innehåll

Rapportens innehåll framgår av FRL, Kommissionens genomförandeförordning (EU) 2015/2450, EIOPA Guideline 15/109 samt FFFS 2015:13, 2015:21, 2016:4 och 2016:5 samt av ”Validering Q1-4”[5].

3.1.3 Ansvarig

Ansvarig för att rapportering sker är ekonomifunktionen. QRT-ansvariga framgår av ”Validering Q1-4”[5].

3.1.4 Kontroll

VD kontrollerar att rapporten upprättats och är korrekt samt att den rapporteras. Validering v ingående del-QRT framgår av ”Validering Q1-4”[5].

3.1.5 Beslut

VD fattar beslut om rapportering.

4 Kompletterande nationell rapportering

Av FFFS 2015:13, 2016:4 framgår att skadeförsäkringsbolag med en balansomslutning som understiger 1000 MSEK, ska utföra kompletterande nationell rapportering som följer:

4.1 Rapporter

Årliga och kvartalsvisa rapporter till Finansinspektionen.

4.1.1 Periodicitet

Årlig och kvartalsvis rapportering enligt Kvartalsvis rapportering enligt FFFS 2015:13, 2015:21, 2016:4, 2016:5.

4.1.2 Innehåll

Innehållet i rapporteringen framgår av FFFS 2015:13 samt FFFS 2016:4.

[5] G/2.3.3.13/Aktuell QRT

4.1.3 Ansvarig

Ansvarig för att rapportering sker är ekonomifunktionen.

4.1.4 Kontroll

VD kontrollerar att rapporten upprättats och är korrekt samt att den rapporteras.

4.1.5 Beslut

VD fattar beslut om rapportering.

5 Rapportering av väsentliga fel, uppdateringar m.m.

Enligt FFFS 2015:13 ska bolaget lämna korrigerade upplysningar till Finansinspektionen om tidigare upplysningar innehåller väsentliga fel eller det vid årsstämman fattas beslut som innebär att tidigare lämnade upplysningar är missvisande.

Om det inträffar betydande utvecklingar ska, utöver att Finansinspektionen informeras, även en uppdatering av SFCR offentliggöras. Se även p6 nedan avseende väsentliga händelser..

5.1 Periodicitet

Så snart som möjligt.

5.2 Definition

5.2.1 Betydande utvecklingar

Bolaget har identifierat bl.a. följande händelser som betydande utvecklingar:

- Förändringar eller händelser som medför att en extraordinär ORSA-process initieras enligt Policy för ORSA.
- Borttagande av koncernens försäkringspolicy (konkurrensutsättning)
- Beslut eller externa händelser som minskar SCR-kvoten med 1,0 eller mer

5.2.2 Väsentliga fel

Med väsentliga fel avses materiella fel enligt definitionen i artikel 222, 291 och 305 i Kommissionens Delegerade förordning (EU) 2015/35.

Ex: Ett fel som skulle kunna påverka beslutsprocessen hos eller den bedömning som görs av användare av denna information, inbegripet tillsynsmyndigheterna.

Bolaget har identifierat bl.a. följande fel som väsentliga:

- Rapporterat kapitalkrav (SCR) är minst 5 procent för lågt eller 10 procent för högt
- Rapporterad kapitalbas är minst 5 procent för hög eller 10 procent för låg
- Felaktigheter som indikerar eller medför allvarliga brister i regelefterlevnad[6].
- Kvantitativa eller kvalitativa uppgifter där felaktigheter väsentligt försämrar jämförbarhet över tid eller mellan olika rapporter (inom och mellan QRT, SFCR, RSR och finansiella rapporter)

[6] Rapportering av felaktiga uppgifter som reflekterar poster som enligt tillstånd eller interna regler inte borde existera utgör väsentliga fel. Uppgifter som är obligatoriska men saknas ingår också om de inte är obetydliga.

För de två senare punkterna där kvantitativa gränser saknas behöver bedömning av upptäckta fel göras från fall till fall. Denna bedömning ska dokumenteras oavsett om felet bedöms väsentligt eller ej för att underlätta uppföljning och vidareutveckling av definitionerna.

5.2.3 Materiella förändringar

RSR ska endast vart tredje år vara fullständig, övriga år ska den avgränsas till materiella förändringar. SFCR ska särskilt belysa materiella förändringar.

Med materiella förändringar menas:

- Sådana förändringar som till sin innebörd skulle motsvara väsentliga fel enligt ovan
- Sådana utvecklingar som anses betydande enligt ovan
- Betydande förändringar i bolagsstyrnings- och riskhanteringssystem
- Utläggning eller hemtagning av väsentlig utlagd verksamhet
- Etc.

5.3 Innehåll

I enlighet med den rapport som är felaktig eller behöver uppdateras alternativt där materiella förändringar beskrivs.

5.4 Ansvarig

I enlighet med ordinarie process för aktuell rapport. Minst 2 på bolaget ska utföra bedömningen av materialitet.

5.5 Kontroll

I enlighet med ordinarie process för aktuell rapport.

5.6 Beslut

I enlighet med ordinarie process för aktuell rapport.

6 Väsentliga händelser

Rapportering av väsentliga händelser framgår av bolagets ”Riktlinjer för hantering och rapportering av händelser av väsentlig betydelse i S:t Erik Försäkrings AB”

Instruktion för hantering av reservsättningsrisker

för

S:t Erik Försäkrings AB

Innehållsförteckning

1. Allmänt

Denna instruktion har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Instruktionens syfte avser reservsättning av bolagets ansvarighet vid försäkringsfall, förvaltningskostnader och andra kostnader såsom ej intjänade premier och kvardröjande risker, oreglerade försäkringsfall och kostnader för reglering av dessa samt risken för att bolagets ansvarighet för försäkringsfall undervärderas. I Försäkringstekniska riktlinjer för S:t Erik Försäkring anges bolagets principer för reservsättning.

2. Reservsättningsinstruktion

Reservsättning av bolagets ansvar vid försäkringsfall ska ske så att risken för att bolagets åtagande underreserveras blir så liten som möjligt. Detta uppnås genom att beakta statistik och erfarenhet i bolagets försäkringsportfölj, erfarenhet från en större marknad av likartade risker och genom bedömning av individuella skadefall. Bedömningen av reserver vid försäkringsfall ska baseras på skriftligt reserveringsförslag från kompetent/a skadereglerare, antingen anställda i S:t Erik Försäkrings AB eller professionellt skaderegleringsföretag.

Vid bedömning av reservsättningsbehov ska beaktas skillnader mellan olika risk- eller produktgrupper.

3. Beslutsordning och befogenheter

Bolagets VD ansvarar för beslut om bolagets reserver med hänsyn tagen till ovanstående reservsättningsinstruktioner.

Bolagets VD beslutar om reserver för inträffade men ej rapporterade skador (IBNR) baserat på skriftlig bedömning av bolagets aktuarie.

4. Reservsättning

A. Inträffade men ej reglerade skador

A.1. Rapporterade skador

Vid bestämmande av skadereserv ska alltid individuell värdering av försäkringsfall göras.

Värderingen ska utgöra den för tidpunkten och övriga förhållanden mest realistiska uppskattningen av försäkringsfallets kostnader som kan göras vid värderingstillfället med särskilt beaktande av att risk för att underreservering kan ske.

Om bolaget upplever att värderingen för ett enskilt skadefall är särskilt osäker kan bolaget föreskriva att en särskild utredning görs och/eller tillämpa ett särskilt säkerhetspåslag. Säkerhetspåslagets storlek bestäms efter samråd med bolagets skadereglerare och/eller bolagets aktuarie.

För mottagen återförsäkring bör bolaget inhämta de uppgifter från cedenten som behövs för att kunna göra en korrekt och nöjaktig bedömning av tillräckligheten i de reservbelopp som rapporteras av denne. Om osäkerhet föreligger bör bolaget inhämta uppgifter från branschen och i förekommande fall också tillämpa tidigare egen erfarenhet för bedömningen.

A.2. Ej rapporterade skador

Avsättningar för IBNR skall beräknas för varje verksamhet och för varje tecknings-period för sig. Avsättning för skadekostnadsbelopp och avsättning för belopp avseende skadebehandlingskostnader bör fastställas var för sig.

Varje risktyp/-grupp skall som huvudprincip beräknas för sig. En kollektiv beräkning, omfattande flera olika risktyper, kan tillämpas om de ingående avtalen i riskkollektivet/ skadegruppen har likartad skadekarakteristik, dvs. är tillräckligt homogena ur skade-processynpunkt.

Inverkan av storskador analyseras separat, om möjligt. Detta är särskilt viktig för avsättning avseende riskgrupper som är återförsäkrade.

De samlade avsättningarna för en verksamhet är summan av varje löpande ingående års avsättning, och bolagets samlade avsättningar är summan av avsättningarna för varje verksamhet.

Avsättningar för IBNR skall i första hand grundas på bolagets egen erfarenhet, och i andra hand på information som kan erhållas från återförsäkrare/mäklare och/eller på branschstatistik som återspeglar liknande risker och avtal.

Närmare principer, och metoder för värdering av IBNR–avsättningar finns beskrivna i bolagets försäkringstekniska beräkningsunderlag.

Om bolagets egen portfölj är alltför begränsad för att uppvisa tillräcklig statistisk stabilitet skall IBNR-avsättningen beräknas med avseende på det egna självbehållet.

IBNR-avsättningen justeras, i förekommande fall, efterhand som nya skador rapporteras för den riskgrupp IBNR-avsättningen avser.

Slutlig bedömning av avsättningar för inträffade men ej rapporterade skador (IBNR) ska göras skriftligen av bolagets aktuarie, eller baseras på skriven instruktion från denne.

B. Ej inträffade skador

Bedömning ska göras avseende reservsättning för kvarvarande avtalsperiod med utgångspunkt i såväl bolagets egen erfarenhet som branscherfarenhet och marknadsinformation.

Som huvudregel gäller att avsättning skall ske pro rata temporis.

5. Registrering

Bolaget ska utan dröjsmål registrera varje försäkringsfall som anmäls. Registreringen ska omfatta följande:

- varje skada ska åsättas ett unikt skadenummer

- uppskattning av försäkringsfallets totala kostnad inklusive separat redovisning av kostnader för skadereglering
- självrisk
- utbetald skadeersättning inklusive separat redovisade skaderegleringskostnader
- ännu ej utbetald skadeersättning inklusive separat redovisade skadereglerings-kostnader
- uppgifterna ska fortlöpande uppdateras
- skadereglerare ansvarig för skadans handläggande skall anges.

6. Dokumentation i skadeakten

Skadeakten skall innehålla information om:

- beskrivning av skadehändelse
- beskrivning av skadeorsak
- uppskattning av totala skadekostnader inklusive separat redovisade skade-regleringskostnad
- självrisk
- beskrivning av hur skadan ska hanteras
- skadeakten ska fortlöpande uppdateras med avseende på utbetald skadeersättning, ännu ej utbetald skadeersättning, skaderegleringsarbetets fortskridande, eventuella nya eller ändrade bedömningar av skadan samt underlag som verifierar utbetald ersättning.

7. Uppföljning, analys och rapportering

Bolaget bör omvärdera och följa upp värderingen av reserver regelbundet, dock minst en gång per år. Beslut för hur ofta reserver bör omvärderas skall grundas på tidigare erfarenhet. Bolagets VD ska regelbundet utvärdera bolagets skadeadministration, bl.a. genom att inhämta uppgifter från skadereglerare och från bolagets aktuarie. I samband med bolagets styrelsemöten ska bolagets VD redovisa dessa analyser till styrelsen.

****

INSTRUKTION FÖR S:T ERIK FÖRSÄKRINGS REVISIONSARBETE

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Denna instruktion har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler” och har fastställts av styrelsen för S:t Erik Försäkrings AB (styrelsen).

Instruktionen ska fastställas årligen av styrelsen och revideras vid behov.

Syftet med instruktionen är att upprätthålla en korrekt revision med god kvalité.

2 Sammansättning

Styrelsen har enligt 8 kap 49 a § 2 st ABL beslutat att själv hantera revisionsfrågorna och därmed inte utse ett revisionsutskott.

3 Uppgifter

3.1 Allmänt

Styrelsen bereder och beslutar i revisionsfrågor.

3.2 Finansiell rapportering

Styrelsen ska övervaka bolagets finansiella rapportering samt vid behov lämna rekommendationer och förslag att säkerställa dess tillförlitlighet. I detta ingår att övervaka effektiviteten avseende den finansiella rapporteringen i bolagets interna kontroll, internrevision, regelefterlevnad och riskhantering.

3.3 Revision

Styrelsen ska hålla sig informerad om revisionen i årsredovisningen samt slutsatserna av Revisorsnämndens kvalitetskontroll. Styrelsen ska övervaka att revisorn följer rapporteringskraven i revisionsberättelsen samt den årliga rapporten till styrelsen.

3.4 Opartiskhet

Styrelsen ska granska och övervaka revisorernas opartiskhet och självständighet.

Detta sker genom att styrelsen:

- Tar in bekräftelse på revisors opartiskhet.
- Kontrollerar att revisor uppfyller kraven på rotation.
- Uppmärksammar om revisorn tillhandahåller bolaget andra tjänster än revision och att dessa godkänts av styrelsen.
- Övervakar revisorns beräkning och uppföljning av arvode för rådgivningstjänster.

Styrelsen ska på förhand godkänna revisorns/revisionsföretagets tillhandahållande av andra tjänster än revision och därvid kontrollera och dokumentera att:

- Tjänsterna har ingen eller obetydlig effekt, separat eller totalt sett på de granskade finansiella rapporterna
- Den uppskattade effekten på de granskade finansiella rapporterna dokumenteras på ett heltäckande sätt och förklaras i den kompletterande rapporten som revisorn/revisionsföretaget ska lämna till RU.
- Revisorns/revisionsföretagets opartiskhet och självständighet respekteras.

- Erforderliga skyddsåtgärder vidtas.

3.5 Revisorsval

Styrelsen ska vid behov biträda vid upprättande av förslag till bolagsstämmans beslut om revisorsval. Om aktieägarna har ett bestämmande inflytande över valberedningen eller motsvarande kan valberedningen lämna förslag till val av revisor.

4 Sammanträden

Styrelsen ska behandla revisonsfrågor regelbundet anpassat till styrelsesammanträdena.

Vid sammanträden utanför styrelsesammanträdena skall protokoll föras som anmäls vid styrelsesammanträdet. Vid behov kallas, VD, ansvarig externrevisor, ansvarig internrevisor, ansvarig för regelefterlevnad, ansvarig för riskkontroll samt ansvarig för finansiell rapportering eller annan bolagsfunktionärer,

5 Rapportering

Styrelsens ordförande skall tillse att styrelsen hålls informerad om revisionsarbetet arbete och att beslut och rekommendationer till beslut motiveras.

Bilaga 1 - Lathund

3.3

- Styrelsen ska hålla sig informerad om revisionen och slutsatserna av Revisorsnämndens kvalitetskontroll

- Årlig revisionsberättelse till styrelsen enligt innehåll i Artikel 10 Förordningen

- Årlig kompletterande rapport till styrelsen enligt innehåll i Artikel 11 Förordningen

3.4

- Årlig skriftligt intygande från revisor om opartiskhet och oberoende, Artikel 6.2.a Förordningen

- Årlig diskussion revisor avseende hot mot opartiskhet samt ev. skyddsåtgärder, Artikel 6.2.b Förordningen

- Årlig kontroll avseende krav på varaktighet/rotation enligt Artikel 17 Förordningen.

    - 10 års rotation för bolag
    - 7 års rotation för påskrivande revisor

- Kontroll om revisorn tillhandahåller andra tjänster till bolaget och om dessa får tillhandahållas enligt Artikel 5 Förordningen.

- Godkänna andra tjänster än revision enligt Artikel 5 Förordningen

- Kontrollera att revisorns beräkningar och uppföljning av arvoden enligt de begränsningar som finns i Artikel 4 i Förordningen

    - Fr o m 2020 får arvode för rådgivning uppgå till max 70% av genomsnittlig revisionsarvode de 3 föregående åren (Artikel 4.2)

    - Om mer än 15% av totala arvodena för revisorn/revisionsbolaget under vart och ett av de senaste tre åren kommer ifrån bolaget ska detta särskilt granskas avseende opartiskhet samt erforderliga skyddsåtgärder vidtas (Artikel 4.3)

3.5

- Upphandling ska ske av revisors/revisionsbolag vart 10:e år.

- RU ska vid behov lämnas förslag på revisor till bolagsstämman, alternativt överlåta detta till valberedningen om aktieägarna har ett bestämmande inflytande över denna. Överlåts beslut till valberedning ska RU hålla denna informerad om behov av förändring behövs enligt punkterna ovan

Bilaga 2 – Styrelsens kontroller

MARS

3.3

1. **Styrelsen ska hålla sig informerad om revisionen och slutsatserna av Revisorsnämndens kvalitetskontroll**

    - Kontakt med revisorer inför styrelsemöte
    - Kontroll med revisorsnämnden och FAR (kvalitetsnämnden) inför styrelsemöte

2. **Årlig revisionsberättelse till styrelsen enligt innehåll i Artikel 10 Förordningen 3 veckor innan årsstämma (21 mars)**

    a. Kontakt med revisorer under våren

3. **Årlig kompletterande rapport till styrelsen enligt innehåll i Artikel 11 Förordningen 3 veckor innan årsstämma (21 mars)**

    - Kontakt med revisorer under våren

3.4

4. **Kontroll om revisorn tillhandahåller andra tjänster till bolaget och om dessa får tillhandahållas enligt Artikel 5 Förordningen.**

    - Kontakt med revisorer och verksamheten inför styrelsemöte

5. **Godkänna andra tjänster än revision enligt Artikel 5 Förordningen**

    - Kontakt med revisorer och verksamheten inför styrelsemöte

6. **Kontrollera att revisorns beräkningar och uppföljning av arvoden enligt de begränsningar som finns i Artikel 4 i Förordningen**

    a) Fr o m 2020 får arvode för rådgivning uppgå till max 70% av genomsnittlig revisionsarvode de 3 föregående åren (Artikel 4.2)

        - Kontakt med ekonomifunktionen innan styrelsemöte

    b) Om mer än 15% av totala arvodena för revisorn/revisionsbolaget under vart och ett av de senaste tre åren kommer ifrån bolaget ska detta särskilt granskas avseende opartiskhet samt erforderliga skyddsåtgärder vidtas (Artikel 4.3)

- Kontakt med revisorer och ekonomi med fråga samt kontroll av revisorers årsredovisning med jfr från ekonomi

MAJ

3.3

1. **Styrelsen ska hålla sig informerad om revisionen och slutsatserna av Revisorsnämndens kvalitetskontroll**

    - Kontakt med revisorer inför styrelsemöte
    - Kontroll med revisorsnämnden och FAR (kvalitetsnämnden) inför styrelsemöte

3.4

2. **Kontroll om revisorn tillhandahåller andra tjänster till bolaget och om dessa får tillhandahållas enligt Artikel 5 Förordningen.**

    - Kontakt med revisorer och verksamheten inför styrelsemöte

3. **Godkänna andra tjänster än revision enligt Artikel 5 Förordningen**

    - Kontakt med revisorer och verksamheten inför styrelsemöte

4. **Kontrollera att revisorns beräkningar och uppföljning av arvoden enligt de begränsningar som finns i Artikel 4 i Förordningen**

    a) Fr o m 2020 får arvode för rådgivning uppgå till max 70% av genomsnittlig revisionsarvode de 3 föregående åren (Artikel 4.2)

        - Kontakt med ekonomifunktionen innan styrelsemöte

    b) Om mer än 15% av totala arvodena för revisorn/revisionsbolaget under vart och ett av de senaste tre åren kommer ifrån bolaget ska detta särskilt granskas avseende opartiskhet samt erforderliga skyddsåtgärder vidtas (Artikel 4.3)

        - Kontakt med revisorer och ekonomi med fråga samt kontroll av revisorers årsredovisning med jfr från ekonomi

5. **Årlig kontroll avseende krav på varaktighet/rotation enligt Artikel 17 Förordningen.**

    - 10 års rotation för bolag
    - 7 års rotation för påskrivande revisor

        - Kontroll mot våra avtal, kontakt jur. SEF inför styrelsemöte.

3.5

6. **Upphandling ska ske av revisors/revisionsbolag vart 10:e år.**

    - Kontroll mot avtal m revisorer

7. **RU ska vid behov lämnas förslag på revisor till bolagsstämman, alternativt överlåta detta till valberedningen om aktieägarna har ett bestämmande inflytande över denna. Överlåts beslut till valberedning ska RU hålla denna informerad om behov av förändring behövs enligt punkterna ovan**

    - Tillse att verksamheten upphandlar eller att Stockholms stad informeras om behovet och de krav som SEF lyder under och att upphandling sker i tid innan årsskiftet.

OKTOBER

3.3

1. **Styrelsen ska hålla sig informerad om revisionen och slutsatserna av Revisorsnämndens kvalitetskontroll**

    - Kontakt med revisorer inför styrelsemöte
    - Kontroll med revisorsnämnden och FAR (kvalitetsnämnden) inför styrelsemöte

3.4

2. **Kontroll om revisorn tillhandahåller andra tjänster till bolaget och om dessa får tillhandahållas enligt Artikel 5 Förordningen.**

    - Kontakt med revisorer och verksamheten inför styrelsemöte

3. **Godkänna andra tjänster än revision enligt Artikel 5 Förordningen**

    - Kontakt med revisorer och verksamheten inför styrelsemöte

4. **Kontrollera att revisorns beräkningar och uppföljning av arvoden enligt de begränsningar som finns i Artikel 4 i Förordningen**

    a) Fr o m 2020 får arvode för rådgivning uppgå till max 70% av genomsnittlig revisionsarvode de 3 föregående åren (Artikel 4.2)

        - Kontakt med ekonomifunktionen innan styrelsemöte

    b) Om mer än 15% av totala arvodena för revisorn/revisionsbolaget under vart och ett av de senaste tre åren kommer ifrån bolaget ska detta särskilt granskas avseende opartiskhet samt erforderliga skyddsåtgärder vidtas (Artikel 4.3)

        - Kontakt med revisorer och ekonomi med fråga samt kontroll av revisorers årsredovisning med jfr från ekonomi

NOVEMBER

3.3

1. **Styrelsen ska hålla sig informerad om revisionen och slutsatserna av Revisorsnämndens kvalitetskontroll**

    - Kontakt med revisorer inför styrelsemöte
    - Kontroll med revisorsnämnden och FAR (kvalitetsnämnden) inför styrelsemöte

3.4

2. **Årlig skriftligt intygande från revisor om opartiskhet och oberoende, Artikel 6.2.a Förordningen**

3. **Årlig diskussion revisor avseende hot mot opartiskhet samt ev. skyddsåtgärder, Artikel 6.2.b Förordningen**

    - Kontakt med revisor inför styrelsemöte

4. **Kontroll om revisorn tillhandahåller andra tjänster till bolaget och om dessa får tillhandahållas enligt Artikel 5 Förordningen.**

    - Kontakt med revisorer och verksamheten inför styrelsemöte

5. **Godkänna andra tjänster än revision enligt Artikel 5 Förordningen**

    - Kontakt med revisorer och verksamheten inför styrelsemöte

6. **Kontrollera att revisorns beräkningar och uppföljning av arvoden enligt de begränsningar som finns i Artikel 4 i Förordningen**

    a) Fr o m 2020 får arvode för rådgivning uppgå till max 70% av genomsnittlig revisionsarvode de 3 föregående åren (Artikel 4.2)

        - Kontakt med ekonomifunktionen innan styrelsemöte

    b) Om mer än 15% av totala arvodena för revisorn/revisionsbolaget under vart och ett av de senaste tre åren kommer ifrån bolaget ska detta särskilt granskas avseende opartiskhet samt erforderliga skyddsåtgärder vidtas (Artikel 4.3)

        - Kontakt med revisorer och ekonomi med fråga samt kontroll av revisorers årsredovisning med jfr från ekonomi

Instruktion för tecknings- och återförsäkringsrisker

för

S:t Erik Försäkrings AB

Innehållsförteckning

1. Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Instruktionen syftar till

- att uppnå en tillfredsställande riskspridning och en i övrigt lämplig sammansättning av bolagets försäkringsportfölj och risker så att dessa motsvarar bolagets risktäckningskapacitet och ej äventyrar bolagets soliditet,
- att säkerställa att bolagets portfölj och risksammansättning överensstämmer med bolagsordning, verksamhetsmål och övriga policydokument,
- att säkerställa att en tillfredsställande dokumentation och rapportering upprätthålls.

2. Teckningsrisker

Endast bolagets VD äger rätt att ikläda bolaget försäkringsåtaganden, som inte anges i tariff eller motsvarande fastställd av styrelsen för bolaget, om inte annat följer nedan.

Bolagets anställda kan utfärda försäkringsbrev i enlighet med bestämmelser i tariff eller motsvarande, eller då sådan inte särskilt är fastställd, som följer.

Risker som ej kan inordnas i ordinarie återförsäkringsavtal får tecknas av enskild anställd upp till ett försäkringsbelopp om högst 1 000 000 kronor, och av VD upp till ett försäkringsbelopp om högst 5 000 000 kronor. Sådana risker får dock högst uppgå till 5 000 000 kronor aggregerat på årsbasis(aggregerad årsrisk) och högst 15 000 000 kronor aggregerat vid var tidpunkt.

Sådana ingångna mindre försäkringsengagemang ska i efterhand anmälas till styrelsen om respektive åtagande överstiger 12 månader.

Försäkringsengagemang för riskgrupper [1]får aldrig slutgiltigt accepteras förrän återförsäkringstäckning kan anses vara säkerställd i enlighet med bestämmelser i bolagets försäkringstekniska riktlinjer.

Vid täckandet av försäkringsengagemang skall maximala bruttoåtagande per risk, bedömd maximal skada (Estimated Maximum Loss, EML) om tillämpligt, bolagets solvens, likviditet och den återförsäkringskapacitet som bedöms vara tillgänglig beaktas.

Bolaget bör inte teckna affär till lägre premie, totalt för bolagets samtliga accepterade risker, än vad som bolagets aktuarie fastställt som minsta rekommenderade premie för fastställd volym (riskexponering) och samtliga portföljer sammantagna (premiesättning).

3. Registrering, dokumentation och rapportering

Bolaget skall utan dröjsmål och på ett tillfredsställande sätt dokumentera alla förhållanden som är relevanta för bedömningen av de försäkringsengagemang

[1] T.ex. ’Egendom, ’Ansvar’ mfl

bolaget ikläder sig; särskilt vikt bör därvid läggas på att risker inte av misstag felkategoriseras. I dokumentationen över försäkringsåtaganden skall framgå försäkringstyp, engagemangets storlek, premiegrundande faktorer, EML-belopp om tillämpligt, självbehåll samt återförsäkring.

Bolagets försäkringsakter skall förvaras på ett sådant sätt att informationen ej kan förkommas genom oförutsedd händelse, och i övrigt enligt bolagets arkivregler.

Vid förvaring av försäkringsakter skall hänsyn tas till försäkringsavtalets längd och tid för slutgiltig skadereglering efter inträffad skada.

Bolaget har fastställt följande rutiner för registrering av tecknade försäkringsengagemang

- Försäkringsbrev skall upprättas och bevaras i försäkringssystemet Insman
- Försäkringsbrev och förekommande försäkringsbevis skall finnas under G-katalogen samt i kundpärm.
- Noteringar om premiefaktorer skall, om möjligt, ske i Insman samt finnas i kundpärm.
- Kopior på samtliga brev och bevis skall tillställas skadereglerare

Bolaget bör tillse att det finns informationssystem som kan tillhandahålla relevant information om ingångna försäkringsengagemang, och att informationen finns lätt åtkomlig för de personer som behöver den.

Bolagets dokumentation av återförsäkringsprogram ska minst innehålla

- principer för val av återförsäkrare och återförsäkringsavtäckning inom respektive riskgrupp
- en förteckning över återförsäkringsavtal i kraft
- självbehållsgränser för respektive återförsäkrad riskgrupp

4. Återförsäkringsrisker

Riktlinjer för vilka risker som bolaget får ikläda sig och vilka självbehåll som ska gälla fastslås av bolagets styrelse med beaktande av bolagsordningen och bolagets försäkringstekniska riktlinjer och bolagets instruktioner för tecknande av försäkring (avsnitt 2 i detta dokument).

Bolagets VD ska tillse att bolaget har ett tillfredsställande återförsäkringsskydd för tecknade risker, och att återförsäkringsavtäckning finns som motsvarar vad som förutsättes i bolagets återförsäkringsprogram. Särskilt bör då beaktas kongruensen mellan bolagets tillämpade villkor och de villkor som tillämpas i återförsäkringsavtalen. Den faktiska risköverföringen ska bedömas samt beaktande av eventuell basrisk (den risk som följer av en situation där den exponering som omfattas av den riskreducerande tekniken inte motsvarar bolagets riskexponering t ex valutamissmatch).

Vidare skall bolagets VD säkerställa att rutiner finns för rapporterings- och avräkningsförfarande mot återförsäkrare, dels så att avräkningsförfarandet görs korrekt, dels så att risken för att avräkning förbises minimeras.

Vid placering av återförsäkring ska återförsäkrares soliditet och betalningsförmåga (security) bedömas.

Återförsäkring ska endast tecknas hos motparter som har en extern rating från ett godkänt ratinginstitut som vid solvenskapitalkravsberäkning motsvarar kreditkvalitetssteg 2 eller bättre[2]. Om motparten saknar extern rating ska den senaste publicerade solvenskvoten (SCR-kvot) medge motsvarande behandling som kreditkvalitetssteg 2[3].

Bolaget ska även göra en egen bedömning av kvalitén på återförsäkraren utifrån tillgänglig information om tillämpligt. Återförsäkrare som har lägre rating eller saknar rating, får endast användas efter särskilt beslut av styrelsen. Det övergripande återförsäkringsskyddet för S:t Erik Försäkring ska godkännas årligen av styrelsen. S:t Erik försäkring ska om möjligt, genom upphandling, placera återförsäkring hos flera olika återförsäkringsgivare och tillse att återförsäkringsavtalens betalningsvillkor överensstämmer med bolagets motsvarande skyldighet mot försäkringstagarna.

Bolaget skall för riskgrupper välja en återförsäkringslösning som begränsar bolagets risktagande i enlighet med följande (riskbedömning).

Bolaget får aldrig ikläda sig större risk än:

- en maximal riskexponering per enskild riskgrupp som överstiger 15% av solvenskapitalet
- en maximal samlad riskexponering som överstiger 20% av solvenskapitalet.

Solvenskapitalet ska här beräknas utan beaktande av eventuellt tilläggskapital, d.v.s. kapitalgarantier e.d. ingår ej. Bolagets maximala riskexponering för en enskild riskgrupp beräknas för nytecknad affär som skillnaden mellan självbehållsnivå och aktuariell riskpremie.

Bolagets maximala samlade riskexponering beräknas genom att addera maximal riskexponering över samtliga riskkollektiv/riskgrupper enligt ovan. Bolaget får därvid göra ett avdrag från den summerade riskexponeringen vilket motsvarar det statistiska oberoendet mellan de olika riskgrupperna och teckningsperioderna (risker som är okorrelerade).

Om bolaget för en begränsad period finner skäl att överskrida maximal riskexponering skall bolagets VD, efter att först ha inhämtat synpunkter från

[2] Godkända ratinginstitut samt mappningen mellan deras ratingskala och kreditkvalitetssteg framgår av Kommissionens genomförandeförordning (EU) 2016/1800. Exempelvis gäller för ratingar från Standard & Poor's respektive Moody's att kreditkvalitetssteg 2 som följer på långfristiga ratingar A- respektive A3 som lägst.

[3] Motsvarande behandling vid saknad rating följer på artikel 199.3 i Solvens II-förordningen (EU 2015/35) för motparter vars solvenskvot är minst 1,75, för dessa blir riskvikten samma som för motparter med kreditkvalitetssteg 2 (d.v.s. 0,05)

bolagets aktuarie, informera styrelsen, som därefter måste ge sitt bifall innan detta får ske.

*****

IT-AVBROTTSPLAN FÖR S:T ERIK FÖRSÄKRINGS AB

Fastställd av styrelsen 2022-05-23

1 Allmänt

Denna avbrottsplan är upprättad i överensstämmelse med Försäkringsrörelselagen, Finansinspektionens riktlinjer samt Stockholm stads Riktlinje för Informationssäkerhet.

Riktlinjerna ska prövas årligen av styrelsen och revideras vid behov.

VD ansvarar för att listade system samt kontaktuppgifter i avbrottsplanen hålls löpande uppdaterade och tillgängliga för styrelsen. Förändringar anmäls vid nästkommande styrelsemöte.

2 Revisionshistorik

Version	Datum	Namn	Beskrivning
V08	2013-07-30	Erik Fischer	Ändringar i hela dokumentet
V09	2013-07-31	Maria Pettersson	Uppdateringar av b la bilagor samt textinformation
V1.0	2013-08-01	Maria Pettersson	Rättningar stavfel
V1.1	2016-05-26	Erik Fischer	Uppdateringar av b la bilagor samt textinformation
V1.2	2017-05-02	Said Tabari	Uppdateringar av b la bilagor samt textinformation
V1.3	2019-05-27	Said Tabari, Ekaterina Raymond, Erik Fischer	Uppdateringar av b la bilagor, textinformation samt beslutanderätt vid ändring av kontaktuppgifter.
V1.4	2020-04-28	Said Tabari	Tieto är nya IT leverantören i Stockholm

3 Syfte

Syftet med en kontinuitets-/avbrottsplan är att företagets verksamhetsprocesser och/eller IT-system, så snabbt som möjligt kan etablera normal verksamhet efter ett eventuellt avbrott och/eller störning. Om företaget inte är förberett kan verksamheten drabbas av långa ledtider och driftstopp. Därför är det av stor vikt att kontinuitets-/avbrottsplanerna på ett enkelt sätt kan hanteras i verksamheten. Vid en störning och/eller driftavbrott kommer stora och i vissa fall speciella krav att ställas på den berörda personalen. Många svåra och ibland snabba beslut måste fattas i en många gånger pressad arbetssituation. För att begränsa skadeverkningarna i verksamheten är det därför av avgörande betydelse att man i förväg har fastställt den organisation som ska fungera när hela och/eller delar av kontinuitetsplanen måste aktiveras. Informationen till personal, användare, kunder och massmedia måste prioriteras.

4 Berörda verksamhetssystem

a) IA
b) Försäkringssystem (INSMAN)
c) E-post
d) Kontorssystem (t ex Microsoft Office)
e) Telefonväxel/Mobilt
f) www.sterikforsakring.se
g) Ekonomisystem Agresso
h) Lönesystem VISMA Agda

Övrig påverkan
i) Virus i arbetsstation
j) Elavbrott i kontorslokalerna
k) Driftstopp hos Tieto
l) Driftstopp hos S:t Erik Kommunikation

5 Avbrott

5.1 Allmänt

Om störningen/avbrottet är av mindre art så skallåtgärden hanteras enligt normal drifthantering.

Vid en längre störning/avbrott som är mellan 0-2 timmar och av mindre art, kontaktas IT-ansvarig som vidtar åtgärder enligt avbrottsplanen. Åtgärder och beslut ska dokumenteras i loggbok..

Om störningen är omfattande beslutar IT-ansvarig ifall katastrofgrupp IT ska aktiveras Åtgärder och beslut ska dokumenteras i loggbok..

5.2 Åtgärder

5.2.1 Samtliga medarbetare

IT-ansvarig ska larmas när det uppstått en störning och/eller ett avbrott, där åtgärden inte hanteras enligt normal drifthantering och/eller att omfattningen kan vara svår att uppskatta.

Larmet ska innehålla följande information:

- Vad som inträffat
- Vem som upptäckte störningen
- Vem som ”äger” ärendet
- Person-/materiella skador
- Åtgärder som har vidtagits
- Hur länge avbrottet beräknas pågå

5.2.2 IT-ansvarig

IT-ansvarig som tar emot larmet ska:

- Besluta om kontinuitetsplanen ska aktiveras enligt bilaga 1.
- Besluta om katastrofgruppen ska aktiveras
- Informera berörd systemförvaltare och systemansvarig
- Undersöka vilka åtgärder som hittills har vidtagits?
- Specificera vem/vilka som ansvarar för att återställa de olika funktioner som avbrottet berör.
- Utreda vem/vilka som har huvudansvaret samt samordnande roll för de återställande aktiviteterna?
- Dokumentera avbrottet i loggbok

5.2.2.1 Loggbok

Vid avbrott skall IT-ansvarig identifiera, beskriva och dokumentera följande i en loggbok:

Tid (när) När inträffade avbrottet?
Hur lång tid beräknas avbrottet vara?

Vem upptäckte störningen/avbrottet?

Vad omfattar avbrottet (system/tjänst, dator, applikation, kommunikation etc.)?

Specificera den funktionalitet som inte fungerar pga. avbrottet. I förekommande fall försök specificera eventuella person-, materiella, immateriella samt ekonomiska skador.

Vilka drabbas av avbrottet (användare, antal, kunder m.m.)?

Se bilaga nr 3 Loggbok avbrott IT

5.2.3 Katastrofgruppen IT

En katastrofgrupp ska inrättas med i förväg utsedda medlemmar, inklusive ersättare.

De personer som ska vara med och ta beslut om alternativa rutiner, återgång till normalläge och eventuella korrigerande åtgärder ska finnas med i gruppen. ***Se bilaga nr 4, Katastrofgrupp IT***

Katastrofgruppen IT har det övergripande ansvaret och ska gemensamt fatta beslut (vid oenighet fattar ordföranden beslut) om bland annat:

- förbereda reservdrift
- övergå till reservdrift
- övergång till alternativa rutiner, manuella eller IT-baserade
- information till användare och andra berörda (ex styrelsen)
- återgång till normal drift

5.2.4 Aktivering av reservrutin

Katastrofgruppen aktiverar övergången till reservdriften i enlighet med detta dokument samt fattar beslut enligt nedan.

- Utse projektledare (prel IT-ansvarig) att leda och samordna arbetet med förberedelser och genomförande av reservdrift/reservrutin. Projektledaren ska också hålla katastrofgruppen uppdaterad med progress samt säkerställa att en loggbok etableras för dokumentation av samtliga åtgärder som vidtas.
- Delegera ansvar och befogenheter till, i förekommande fall, projektledaren för reservdriften
- Förberedelser för reservrutinen: Säkerställ viktig infrastruktur och logistik såsom lokal, utrustning, elförsörjning, ev klimatförsörjning, kommunikationslösningar, papper, förbrukningsmaterial, blanketter m.m
- Behov av större inköp/investeringar gör det
- Disponera personal utöver ordinarie arbetstid
- Övergång till reservrutin
- Öppethållande
- Information

- Avsluta reservrutinen för återgång till normalläge

5.2.5 Återgång till normal drift

Katastrofgruppen fattar beslut om att:

- reservdriften avslutas för övergång till normal drift.
- avveckling av projektet för reservdriften

BILAGA 1 - Verksamhetssystem, information, reservrutin m.m.

1.IA	
Allmänt	Incidentrapporteringssystem, ia.stockholm.se Driftas av AFA försäkring
Accepterad avbrottstid	5 dagar
Information	Via www.sterikforsakring.se samt epostmeddelande till alla IA-ansvariga och säkerhetsansvariga inom staden. Vid omfattande driftstopp skickas epostmeddelande även till stadsdelsdirektörer/avdelningschefer/VD:ar samt att information läggs ut på stadens intranät. *Se bilaga nr 5 ”Textförslag felmeddelande vid driftstopp”*
Vid driftstörning/avbrott/ reservrutin	Incidentrapporter läggs på hög hos rapportörer/lokala administratörer. Incidenter som ska rapporteras som en skada till SEF ska tas emot manuellt hos SEF och dokumenteras under G:\ verksamhetsstöd\IT och telefoni\avbrottsplan \Avbrottsplan IT\avbrott IA_INSMAN. Övriga förfrågningar och skadeärenden till SEF dokumenteras under G:\ verksamhetsstöd\IT och telefoni\avbrottsplan \Avbrottsplan IT\avbrott IA_INSMAN. Epost hanteras som vanligt.
Återgång till normalläge	Inrapportering av det material som lagrats på hög, görs av rapportörer och lokala administratörer hos våra kunder. Övriga frågor och skadeärenden uppdateras i systemet av SEF och i förekommande fall telefonkontakt med berörda. Ta bort information på hemsidan.
Drabbad	Alla användare i staden (som finns i IDportalen m.m) samt skadereglerare, konsulter ochandra externa användare som loggar in med Mobilt BankID

2.VERKSAMHETSSYSTEMET INSMAN	
Allmänt	Försäkringssystem/Skadesystem iFACTS
Accepterad avbrottstid	5 dagar
Information	Via www.sterikforsakring.se samt epostmeddelande till berörda användare. *Se bilaga nr 5 ”Textförslag felmeddelande vid driftstopp”*
Vid driftstörning/avbrott/ reservrutin	Förfrågningar och behov av ärendeinformation från systemet dokumenteras under G:\ verksamhetsstöd\IT och telefoni\avbrottsplan \Avbrottsplan IT\avbrott RISK_INSMAN. Använd manuell skadeanmälan till Crawford, *se bilaga nr 6 ”Manuell skadeanmälan till skadereglerare”* . Epost hanteras som vanligt.
Återgång till normalläge	Registrering av det material som lagrats på hög (G:\ verksamhetsstöd\IT och telefoni\avbrottsplan \Avbrottsplan IT\avbrott RISK_INSMAN). Övriga frågor och

	försäkringsärenden uppdateras nu i systemet och i förekommande fall telefonkontakt med berörda.
Drabbad	SEF, Säkerhetsfunktionen SLK, skadereglerare, konsulter och andra externa användare som loggar in med Mobilt BankID.

4.E-POSTSYSTEMET (OUTLOOK/EXCHANGE)	
Allmänt	E-post
Accepterad avbrottstid	1 arbetsdag
Information	Via www.sterikforsakring.se och meddelande till växeln. *Se bilaga nr 5 ”Textförslag felmeddelande vid driftstopp”*
Vid driftstörning/avbrott/ reservrutin	Använd istället telefon, fax samt utskick av vanliga brev. Telefonkontakter, fax och brev dokumenteras under G:\officiella dokument\Avbrottsplan IT\avbrott EPOST
Återgång till normalläge	Epost skickas nu och handläggarna arbetar ikapp den epost som inte skickats pga. störningen/driftstoppet. Ta bort information på hemsidan.

5.KONTORSSYSTEM OCH DOKUMENT	
Allmänt	Microsoft Officepaketet inkl e-post och dokument
Accepterad avbrottstid	2 arbetsdagar
Information	Via www.sterikforsakring.se och telefon. *Se bilaga nr 5 ”Textförslag felmeddelande vid driftstopp”*
Vid driftstörning/avbrott/ reservrutin	Använd telefon, fax och utskick av vanliga brev (handskrivet). Använd bärbar dator om driftstoppet berör stationär dator och använd stationär ifall det är störning på bärbar dator. Behov av att skicka mail dokumenteras manuellt i pärm ”Avbrottsplan IT”. Telefonkontakter, fax och utskick av vanliga brev dokumenteras under G:\officiella dokument\Avbrottsplan IT\avbrott Kontorssystem
Återgång till normalläge	Handläggarna arbetar ikapp de ärenden som kommit in. Ta bort information på hemsidan.

7.TELEFONVÄXEL	
Allmänt	Avser de stationära telefonerna och gruppnumret.
Accepterad avbrottstid	5 arbetsdagar
Information	Via www.sterikforsakring.se *Se bilaga nr 5 ”Textförslag felmeddelande vid driftstopp”*
Vid driftstörning/avbrott/ reservrutin	Använder mobiltelefonerna om driftstoppet berör fast telefoni och använd fast telefoni ifall det är störning på mobiltelefonin.
Återgång till normalläge	Ingen åtgärd. Ta bort information på hemsidan.

8.WWW.STERIKFORSAKRING.SE	
Allmänt	S:t Erik Försäkrings hemsida Ombraco
Accepterad avbrottstid	5 arbetsdagar
Information	Skicka epostmeddelande till alla risk- och säkerhetsansvariga, stadsdelsdirektörer/vd:ar och högre chefer, skadereglerare och övriga konsulter som är aktuella. Meddela stadens växel.
Vid driftstörning/avbrott/ reservrutin	Övriga förfrågningar och skadeärenden dokumenteras under G:\ verksamhetsstöd\IT och telefoni\avbrottsplan officiella dokument\Avbrottsplan IT\avbrott HEMSIDA. Epost hanteras som vanligt. Använd telefon.
Återgång till normalläge	Inrapportering av det material som lagrats på hög. Övriga frågor och ärenden uppdateras nu i systemet och i förekommande fall telefonkontakt med berörda. Ta bort information på hemsidan.

9.EKONOMISYSTEMET *Agresso*	
Allmänt	Ekonomisystemet
Accepterad avbrottstid	5 arbetsdagar
Information	Information sprids internt inom SEF. Vid allvarligare avbrott informeras Servicecentrum och styrelsen.
Vid driftstörning/avbrott/ reservrutin	Förfrågningar och behov av ärendeinformation från systemet dokumenteras under G:\verksamhetsstöd\IT och telefoni\avbrottsplan officiella dokument\ Avbrottsplan IT\avbrott EKONOMISYSTEM samt G:\Ekonomi. E-post hanteras som vanligt. All utbetalning kan ske manuellt via internetbank av ekonomiansvarig. För att ekonomiansvarig ska kunna göra alla bokslut behövs ekonomisystemet. Det finns backup-rutiner för ekonomisystemet.
Återgång till normalläge	Registrering av det material som lagrats på hög (G: \verksamhetsstöd\IT och telefoni\avbrottsplan\Avbrottsplan IT\avbrott EKONOMISYSTEM samt G:\Ekonomi). Övriga frågor och ekonomiärenden uppdateras nu i ekonomisystemet och i förekommande fall telefonkontakt med berörda.
Drabbad	Anställda inom SEF/Serviceenheten/Styrelsen

10.LÖNESYSTEMET *VISMA Agda*	
Allmänt	Lönesystemet
Accepterad avbrottstid	5 arbetsdagar
Information	Information sprids internt inom SEF
Vid driftstörning/avbrott/ reservrutin	Skulle avbrott inträffa vid utbetalningsdag för lön kontaktas HH Lönekonsult som tillhandahåller underlagen. Vidare kan utbetalning ske manuellt från bolagets konto Förfrågningar och behov av ärende-information från systemet

	dokumenteras under G:\ verksamhetsstöd\IT och telefoni\avbrottsplan \Avbrottsplan IT\avbrott LÖNESYSTEM samt G:\Ekonomi. Epost hanteras som vanligt. All utbetalning kan ske manuellt via internetbank av ekonomiansvarig. Det finns backup-rutiner för ekonomisystemet.
Återgång till normalläge	Registrering av det material som lagrats på hög (G:\ verksamhetsstöd\IT och telefoni\avbrottsplan \Avbrottsplan IT\avbrott LÖNESYSTEM och G:\Ekonomi). Övriga frågor och ekonomiärenden uppdateras nu i lönesystemet och i förekommande fall telefonkontakt med berörda.
Drabbad	Anställda inom SEF

11.VIRUS I ARBETSSTATIONEN	
Allmänt	Virus eller motsvarande smitta
Accepterad avbrottstid	5 arbetsdagar
Information	Inget behov.
Vid driftstörning/avbrott/ reservrutin	Vid misstanke om smitta med datavirus eller motsvarande gäller följande: 1. Rör ingenting. 2. Ring Service Desk 08-508 48 200 3. Invänta besked och åtgärdsförslag från Service Desk
Återgång till normalläge	Ingen åtgärd.

12.ELAVBROTT I KONTORSLOKALERNA	
Allmänt	Elförsörjningen till kontorslokalerna
Accepterad avbrottstid	2 arbetsdagar
Information	Meddela växeln.
Vid driftstörning/avbrott/ reservrutin	Ring felanmälan hos Fastighetskontoret 08-508 28 680. och anmäl strömavbrottet. Reservrutinen är att använda mobiltelefon och bärbar dator på anvisad plats.
Återgång till normalläge	Informera på hemsidan att vi har haft driftstopp. Meddela växeln normalläge

14.DRIFTSTOPP HOS S:T ERIK KOMMUNIKATION	
Allmänt	Fiberförbindelsen till Volvo-IT
Accepterad avbrottstid	3 arbetsdagar
Information	Rapportera till St Erik kommunikation. Beroende på felets art även informera på hemsidan om det är möjligt samt meddela växeln.
Vid driftstörning/avbrott/ reservrutin	Reservrutinen är att använda mobiltelefon och bärbar dator.
Återgång till normalläge	Informera på hemsidan att vi har haft driftstopp.

Bilagor till IT-AVBROTTSPLAN FÖR S:T ERIK FÖRSÄKRINGS AB

Fastställt av styrelsen 220523

Innehållsförteckning

Allmänt

Detta dokument innehåller alla bilagor som refereras i dokumentet IT-avbrottsplan.

Revisionshistorik

Version	Datum	Namn	Beskrivning
V01	2017-05-03	Said Tabari	Skapat dokument
V02	2019-05-27	Erik Fischer	Uppdaterade leverantörer och kontaktuppgifter, reviderad utformning av katastrofgrupp.
V03	2020-04-27	Said Tabari	Uppdatering av kontaktuppgifter

BILAGA 2a Kontaktlista System/Funktion	Företag	Kontaktperson	Kontaktuppgifter
Totalt IT-drifts ansvar	Tieto	Patrik Burlin Kundansvarig	+46-070 534 9168 https://11800.stockholm.se Patrik.Burlin@tietoevry.com
Avtalspart med Tieto	SLK/SLK-IT		
Ansvar avtal Tieto	SLK-IT	X, Kundansvarig	
idPortalen	Tieto	Per Ågren, Expert idPortalen	0702-379 428 support: 08-508 48 200 https://11800.stockholm.se
Teknikleverantör brandvägg	S:t Erik Komm		020-83 83 00, arende@servicecentrum.stockholm.se
Driftspartner brandväggsöppning	TDC		arende@servicecentrum.stockholm.se
INSMAN	iFACTS	Ulf Åkesson, Kundansvarig	0735-033 250 support: 040-10 77 99 Ulf.akesson@ifacts.se support@ifacts.se
IA	AFA	Kundtjänst	08-696 40 00iasupport@afaforsakring.se
Ombraco/Hemsidan	Graz	Jonas Olsson	+46 704 493 006
Agresso	Tieto		08-508 11800 https://11800.stockholm.se
Visma Agda	SBR	Daniel Hök	070-534 64 13 daniel.hok@hhlonekonsult.se
FinLarm	Finlarm	Mikael Wessman	08-562 920 92, micke@finlarm.se
Återkalla larm	Nokas	Support/återkalla	08-619 50 00

Fastställt av styrelsen 220523

BILAGA 2b –Lathund avbrott IT

Avbrott IT		
Typ av fel	**System**	**Kontakta**
Lösenord/anv.namn	https://11800.stockholm.se	Tieto
Funktion fungerar inte	INSMAN	iFACTS
Systemet fungerar inte	INSMAN	Insman
E-post/kontorssystem	Officepaketet etc	Tieto
Fel på hemsida	Umbraco	Graz
Telefon/mobilfel	Telefoni	ServiceCentrum
Ekonomi-Lönesystem	Visma Agda	HH Lönekonsult
EL-avbrott	EL (Fortum)	Fastig.kontoret
Larmet går/återkalla	Finlarm	Nokas
Incidentrapportering	IA	AFA

Kontaktlista		
Företag	**Person**	**Telefon**
iFACTS	Support	040-10 77 99
Tieto	Servicedesk	08-508 11800
Telefoni/Mobil	Tieto/ServiceCenter	08-508 11800
Intellecta	Bengt Wennström	08-506 28 600
HH Lönekonsult	Daniel Hök	070-534 64 13
Fastig.kontoret	Felanmälan	08-508 28 680
Nokas	Support	08-619 50 00
AFA	Kundtjänst	08-696 40 00

Fastställt av styrelsen 220523

BILAGA 3 – Loggbok Avbrott IT

Inledande	Förklaring
Larmet	*När det uppstått en störning och/eller ett avbrott, där åtgärden inte hanteras enligt normal drifthantering och/eller att omfattningen kan vara svår att uppskatta. Larmet ska gå till IT-ansvarig*
Inledande aktivitet	*Innan åtgärden för att återskapa normalläge påbörjas, ska IT-ansvarig genomföra en snabb analys av omfattning och ev konsekvenser*
Kontinuitetsplan	*Den person som tar emot larmet kontrollerar om kontinuitetsplanen ska aktiveras enligt villkoren nedan. Om kontinuitetsplanen ska aktiveras ska katastrofgruppen sammankallas snarast. Se vidare avsnitt ”Katastrofgrupp”*

Loggning	Kommentar
Datum för loggning	
IT-Ansvarig	
Tidpunkt avbrott	
Vad *Specificera den funktionalitet som inte fungerar* *-system/tjänst, dator, applikation* *-ev person-, materiella-, immateriella- samt ekonomiska skador*	
Vem *Vem upptäckte avbrottet?*	
Ansvarig *Vem ”äger” ärendet?*	
Avbrottstid *Hur lång tid beräknas avbrottet vara?*	
Vilka *Vilka drabbas av avbrottet?* *-användare (antal), kunder etc*	
Anmäld i IA *Ja/Nej och ev löpnummer*	
Avbrottsplan IT aktiveras? *Ja/Nej*	
Åtgärder *Vilka åtgärder kommer att vidtas eller har vidtagits?*	
Funktionsansvariga, återställandet *Specificera vem/vilka som ansvarar för att återställa de olika funktionerna som avbrottet berör*	
Huvudansvaret, återställandet *Vem/vilka har huvudansvaret samt samordnande roll för de återställande aktiviteterna?*	
Införande av uppgifter *Notera datum när uppgifterna i denna logg skrevs in i dokumentet ”Loggbok avbrott IT” under G, när normalläge åter gäller.*	

Fastställt av styrelsen 220523

BILAGA 4 - Katastrofgrupp Avbrott IT

Normal grupp

Namn	Titel	Roll i katastrofgruppen
	VD	Ordförande
	IT-Ansvarig	Sammankallande/Informatör
	Risk Manager	Sekreterare
	Bolagsjurist	Dataskyddsombud

Ersättare utses normalt i fallande ordning, ex. VD-IT Ansvarig, IT-Ansvarig – Risk Manager osv.

Vid behov kan:

- gruppen utökas med ytterligare personer från verksamheten eller externt,
- en tillfälligt sammansatt katastrofgrupp, med vid tillfället befintliga resurser, sammankallas.

Fastställt av styrelsen 220523

BILAGA 5 – Textförslag felmeddelande vid driftstopp

Textförslag felmeddelande vid driftstopp/avbrott IT

System	Typ av fel	Meddelandet placeras	Text
IA			
	Systemet har extremt långa svarstider	• Notis på SEFs hemsida • Mail till superanvändare	”Teknisk störning IA För närvarande har vi längre svarstider än normalt i systemet. Vi arbetar med att lösa problemet och beklagar störningen.
	Systemet ligger nere helt	• Notis på SEF:s hemsida • Mail till superanvändare • Vid längre avbrott, notis på stadens intranät	” Driftstörning IA Just nu kan du inte nå stadens incidentrapporteringssystem IA. Vi arbetar intensivt för att lösa problemet och beklagar de olägenheter som störningarna innebär för dig.
		•	
INSMAN	**Systemet har extremt långa svarstider**	• **”popruta” i systemet**	**”Teknisk störning INSMAN För närvarande har vi längre svarstider än normalt i systemet. Vi arbetar med att lösa problemet och beklagar störningen.**
	Systemet ligger nere helt	• Mail till ev berörda • Vid längre avbrott, notis på stadens intranät.	” Driftstörning INSMAN Just nu kan du inte nå systemet INSMAN. Vi arbetar intensivt för att lösa problemet och beklagar de olägenheter som störningarna innebär för dig. ”

Fastställt av styrelsen 220523

Hemsidan	Hemsidan har långa svarstider	• Lägga ut info på hemsidan om det går	” ”Teknisk störning För närvarande har vi längre svarstider än normalt i systemet. Vi arbetar med att lösa problemet och beklagar störningen.
	Vissa sidor eller funktioner inte fungerar	• Lägga ut info på hemsidan om det går	”Teknisk störning För närvarande har vi tekniska problem med vissa sidor och funktioner på hemsidan. Det innebär att du inte kan komma åt vissa sidor eller funktioner på sidan. Vi arbetar intensivt för att lösa problemet och beklagar de olägenheter som störningarna innebär för dig.

BILAGA 6 – Manuell skadeanmälan till externa skadereglerare

Uppgifter	Notering
Skadedatum	
Anmälningsdatum	
Incidentgrupp	
Drabbad	
Incidenttyp	
Berörd enhetet	
Anmälare till SEF	
Skadeplats	
Fastighetsbeteckning	
Beskrivning	
IA löpnr ifall sådant finns Blir skadenr hos skadereglerare	
Inrapporterat till skadereglernigsföretag	
Anmälare till skaderegleringsföretag	

Fastställt av styrelsen 220523

Katastrofplan för S:t Erik Försäkrings AB

FASTÄLLD AV STYRELSEN 2022-05-23

Innehållsförteckning

1. Inledning

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”. Planen ska revideras årligen eller vid behov.

Syftet med denna katastrofplan är att den ska fungera som en åtgärdsplan möjlig att använda vid större oförutsedda händelser som drabbar bolaget.

Bilaga 1 fastställs av VD och ska hållas löpande uppdaterad och tillgänglig för styrelsen.

2. Verksamheten

Stockholms kommunfullmäktige har beslutat att *S:t Erik Försäkring ska ha som uppgift att svara för att det finns en effektiv riskfinansiering av anläggningar och verksamheter ägda av staden och närstående bolag genom ökad konkurrensutsättning. Bolaget ska förmedla försäkringslösningar, minimera försäkringskostnaderna och förbättra riskhanteringen för samtliga berörda enheter inom kommunkoncernen. S:t Erik Försäkring ska vara det bästa och mest kostnadseffektiva alternativet för stadens förvaltningar och bolag.*

Verksamheten hos S:t Erik Försäkring består i att identifiera risker och analysera försäkringsbehovet hos bolagets kunder. Bolaget ska stimulera till att förebygga och begränsa skador inom kommunkoncernen. När det gäller försäkring har bolaget en skyldighet att erbjuda försäkring till bolagets kunder. Normalt utfärdas försäkring direkt av bolaget. Försäkringar som bolaget inte får utfärda eller av andra skäl inte kan tillhandahålla direkt ska upphandlas enligt gällande upphandlingsregler. Vid inträffad skada hos kund har S:t Erik Försäkring skyldighet att ta hand om skadesituationen på det sätt och i den omfattning som är normalt inom försäkringsbranschen.

Bolagets prioriterade arbetsuppgifter som måste fungera

- Årligen, normalt vid årsskiftet, ska S:t Erik Försäkring utfärda försäkringsbrev till varje kund.
- Vid inträffad större skadehändelse ska bolagets skadereglerare snarast infinna sig vid skadeplatsen.
- Bolaget ska skyndsamt betala ut försäkringsersättning efter skriftlig skaderapport från skadereglerare.
- Inom det skadeförebyggande området fungerar bolaget som katalysator.
- Bolaget ska vårda och utveckla det egna försäkringssystemet som bland annat har till uppgift att utfärda försäkringsbrev.
- Skaderapporteringssystemet IA ska driftas och underhållas av bolaget.
- S:t Erik Försäkring ska köpa återförsäkring för risker ovanför bolagets självbehåll.
- S:t Erik Försäkring ska ha rutiner och system för god redovisning och bokföring av skadehändelser och ekonomiska transaktioner. Detta arbete ska ske enligt stadens riktlinjer och Finansinspektionens anvisningar.
- Kunder och allmänhet måste kunna nå bolaget via telefon och hemsida.

3. Vitala resurser

Bolaget har identifierat vilka vitala resurser som behövs för att kunna uppfylla de prioriterade arbetsuppgifterna.

- Nyckelfunktioner
- IT
- Lokaler

3.1 Nyckelfunktioner

I den egna organisationen utgör VD, samtliga anställda samt vissa outsourcade verksamheter nyckelfunktioner. Bolaget har två kundansvariga, en riskhanteringsansvarig, en skadeansvarig, en bolagsjurist, en IA ansvarig och en ekonomiansvarig.

För de aktuella tjänsterna gäller att ersättaren kanske inte fullt ut kan ta över samtliga arbetsuppgifter. Emellertid finns kompetens hos konsulter, närstående bolag och förvaltningar i staden som kan utnyttjas.

Kontaktuppgifter till externa parter framgår av bilaga 1.

Väldigt få arbetsmoment kräver akuta insatser av bolagets personal. De mest akuta momenten är att bolaget sköter sina betalningar. Dessa kan utföras av bolagets personal eller av bolagets styrelse. Bolaget bedöms klara sig utan sin ordinarie personal utan problem i två veckor. Därefter krävs engagemang från utomstående personer. I ett sådant läge krävs ersättare i enlighet med punkten 3 ovan.

VD
I det fall VD måste ersättas kommer Jan Willgård, S:t Erik Livförsäkring AB, ta över ansvaret för verksamheten som tillförordnad VD. Detta ansvar gäller till dess att styrelsen beslutat om en ersättare.

Kundansvarig
I det fall någon av de båda kundansvariga måste ersättas kommer den andra kundansvariga att ta över arbetsuppgifterna fram till dess att en permanent ersättare kommit på plats. Om båda kundansvariga måste ersättas kontaktas försäkringsförmedlare, se bilaga 1.

Ekonomifunktionen
Bolagets ekonomifunktion sköts av en ekonomiansvarig. Funktionen kan tillfälligt skötas av konsult enligt gällande uppdragsavtal, bilaga 1.

Skadeansvarig
Skadeansvarige ersättas vid behov av VD, alternativt genom att funktionen tillfälligt sköts av skaderegleringsfunktionen genom gällande uppdragsavtal.

Skaderegleringsfunktionen
Skadereglering sköts genom uppdragsavtal, bilaga 1. I de fall uppdragstagaren behöver ersättas sker direktupphandling av annan leverantör, förslagsvis enligt bilaga 1.
Aktuariefunktionen

Aktuariefunktionen sköts genom uppdragsavtal med S:t Erik Livförsäkring. I de fall uppdragstagaren behöver ersättas sker direktupphandling av annan leverantör, förslagsvis enligt bilaga 1.

Riskhanteringsfunktionen
Riskhantering sköts genom uppdragsavtal, bilaga 1, och riskhanteringsansvarig kommer vid behov att ersättas av annan person från uppdragstagaren enligt gällande uppdragsavtal. I de fall uppdragstagaren måste ersättas sker direktupphandling av annan leverantör, förslagsvis enligt bilaga 1.

Regelefterlevnadsfunktionen
Regelefterlevnaden sköts genom uppdragsavtal, bilaga 1, och regelefterlevnadsansvarig kommer vid behov att ersättas med annan person från uppdragstagaren enligt gällande uppdragsavtal. I de fall uppdragstagaren måste ersättas sker direktupphandling av annan leverantör, förslagsvis enligt bilaga 1.

IA funktionen
IA-ansvarig ersätts vid behov av skadeansvarig. Mindre åtgärder kan vid akuta behov beställas hos AFA Försäkring, se bilaga 1, som tillhandahåller eller driftar systemet.

3.2 IT och telefoni

Hur bolaget ska hantera en större IT-systemkrasch beskrivs i S:t Erik Försäkrings IT-avbrottsplan.

3.3 Lokaler

När det inte är möjligt att använda bolagets egna lokaler är det fullt möjligt att bedriva verksamheten från en annan geografisk plats. Dagens teknik gör det exempelvis möjligt att bedriva all verksamhet från hemmet för samtliga anställda. Att det inte uppstår några större problem beror på att samtliga system går att nå via internet samt att de anställda har tillgång till bärbara PC-datorer.. Datorer kan även avropas enligt gällande avtal med Tieto, vidare finns möjlighet till arbetsplatser vid andra enheter i staden.

4. Krisledningsorganisation

Bolagets krisledningsgrupp består av följande funktioner.

<u>Krisledning- och kommunikationsansvarig (Ordförande och sammankallande)</u>

VD eller VD:s ställföreträdare. Ansvarar även för att ta kontakt med Stadsledningskontorets Kommunikatör i Beredskap vid behov.

<u>Administrativ funktion</u>

Ansvara för att planera och genomföra de administrativa arbetsuppgifterna kopplat till krisledningsarbetet, t ex teknisk utrustning, bemanning.

<u>Samverkansfunktion:</u>

Ansvarar för att identifiera och samordna eventuellt arbete med externa aktörer.

Analysfunktion

Ansvarar för att omvärldsbevaka och följa händelsens utveckling, bygga upp en samlad lägesbild och lägesuppfattning, samt att analysera konsekvenser på kort och lång sikt. Analysfunktionen ska stödja med handlingsalternativ och förslag på åtgärder.

Funktionerna bemannas upp av tillgänglig personal inom bolaget. Beroende på händelse kan en och samma person utföra flera av de olika funktionerna.

4.1 Aktivering av krisledningsorganisationen

Krisledningsorganisationen aktiveras av bolaget VD eller dennes företrädare. Samtliga bolagets anställda ska rapportera till VD händelser som skulle kunna leda till en kris för bolaget. Skadeansvarig har ett särskilt ansvar att bevaka eventuella händelser kopplat till bolagets skadeprocess. Se även bolagets riktlinjer för rapportering av händelser av väsentlig betydelse.

BILAGA 1

Fastställd av VD 2019-05-27

Skadereglering		
Sedgwick (Egendom och ansvar)	08-98 33 60 info@se.sedgwick.com	Gällande uppdragsavtal
Crawford & Co (Olycksfall)	08-514 200 00 sterik.olycksfall@crawco.se claes.frick@crawco.se	Gällande uppdragsavtal
SFOS	www.sfos.org	Branschorgan oberoende skadereglerare
Ekonomifunktionen		
Marsh	08-412 42 00	Gällande uppdragsavtal
Aon	08 697 40 00	
Aktuariefunktionen		Direktupphandlas
AON	08-614 17 00	
Marsh	08-412 42 00	
PwC	010-213 30 00	
Försäkringsförmedlare		
Söderberg & Partners	08-451 50 00	Gällande uppdragsavtal
WILLIS	08-463 89 00	Direktupphandlas
Marsh	08-412 42 00	Direktupphandlas
AON	08-697 40 00	Gällande uppdragsavtal (återförsäkring)
Regelefterlevnadsfunktionen		
Wesslau & Söderqvist	08-407 88 00	Gällande uppdragsavtal
Mats Björkbom	08-407 88 00	
Johan Grenfalk	076-525 13 17	
FCG Risk & Compliance	08-410 75 910	Direktupphandlas
Riskhanteringsfunktionen		
Periculo AB	072-336 91 45	Gällande uppdragsavtal
George Englund	072-336 91 44	
Rasmus Nilsson	073-336 16 38	
Wesslau & Söderqvist	se ovan	Direktupphandlas
IA		
AFA Försäkring kundtj.	08-696 40 00 iasupport@afaforsakring.se	Gällande avtal avseende IA finns

PLACERINGSRIKTLINJER FÖR S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLT AV STYRELSEN 2022-05-23

1 Generella principer

1.1 Styrdokument

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Utöver detta regleras finansverksamheten i S:t Erik Försäkring av finanspolicy för kommunkoncernen Stockholms stad och finanspolicy för Stockholms Stadshus AB. S:t Erik Försäkring skall löpande tillse att det i verksamheten finns placerat kapital som minst svarar mot det åtagande S:t Erik Försäkring har i form av försäkringsrisker, placeringsrisker och riskmål. Kapitalet skall vid var tid vara placerat på ett betryggande sätt och så att S:t Erik Försäkrings betalningsberedskap är tillfredställande.

Dessa placeringsriktlinjer ersätter placeringsriktlinjer för S:t Erik Försäkrings AB som fastställdes av styrelsen den 27 maj 2020.

1.2 Syfte med placeringsriktlinjerna

Syftet med placeringsriktlinjerna är att ange principer för placering av samtliga tillgångar. Värdering av tillgångarna framgår av bolagets ”Riktlinje för värdering av tillgångar och skulder, bolagets kapitalbas och finansieringsplan på medellång sikt”.

2 Ansvarsfördelning och riskstyrning

2.1 Ansvarsfördelning

2.1.1 Bolagsstyrelsens ansvar

Styrelsen ska:

- Årligen fastställa placeringsriktlinjerna, samt ansvara för att de följs och fortlöpande pröva om de behöver ändras.
- Årligen anta finanspolicyn för Stockholms Stadshus AB.

2.1.2 VD:s ansvar

VD ska:

- Tillse att sakbolagets finansiella tillgångar placeras i enlighet med placeringsriktlinjerna.
- Föreslå styrelsen förändringar av placeringsriktlinjerna. VD ska då begära in information från bolagets riskhanteringsfunktion avseende påverkan på bolagets riskprofil avseende planerade förändringar. Samråd ska ske med internbanken inom Stockholms stad inför revidering och fastställande av placeringsriktlinjerna.

3 S:t Erik Försäkrings placeringsstrategi

Tillåtna placeringstillgångar och principer för placeringarna av S:t Erik Försäkrings finansiella tillgångar beskrivs nedan.

3.1 Placeringsstrategi

S:t Erik Försäkring ska placera sina finansiella tillgångar på ett aktsamt sätt så att god betalningsförmåga upprätthålls vid varje tidpunkt. Hänsyn ska tas till eventuell profil på förväntade skadeutbetalningar, villkor i gällande återförsäkringsavtal, SCR-kvot och resultatet av ORSA.

3.2 Riskmål

Enligt 7 kap. Försäkringsrörelselagen ska kapitalbasen minst uppgå till solvenskapitalkravet (SCR), dock aldrig mindre än minimikapitalbeloppet (MCR).

Bolagets aktuella riskmål framgår av Riktlinje för riskhantering avsnitt 7.

3.3 Tillåtna tillgångsslag

Vid val av tillåtna tillgångsslag har S:t Erik Försäkring utgått ifrån 6 kap. Försäkringsrörelselagen. Både aktsamhet och riskspridning har tagits hänsyn till för att skapa en balanserad flexibilitet.

Tillåtna tillgångsslag framgår av Riktlinje för riskhantering avsnitt 9.3 och 9.4.

Om det av driftsskäl inte kan undvikas att medel placeras på annat sätt ska så ske med beaktande av kommunkoncernen Stockholm stads begränsningar enligt nedanstående tabell och gällande regelverk avseende förmånsrättstillgångars kvalité (se Riktlinje för värdering av tillgångar och skulder). Placeringen får endast avse vad som är nödvändigt till omfattning och tid samt ska ske efter gemensam bedömning av VD, styrelse, riskhanteringsfunktionen, regelefterlevnadsfunktionen samt internbanken.

Kortfristig rating, lägst		Långfristig rating, lägst		Max exponering per motpart eller instrument (mnkr)
Standard & Poor´s	Moody´s	Standard & Poor´s	Moody´s	
Svenska staten		Svenska staten		Obegränsat
A-1	P-1	AAA	Aaa	4 000
A-2	P-2	AA-	Aa3	2 500
		A-	A3	2 000
		BBB+	Baa1	1 000

4 Risk

Vid tillgångarnas placering ska en begränsad och rimlig risknivå tillämpas. Hantering av risker framgår av bolagets Riktlinje för riskhantering

5 Asset/Liability Management (ALM)

S:t Erik Försäkring ska identifiera och bedöma skillnaderna (mismatch) mellan tillgångar och skulder, åtminstone då det gäller villkor och valuta. Då endast en valuta förekommer är det främst avseende villkor som skillnader kan uppstå. Vid beaktande av placeringar ska villkor

avseende tillgångarna i rimlig mån matcha motsvarande villkor avseende skulderna. Vid ändringar av tillgångsslag ska relevanta stress- och scenariotester utföras innan tillgångarna byts ut för att bedöma skillnaderna och eventuell påverkan på risken.

6 Intressekonflikter

Bolaget ingår i kommunkoncernen Stockholms stad och utgör dess captivebolag. Då bolagets tillgångar placerats i kommunkoncernen hanteras eventuella intressekonflikter genom bolagets riskhantering av finansiella tillgångar, vilka framgår av Riktlinje för riskhantering.

7 Uppföljning

Det ska finnas en oberoende funktion för riskhantering som löpande ska följa upp risk bl.a. utifrån dessa placeringsriktlinjer. Se vidare i dokumentet Riktlinjer för riskhantering och instruktion för riskhanteringsfunktionen.

Policy för bisyssla för anställda hos S:t Erik Försäkring

Styrelseordföranden ska besluta om eventuella avsteg från principen att VD inte äger bedriva verksamhet (inneha bisyssla) vid sidan av sin anställning i bolaget.

Beträffande övriga anställdas eventuella bisysslor fattas beslut av VD.

Anställda vid bolaget ska anmäla bisyssla och lämna de uppgifter, som arbetsgivaren anses behöva för att bedöma bisysslan.

Förtroendeuppdrag i fackliga, politiska eller ideella organisationer är inte bisyssla.

Förfrågan ska göras regelbundet om eventuella bisysslor och ska redovisas på bifogad blankett.

Fastställd av styrelsen 2022-05-23

UPPGIFT OM BISYSSLOR

Härmed förklarar jag mig icke inneha sådan bisyssla som gör att jag hamnar i lojalitetskonflikt eller på något annat sätt hindras eller påverkas i arbetet hos S:t Erik Försäkring.

År	Uppgiftsdatum	Namnteckning ……

Fastställd av styrelsen 2022-05-23

S:T ERIK FÖRSÄKRINGS AB:S POLICY FÖR MOBILTELEFONER

FASTÄLLD AV STYRELSEN 2022-05-23

Innehållsförteckning

1. Inköp av mobiltelefoner och tecknande av abonnemang

Beslut om inköp av mobiltelefoner skall fattas av VD. Vid inköp och tecknande av abonnemang ska stadens upphandlingsavtal utnyttjas i möjligaste mån. Telefon- och abonnemangsuppgifter ska registreras i enlighet med dessa avtal. Vid abonnemangsteckning skall specificerad faktura beställas.

2. Användning av mobiltelefoner

Vid användning av mobiltelefoner gäller på samma sätt som för vanliga telefoner att privatsamtal under tjänstetid endast är tillåtet i begränsad omfattning och att sådan användning, om inte särskilda omständigheter föreligger, ska avse korta samtal.

Anställd som får privat mobiltelefonanvändning betald av arbetsgivaren ska enligt skattelagstiftningen förmånsbeskattas och sociala avgifter ska betalas för förmånsbeloppet.

När mobiltelefonen utnyttjas under semester och annan ledighet skall privatsamtal betalas av innehavaren. Vid fakturakontroll ska därför respektive användare notera sådana privata samtal på samtalsspecifikationen. Beloppet dras sedan på lönen. Om telefonen används privat för SMS-meddelanden, WAP-funktioner, e-post e. d. ska även detta betalas av innehavaren.

POLICY FÖR ORSA INOM S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Syfte

Denna policy har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna är föremål för revidering årligen och skall fastställas av styrelsen för S:t Erik Försäkrings AB.

Syftet med denna policy är att beskriva och fastställa principerna för arbetet med ORSA (Den egna risk- och solvensbedömningen, oftast benämnd efter den engelska termen, ”Own Risk and Solvency Assessment”) inom S:t Erik Försäkrings AB (”S:t Erik”, bolaget).

Den Egna risk- och solvensbedömningen tjänar bland annat syftet att:

a) Bedöma S:t Eriks totala solvensbehov på kort (upp till ett år) och medellång sikt (tre år) med beaktande av riskprofil, risktolerans och affärsstrategi,

b) vara underlag för finansieringsplan,

c) ge styrelsen en fördjupad förståelse för de risker som verksamheten är förknippad med och utmana bedömningen av dessa

d) ingå som en integrerad del i affärsstrategin och beaktas vid företagets strategiska beslut, affärsplaner och budget,

e) Bedöma S:t Eriks fortlöpande efterlevnad av bestämmelserna om solvens- och minimikapitalkrav.

f) Bedöma hur betydande skillnaderna är mellan S:t Eriks riskprofil och de antagande om risker som har legat till grund för beräkning av solvenskapitalkravet.

2 Bakgrund

ORSA-processen ingår som ett obligatoriskt moment enligt Solvens II-regelverket i försäkringsföretags bolagsstyrnings- och riskhanteringssystem.

ORSA är en central process i ledningen och styrelsens utvärdering av bolagets risker och kapitalisering. ORSA knyter ihop regelverken kring kapitalkrav, företagsstyrning och rapportering till en enda process, som ska mynna ut i en rapport med kvantitativa och kvalitativa slutsatser.

Analysen och slutsatserna ska omfatta beroenden och samspel mellan solvenskapital, kapitalanskaffning och förvaltning samt ordningen för beslutsfattande och affärsplanering. Det ska hela tiden finnas hållbara bedömningar av risk och motsvarande kapitalbehov som en grund för beslut.

I processen ska bolaget bedöma sitt totala kapitalbehov och att riskhanteringssystemet är effektivt. Processen innefattar både kvalitativ och kvantitativ analys. En central del i den kvantitativa analysen och i kvantifieringen av kapitalbehovet är prognoserna för bolagets

framtida finansiella ställning under både en förväntade utveckling och olika alternativa (stressade) mer negativa scenarier.

Genom arbetet med ORSA skall S:t Erik beräkna hur mycket kapital som fordras för att bedriva verksamheten på såväl kort som lång sikt. Detta mer övergripande kapitalbehov (i direktivet kallat totalt solvenskrav) är inte detsamma som solvenskapitalkravet.

Solvenskapitalkravet kan beräknas enligt en standardmodell som finns beskriven i Solvens II-direktivet (SCR), men företagen har också möjlighet att helt eller delvis istället använda en egen intern modell, som dock måste godkännas av tillsynsmyndigheten. S:t Erik Försäkring använder standardmodellen. I ORSA-processen ingår det att bedöma om standardformeln är lämplig utifrån riskprofilen eller om det krävs ytterligare kapital för att täcka bolagets risker, det vill säga om det övergripande kapitalbehovet är större än solvenskapitalkravet. Detta kapitalbehov ska i så fall också kvantifieras.

Genom kravet på en egen bedömning av totalt kapitalbehov och riskprofil skapas en koppling mellan de regelstyrda kraven på kapital och riskhantering och företagens egen bedömning i dessa frågor. Genom bedömningen av den egna risken och solvensen ges företaget också vissa möjligheter att bedöma för- och nackdelar med att ta fram en intern modell för beräkningen av kapitalkraven. Bedömningen kan slutligen sägas utgöra en sammanfattning av riskhanteringssystemet.

3 Metod och process

3.1 Initiering av ORSA

ORSA ska minst genomföras årligen.

En extraordinär ORSA ska även initieras vid konstaterade överträdelser eller väsentligt förhöjd risk för överträdelse av bolagets toleransnivåer för kapitalisering (solvenskvot) eller försäkringsrisker (maximal riskexponering).

En väsentligt förändrad riskprofil ska också medföra att en extraordinär ORSA initieras. Faktorer som ska ingå i bedömningen av om väsentliga förändringar har skett är vid förändring av självbehåll, omfattning av återförsäkring, försämrad betalningsförmåga hos viktiga återförsäkringsmotparter, betydande ökningar av skadekostnader, väsentlig ändring av villkor samt introduktion av nya produkter. Även överträdelse av eller förhöjd risk för överträdelse av andra limiter än de gällande solvenskvot och riskexponering ska beaktas i utvärderingen.

ORSA initieras av styrelsen. VD ansvarar för att underlag i form av tidplaner, beskrivningar och rapporter i genomförandet av ORSA framläggs för styrelsen.

Riskhanteringsfunktionen ansvarar i sin övervakning av bolagets riskprofil att VD utan dröjsmål informeras om att limiter överträtts eller om en väsentlig förändring kan ha inträffat vilket ska medföra att styrelsen bedömer om en extraordinär ska initieras eller ej. Även enskilda styrelseledamöter, VD och aktuarie har rätt att och ansvar för att till VD föreslå att en extraordinär ORSA initieras om de bedömer att ovan angivna förutsättningar gäller. När VD fått information om att en extraordinär ORSA behöver genomföras eller ska övervägas ska

VD utan dröjsmål informera styrelsens ordförande som beslutar om styrelsen ska sammankallas.

3.2 Metod

Metoden för ORSA går ut på att identifiera samtliga väsentliga risker samt estimera och bedöma S:t Eriks kapitalbehov genom följande steg:

a) Analys av S:t Eriks finansiella position med beaktande av strategi, affärsplan och marknadsläge,

b) Identifiering av samtliga väsentliga risker,

c) Framtagande av S:t Eriks riskprofil,

d) Uppskattning av kapitalbehovet för identifierade risker

3.2.1 Analys av S:t Eriks finansiella position, strategi och förväntade marknadsutveckling

Analys av S:t Eriks nuvarande finansiella ställning, förväntad marknadsutveckling, framtida strategi och finansiell utveckling ska avse utvecklingen de kommande tre åren.

3.2.2 Identifiering av samtliga väsentliga risker

Alla väsentliga risker skall definieras, identifieras och kapitalbedömas. Riskbedömningen ska ske per riskkategori. Både kvantitativa och kvalitativa metoder skall användas i processen för simulering av nuvarande och framtida kapitalbehov.

Åtminstone följande riskkategorier ska ingå i S:t Eriks utvärdering av väsentliga risker:

Risker som ingår i standardformeln:

- Försäkringsrisk, risken för förlust eller negativ förändring avseende försäkrings-förpliktelsens värde till följd av otillräckliga tariffer och antagande om avsättningar.
- Marknadsrisk, risken för förlust eller negativ förändring avseende den finansiella ställningen som direkt eller indirekt orsakas av svängningar i nivån eller volatiliteten när det gäller marknadspriserna för tillgångar, skulder och finansiella instrument.
- Motpartsrisk, risken till följd av oväntade brister i betalningsförmågan, viljan att betala eller försämrad kreditvärdighet hos företagets motparter och gäldenärer.
- Operativ risk, risken för förlust till följd av att interna rutiner har visat sig otillräckliga eller fallerat, orsakad av personal eller system eller av externa händelser. Operativa risker finns i all verksamhet inom organisationen, i verksamhet som lagts ut till underleverantörer och i all samverkan med externa parter.

  Typiska exempel på operativa risker är:

  a) IT-risk, d.v.s. risken för att något av S:t Eriks IT-system eller den elektroniska kommunikationen inte fungerar som avsett.

  b) Regelefterlevnadsrisker vilket är risken för att bryta mot regelverket.

Risker som bolaget är eller kan vara exponerat för utöver de som ingår i standardformeln:

- Likviditetsrisk, risken för att S:t Erik inte kan avyttra placeringar och andra tillgångar för att uppfylla sina finansiella åtaganden när de förfaller till betalning.

- Strategisk risk, vilket refererar till S:t Erik styrelses och lednings förmåga att planera, organisera och kontrollera verksamheten d.v.s. risken för ett misslyckande att anpassa rörelsen till trender i nya försäkringstyper, parera för ökad konkurrens eller generellt reagera på förändringar i marknadsförutsättningarna.
- Ryktesrisk, vilket refererar till risken att inkomster och kapital påverkas negativt pga. ett skadat varumärke.

3.2.3 Uppskattning av kapitalbehovet för identifierade risker

Efter att S:t Eriks riskprofil har blivit identifierad och definierad skall kapitalåtgången uppskattas. Processen skall ske enligt följande steg:

3.2.3.1 Utvärdering per riskkategori

Varje riskkategori som har identifieras måste utvärderas individuellt. Utvärderingen måste dokumenteras och alltid resultera i en kvalitativ bedömning. Även en kvantitativ bedömning skall genomföras om så är möjligt.

3.2.3.2 Utvärdering av hur risker är hanterade och kontrollerade

Även om inte alla risker kan kvantifieras så skall de beskrivas och hanteringen av dessa dokumenteras och utvärderas.

3.2.3.3 Kapitalutvärdering

Uppskattningen av kapitalbehovet skall grunda sig på den kvalitativa och kvantitativa analysen enligt ovan. I utvärderingen bör även korrelation mellan olika riskkategorier tas i beaktande. Uppskattat kapitalbehov ska jämföras med S:t Eriks analys av nuvarande och framtida finansiella situation. S:t Eriks förväntade kapitalutveckling, planerad utdelning och möjliga kapitalanskaffningskällor skall framgå från utvärderingen.

3.2.3.4 Framtagande av stressade scenarier

För bolagets riskprofil och affärsplan relevanta scenarier som innebär en negativ utveckling ska tas fram och utvärderas för att bedöma bolagets motståndskraft och identifiera åtgärdsbehov eller beredskapsplaner.

Scenarierna bör sammantaget innefatta utvärdering av de mest väsentliga hoten mot bolagets kapitalisering. Faktorer att beakta vid utformningen är exempelvis ökade skadefrekvenser, att stora skador eller katastrofer inträffar, försämrad betalningsförmåga hos återförsäkrare, ökade kostnader för drift eller återförsäkring samt regulatoriska förändringar.

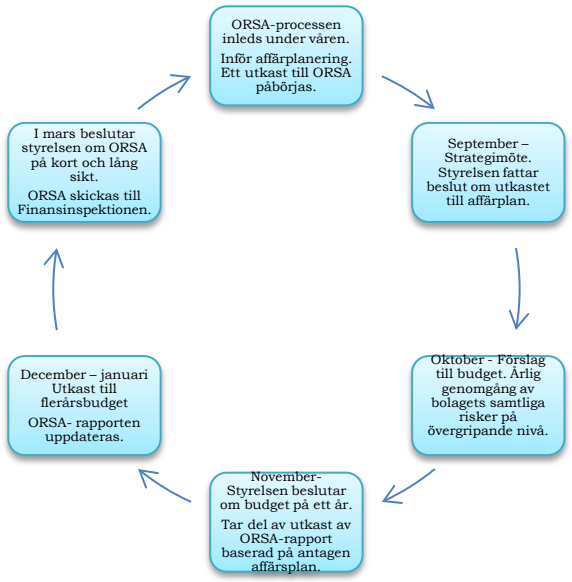
3.3 Process

3.3.1 Årsprocess för ORSA

Följande är processen för den ordinarie, årliga ORSA:n:

1. ORSA- processen inleds under våren då verksamheten har affärsplanering. En bedömning utförs om eventuella framtidsplaner och förväntad marknadsutveckling föranleder att ett utkast till ORSA ska tas fram till styrelsens strategimöte.
2. Vid styrelsens strategimöte i september fattar styrelsen beslut om utkastet till affärsplan (verksamhetsplan) och beaktar då resultatet av ORSA kopplat till relevanta strategiska beslut.

3. I oktober utarbetar verksamheten ett förslag till budget där verksamhetsplanen kläs i siffror. I samband med detta genomförs en årlig genomgång av bolagets samtliga risker på en övergripande nivå. Ett underlag till ORSA-rapporten tas fram.
4. Vid styrelsemötet i november beslutar styrelsen om bolagets budget på ett år. De tar även del av ett utkast till ORSA-rapport baserad på antagen affärsplan.
5. Under december och januari utarbetar verksamheten ett utkast till flerårsbudget. ORSA-rapporten uppdateras utifrån årsbokslut och prognos. Då årsbokslutet fastställs justeras ORSA-rapporten.
6. Vid styrelsemötet i mars beslutar styrelsen om ORSA på kort och medellång sikt.
7. VD tillser att verksamheten informeras om ORSA-rapporten och att ORSA skickas in till Finansinspektionen.



3.3.2 Process vid extraordinär ORSA

Ovan framgår när extraordinär ORSA ska upprättas eller övervägas. Följande steg ingår i beslut om upprättande av extraordinär ORSA:

1. VD informeras att skäl för extraordinär ORSA föreligger
2. VD informerar styrelseordförande om detta
3. Styrelseordförande avgör om styrelsen ska sammankallas för extra möte eller informeras
4. VD avgör i samråd med styrelseordförande om processen ska inledas i avvaktan på beslut från styrelsen
5. Underlag för beslut om genomförande av extraordinär ORSA tillställs styrelsen som beslutar om genomförande ska ske

I övrigt hanteras denna process enligt samma metod som för årlig ORSA. Processtegen enligt den årliga ORSA:n gäller där så är tillämpligt, med beaktande att den extraordinära ORSA:n ska slutföras på väsentligt kortare tid varför endast de steg som är nödvändiga behöver genomföras.

3.3.3 Granskning av ORSA-process

Den årliga ORSA-processen ska utvärderas av styrelsen. VD och Riskhanteringsfunktionen ansvarar för att styrelsen erhåller underlag för utvärderingen. Utvärderingen ska sammanfattas i ORSA-rapporten.

Styrelsen kan även besluta om att processen ska granskas av internrevisionen eller annan funktion, vilket dokumenteras i separat rapport.

3.4 ORSA-organisation; ansvar, kontroller och dokumentation

3.4.1 Styrelsen

Styrelsen är ytterst ansvarig för ORSA-processen och ska initiera denna, delta aktivt och utmana de kvalitativa och kvantitativa bedömningarna, risker, stresstester m.m., och fatta beslut om ORSA. Styrelsens beslut dokumenteras i protokoll.

3.4.2 VD

VD har det operativa ansvaret för att arbetet med ORSA genomförs i enlighet med dessa riktlinjer.

VD ansvarar för att:

a) Tillställa styrelsen underlag för initierande av årlig eller extraordinär ORSA
b) Riskhanteringsfunktionen driver och sammanställer arbetet med ORSA
c) Fördelar ansvar och uppgifter utöver det som anges i denna policy
d) Det finns tillräckliga resurser för arbetet och att de olika funktionerna inom bolaget är delaktiga
e) Tillställa styrelsen förslag till ORSA-rapport
f) Inrapportera ORSA-rapporten till Finansinspektionen

3.4.3 Riskhanteringsfunktionen

Riskhanteringsfunktionen ansvarar för att:

a) Driva ORSA-processen och sammanställa ORSA-rapporten
b) Genomföra riskworkshop och ta fram beskrivning av riskprofil
c) Beskriva stressade scenarier
d) Översiktligt kontrollera beräkningar och utfall
e) Utvärdera riskhanteringssystemet
f) Med stöd av aktuarien utvärdera standardformelns lämplighet

3.4.4 Aktuarien

Aktuarien ansvarar för att:

a) Bidra till utformning av stressade scenarier
b) Bidra till utvärdering av bolagets kapitalbehov
c) Göra aktuariella beräkningar för nuvarande och framtida finansiell ställning
d) Kontrollera rimlighet i utfallen i prognoserna
e) Uttala sig om kvalitéten på datakällor

f) Utvärdera och uttala sig om regelefterlevnaden kring FTA och kapitalkrav (MCR och SCR)

4 Kontroller och dokumentation

Vid arbete med framtagande av ORSA sker en mängd behandling av data som måste kontrolleras avseende datakälla och kvalité.

Det ska eftersträvas en dualitet, så att prognoser och beräkningar om möjligt kontrolleras av annan funktion eller medarbetare än de som utfört dem. Riskhanteringsfunktionen har huvudansvar för att kontrollera och sammanställa resultat och ska i detta arbete bedöma tillförlitligheten i dessa.

En mycket viktig del i hela denna ORSA-process är att varje resultat och, i rimlig utsträckning, alla delresultat sparas på ett säkert sätt för att underlätta revision av processen samt säkerställa en god årlig process vid genomförandet av ORSA.

5 Struktur och innehåll i ORSA-rapporten

Det finns ingen i regelverken bestämd form för ORSA-rapporten. Det finns dock krav på att vilken information som ska ingå i rapporten. S:t Eriks bedömning är att följande ska ingå, dock utan att i denna policy ange hur rapporten ska disponeras:

- Lagrum och andra tillståndsfrågor relevanta för bedömningen
- Målet med ORSA-processen
- En beskrivning av affärsmodellen, organisationen, legal struktur och affärsplan, med särskilt fokus på riskhanteringssystemet
- En beskrivning av bolagets nuvarande riskprofil och eventuella förväntade förändringar av denna under prognosperioden. Beskrivningen ska innefatta samtliga väsentliga risker, inte endast de som innefattas i standardformeln
- En utvärdering om bolagets riskhanteringssystem är lämpligt givet nuvarande och förväntad riskprofil
- Historisk utveckling av bolagets finansiella ställning, inklusive resultat, balansräkning och kapitalisering (om relevant även enligt tidigare gällande regelverk)
- Nuvarande finansiell ställning och kapitalisering, inklusive kapitalbasens och kapitalkravens sammansättning
- Framtida resultat och solvens vid en förväntad utveckling enligt affärsplan och treårsbudget
- Framtida resultat och solvens vid olika scenarier för negativ utveckling relativt affärsplanen
- Slutsatser från bedömningen i fråga om bolagets nuvarande och framtida kapitalisering, affärsmodell och riskhanteringssystem ska ingå, inklusive vilka åtgärder dessa föranleder och vilka åtgärder (beredskapsplaner) som bör övervägas
- En utvärdering av standardformelns lämplighet inklusive en bedömning av om ytterligare kapital utöver det som resulterar från standardformeln krävs
- En bedömning av bolagets solvens- och kapitalbehov
- En bedömning av kvaliteten i datakällor som använts i arbetet
- En utvärdering och bedömning av regelefterlevnaden kring FTA och kapitalkrav (MCR och SCR)

- En utvärdering av processen inklusive förslag till förbättringar

6 Rapportering

Rapporten som beskriver den egna risk- och solvensbedömningen ska inlämnas till Finansinspektionen senast två veckor efter att den fastställts av styrelsen. VD ansvarar för att inlämning sker.

RIKTLINJE FÖR DIREKTUPPHANDLING
S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna är föremål för revidering årligen och skall fastställas av styrelsen för S:t Erik Försäkrings AB.

2 Ansvar

Styrelsen ansvarar för att riktlinjerna upprättas.

VD ansvarar för att riktlinjerna implementeras, följs av verksamheten samt att delegering och samordning sker korrekt.

Den som handlägger eller fattar beslut avseende direktupphandling ansvarar för att efterleva dessa riktlinjer.

3 När direktupphandling får ske

Direktupphandling är ett upphandlingsförfarande som får användas om värdet på inköpet understiger direktupphandlingsgränsen. Direktupphandlingsgränsen varierar beroende av vilken upphandlingslag som är tillämplig. Beloppsgränsen uppdateras vart annat år. Aktuella värden finns på stadens samarbetsyta Inköp och upphandling som nås via intranätet

Värdet ska beräknas exklusive mervärdesskatt, men inklusive options- och förlängnings-klausuler.

Det är den upphandlande myndighetens samlade behov, det vill säga hela nämndens eller bolagets inköp av samma slag under räkenskapsåret, som ska beaktas vid bedömningen av om anskaffningen kan göras genom en direktupphandling.

Direktupphandling kan även göras i vissa andra fall, förutsatt att något av de lagstadgade undantagen är tillämpligt på det aktuella inköpet (6 kap 12-19 §§ LOU/LUF).

4 Process för direktupphandling

4.1 Kontroll av befintliga avtal samt samordning

Innan direktupphandling ska kontroll ske av att det inte finns något upphandlat avtal för den vara/tjänst som avses.

Vidare ska kontroll ske av att inte tidigare direktupphandlingar inom samma område innebär att bolaget sammantaget överskrider direktupphandlingsgränsen. Lista över direktupphandlingar finns i bolagets G:katalog.

Vid upphandlingar över 100 000 kr ska samråd ske med upphandlingsansvarig.

4.2 Konkurrensutsättning

Även vid direktupphandling ska konkurrensutsättning övervägas, dvs att flera eventuella anbudsgivare erbjuds att lämna anbud.

Vid varje direktupphandling ska således en avvägning göras mellan konkurrensutsättning och kostnad för upphandling, kvalitet och pris avseende föremålet för inköpet i syfte att erhålla en vara eller tjänst med önskad kvalitet till ett förmånligt pris enligt nedan.

0-30 000 kr	Konkurrensutsättning kan övervägas.
30000 kr – 100 000 kr	Konkurrensutsättning bör övervägas (bör vara minst 3 st).
Över 100 000 kr	Konkurrensutsättning ska ske såvida inte starka ekonomiska skäl eller andra omständigheter (ex brådska enligt avsnitt 3 ovan) föreligger (bör vara minst 3 st). Annonsering ska övervägas.

4.3 Seriositetsprövning

Även vid direktupphandling ska kontroll ske av att leverantören fullgör sina skyldigheter mot samhället, såsom betalning av skatter och avgifter. Seriositetsprövnings innehåll och omfattning beror på såväl värdet av, som föremålet för direktupphandlingen.

(Exempelvis kan Skatteverkets blankett SKV 4820 inhämtas av nämnden för att kontrollera att företaget betalat skatt och sociala avgifter. Vidare kan kontrolluppgifter infordras från ett kreditvärderingsföretag för att kontrollera företagets stabilitet och ekonomiska ställning.)

0-30 000 kr	Seriositetsprövning kan övervägas.
30000 kr – 100 000 kr	Seriositetsprövning bör övervägas.
Över 100 000 kr	Seriositetsprövning ska ske.

4.4 Kommunikation

Kommunikation kan ske på olika sätt med ev. leverantörer. Företrädesvis ska detta ske skriftligt (dokument, mail, etc.) så vad som förekommit kan dokumenteras (se 4.5 nedan).

För mindre värden (ex. inköp av kaffebröd m.m.) kan endast verbal kommunikation användas om detta är lämpligt.

0-30 000 kr	Verbal eller skriftlig kommunikation (särskilt vid högre belopp inom spannet).
30 000 kr – 100 000 kr	Skriftlig kommunikation bör användas.
Över 100 000 kr	Skriftligt kommunikation ska användas.

4.5 Dokumentation

Grundregeln är att genomförande av direktupphandling ska dokumenteras på ett sådant sätt att det framgår vem som har fattat beslutet, i vilket syfte samt det ungefärliga värdet av upphandlingen.

Dokumentationen ska samlas under bolagets G:katalog avseende aktuell upphandling samt i förekommande fall arkiveras. Vidare ska direktupphandlingen noteras i listan för direktupphandlingar under G:katalogen.

Förutom att spara kommunikation bör bolagets avtalsmall för direktupphandling användas för dokumentation av själva upphandlingen.

För direktupphandlingar **över 30 000** kr ska följande dokumenteras.

- Upphandlande myndighets namn och org.nummer.
- Föremålet för upphandlingen
- Hur konkurrensen togs till vara
- Vilka leverantörer som tillfrågades
- Hur många som lämnade anbud
- Vilken leverantör (inkl. org.nummer) som tilldelades kontraktet
- Det viktigaste skälet för tilldelningen
- Avtalets värde
- Tidpunkten för kontraktets genomförande eller löptid

4.6 Avtal

Vid direktupphandling ska skriftligt avtal slutas med den leverantör som tilldelats kontraktet såvida det inte rör sig om sedvanliga belopp om mindre värden (ex. inköp av kaffebröd mot kvitto m.m.)

Checklista

Checklista för direktupphandling.

0-30 000 kr

- Kontrollera befintliga avtal och samordning
- Konkurrensutsättning kan övervägas
- Seriositetsprövning kan övervägas
- Kommunikation kan vara verbal eller skriftlig (särskilt i övre delen av spannet)
- Dokumentation ska ske så att det går att följa upphandlingen, se 4.5.
- Avtal ska vara skriftligt om inte mycket små värden (ex. kaffeköp)

30 000 – 100 000kr

- Kontrollera befintliga avtal och samordning
- Konkurrensutsättning bör övervägas (bör vara minst 3 st)
- Seriositetsprövning bör övervägas
- Skriftlig kommunikation bör användas
- Dokumentation enligt lista under 4.5.
- Skriftligt avtal ska upprättas.

Över 100 000 kr

- Kontrollera befintliga avtal och samordning
- Konkurrensutsättning ska ske om inte särskilda skäl överväger, se 4.2 (bör vara minst 3 st)
- Överväg annonsering
- Samråd med upphandlingsansvarig.
- Seriositetsprövning ska ske.
- Skriftlig kommunikation ska användas
- Dokumentation enligt lista under 4.5.
- Skriftligt avtal ska upprättas.

RIKTLINJER FÖR S:T ERIK FÖRSÄKRINGS FUNKTION FÖR REGELEFTERLEVNAD

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Inledning och syfte

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Syftet med instruktionen är att säkerställa att arbetet med regelefterlevnad inom bolaget bedrivs på ett väl fungerande och effektivt sätt i enlighet med gällande regelverk samt med tydliga gränssnitt och väl fungerande samarbete gentemot verksamheten och andra kontrollfunktioner. Denna instruktion tillsammans med interna och externa föreskrifter, riktlinjer och rutiner reglerar funktionens ansvar och arbetsuppgifter.

Ansvarig för funktionen för regelefterlevnad utses av VD.

2 Ikraftträdande och ändringar

Denna instruktion träder ikraft dagen för beslut. Instruktionen ska fastställas och godkännas av styrelsen minst en gång per år även om inga ändringar beslutas. Ansvarig för att instruktionen uppdateras är ansvarig för funktionen för regelefterlevnad och uppdateringen ska ske efter samråd med VD.

3 Ansvarsområden

Verksamheten ansvarar för att bolaget drivs i enlighet med de regler som gäller för verksamheten.

Funktionen för regelefterlevnad ansvarar enligt p 4 för följande regelområde (”regelverket”):

- bestämmelser i och föreskrifter meddelade med stöd av FRL
- bestämmelser meddelade i Solvens 2-direktivet (2009/38/EG)
- bestämmelser meddelade av Europeiska kommissionen med anledning av Solvens 2 direktivet
- riktlinjer och rekommendationer avseende Solvens 2 direktivet meddelade av EIOPA och Finansinspektionen.

Funktionen ansvarar inte för att informera om, identifiera eller bedöma finansiella, civilrättsliga, skatterättsliga, redovisningsrättsliga, konkurrensrättsliga risker eller frågor som rör hantering av personuppgifter eller säkerställande av det numeriska underlaget för Bolagets kapitaltäckning.

Funktionen granskar således verksamheten och inte de andra centrala funktionerna. En granskning kan dock ske till den del som andra centrala funktioners arbete behöver kontrolleras för att säkerställa att verksamheten uppfyller regelefterlevnaden, ex att funktionerna upprättats, har rätt kompetens, bidrar till verksamheten rapportering enligt regelverket m.m.

Funktionen ska vid utövandet av sitt ansvar enligt ovan, löpande utbyta information och samråda med verksamheten, riskkontroll och internrevision så att arbetet bedrivs så effektivt som möjligt.

Funktionen ska så långt det är möjligt ha en självständig ställning till den direkt affärsdrivande verksamheten. och ska inte delta i beslutsfattande, ansvara för eller delta i utförandet av tjänster i verksamheten.

Funktionen ska ha de befogenheter, resurser och de goda sakkunskaper som krävs, tillgång till relevant information, fullständig åtkomst till material, personal och egendom som är relevanta för utförande av de arbetsuppgifter som åligger funktionen. Medarbetare ska fullt ut samarbeta med funktionen. som har rätt att delta som observatör vid möten i verksamheten. All begränsning avseende denna rätt skall snarast rapporteras till styrelsen av envar.

4 Arbetsuppgifter

Funktionen för regelefterlevnad ska

- rapportera regelefterlevnaden till VD och styrelse enligt p5
- lämna råd till styrelse och VD i syfte att förebygga bristande regelefterlevnad
- bedöma och informera verksamheten, VD och styrelsen om konsekvenserna av ändrat regelverk
- identifiera och bedöma risker för bristande efterlevnad av regelverket, tex vid framtagande av nya produkter
- följa upp regelefterlevnaden och utvärdera de åtgärder som vidtagits för att minimera risken för och avhjälpa eventuella brister i bolagets regelefterlevnad
- biträda vid utformning av interna regler
- verka för att intressekonflikter mellan bolagets intressenter hanteras adekvat

Funktionen ska vid genomförandet av sitt arbete prioritera de största regelefterlevnadsriskerna och de som är förknippade med den tillståndspliktiga verksamheten.

Funktionen ska per den 1 januari eller alternativt per den 1 juli upprätta en riskbaserad plan för arbetet under den kommande 6 alternativt 12-månadersperioden baserad på risker som kan uppkomma till följd av bristande regelefterlevnad, förändringar av regelverket eller omvärlden. Planen ska godkännas av styrelsen och kan vid behov revideras under året.. VD ska informeras om planen.

5 Rapportrutiner för iakttagelser

Funktionen ska kontinuerligt rapportera regelefterlevnad och regelefterlevnads-risker enligt p3 och 4 till styrelsen, VD samt riskhanteringsfunktionen. Om allvarliga brister avseende regelefterlevnad upptäcks, eller om allvarliga incidenter inträffar, ska frågan snarast möjligt anmälas till VD, riskhanteringsfunktionen och rapporteras till styrelsen genom styrelseordföranden.

Funktionen ska till varje ordinarie styrelsemöte avge en skriftlig rapport som bland annat ska omfatta information om:

- relevanta inträffade händelser avseende regelefterlevnad
- pågående och kommande aktiviteter inom arbetet med regelefterlevnad
- viktigare regelverksförändringar.

Funktionen ska minst en gång per år, eller med den frekvens som styrelsen önskar, muntligen föredra rapporten vid styrelsemöte.

Funktionen ska en gång per år ge styrelsen en skriftlig samlad utvärdering över bolagets efterlevnad och åtgärdade brister.

Kontakter med Finansinspektionen sker av VD eller den person som VD utser.

6 Efterlevnad

Internrevision ansvarar för kontroll av efterlevnaden av denna instruktion.

RIKTLINJER FÖR FÖRSÄKRINGSDISTRIBUTION

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”. (Lag om försäkringsdistribution samt FAL).

Dessa riktlinjer syftar till intern kontroll och styrning av försäkringsdistribution och kompetens för de personer som leder företaget eller arbetar med försäkringsdistribution eller rådgivning.

Riktlinjerna är föremål för revidering och skall fastställas årligen av styrelsen för S:t Erik Försäkrings AB (S:t Erik).

VD ansvarar för att de skyldigheter som anges i denna riktlinje avseende kunskap och kompetens för de som direkt deltar i distributionen av försäkringar fullgörs.

2 Produkttillsyn och styrning

2.1 Målgrupp

S:t Erik är ett captivebolag (sex anställda och en VD) som ingår i koncernen Stockholms Stadshus AB som är moderbolag för Stockholms stads aktiebolag.

S:t Erik försäkrar endast verksamhet som bedrivs av Stockholms kommun och av staden ägda bolag. Bolaget tillhandahåller egendom- olycksfalls- och ansvarsförsäkring samt upphandlar försäkring i övrigt (t.ex. motorfordon, tjänsteresa, VDS m.m.) enligt LOU. Skadereglering och riskbesiktningar är outsourcade på externa parter och bolaget upphandlar återförsäkring för sin verksamhet.

Stockholms stad består utav bolag, fackförvaltningar och stadsdelsförvaltningar, samt upprättar sammanställd redovisning för koncernen. Således undantas stora delar av lagens krav på information och produktgodkännande avseende egendoms- och ansvarsförsäkring med hänvisning till 4 kap 12§ samt 5 kap. 22§ lagen om försäkringsdistribution.

S:t Erik tillhandhåller även olycksfallsförsäkring för elever m.fl. och har av den anledningen visst behov av riktlinjer. Försäkringen är en kollektiv försäkring för vilken de försäkrade inte själva erlägger premie, utan denna betalas av Stockholms kommun.

S:t Erik har således inte en traditionell försäljning och distribution, utan är begränsad till försäkring för ägarna och vad de uppger att de vill ha för försäkringsskydd.

2.2 Rådgivning

Som beskrivits ovan är det inte S:t Erik, utan ägaren/försäkringstagaren själv, som avgör vad för slags försäkring som ska tillhandahållas. Inom ramen för detta har S:t Erik att på bästa sätt rådgöra med ägaren och se till att det försäkringsskydd som framtas är anpassat efter de önskemål och behov som denne har baserat på ett tillräckligt stort analysmaterial till omfattning och kvalité.

All rådgivning ska dokumenteras och sparas under bolagets G/katalog för resp. kund i enlighet med de krav som ställs i 12 kap. FFFS 2018:10.

2.3 Produktutveckling och godkännande

Produktutveckling sker i samråd med ägaren (försäkringstagaren),skadereglerare, kundansvariga, aktuarie, riskhanteringsansvarig och styrelsen. I bolagets instruktioner och riktlinjer för reservsättningsrisker, riskhantering, tecknings- och återförsäkringsrisker finns ytterligare detaljerade krav på processen.

Produkten ses över löpande och kundens behov fångas upp genom årliga kundmöten samt möten vid behov. S:t Erik beaktar därvid villkorens utformning och omfattning på marknaden genom att granska andra bolags villkor och rådgöra med upphandlad försäkringsrådgivare eller förmedlare.

När extern förmedlare anlitas finns krav i upphandlingarna att denne ska samarbeta och tillhandahålla all den information som S:t Erik behöver för att kunna bedöma försäkringarnas omfattning och kvalité, samt vid behov processen för produktens framställning och målgrupp.

Godkännande av mindre ändringar inom ramen för bolagets instruktioner och riktlinjer sker av VD, större förändringar där behov finns av strategiska överväganden beslutas av styrelsen.

2.4 Klagomål

Klagomål handhas genom klagomålsansvarig, se bolagets Riktlinjer för hantering av klagomål.

3 Kunskap och kompetens

3.1 Generella krav

S:t Erik har fastställt en riktlinje för lämplighetsprövning avseende styrelse, ledning och nyckelfunktioner samt även krav i form av befattningsbeskrivningar.

Bedömningen ska innefatta professionella meriter, formella kvalifikationer, kunskaper och relevanta erfarenheter inom försäkringssektorn, andra finanssektorer eller andra branscher och ska beakta de arbetsuppgifter som personen tilldelats och i dennes fall de relevanta kunskaper som behövs när det gäller försäkringar, finansområdet, redovisning, aktuariell förmåga och ledarskapsförmåga.

Dessa krav dokumenteras vid anställningen och följs upp vid utvecklingssamtal

3.2 Krav för de som handhar distribution

3.2.1 Personalkategorier som direkt deltar i distributionen av försäkringar

Följande personalkategorier omfattas av de särskilda kraven:

- Kundansvariga
- Skadeansvarig
- Villkorsansvarig
- VD

3.2.2 Allmänna krav

De som sysslar med distribution inom företaget får inte vara underårig, i konkurs, ha näringsförbud eller förvaltare. De får inte förekomma belastningsregistret avseende allvarliga förmögenhetsbrott eller viss allvarlig ekonomisk brottslighet samt ska ha visat skötsamhet i

ekonomiska angelägenheter. De ska även ha lämplig kunskap och kompetens för den verksamhet som ska bedrivas och uppfylla kraven på fortlöpande fortbildning och yrkesutveckling.

Dessa krav dokumenteras vid anställningen och följs upp vid utvecklingssamtal (belastningsregistret kontrolleras efter anställningen endast på förekommen anledning).

3.2.3 Särskilda krav på kunskap och kompetens

Reglerna kring vilken kunskap som krävs utgår från den typ av försäkringsprodukter som distribueras. Nivån på kunskapen ska alltid vara lämplig och tillräcklig för den verksamhet som S:t Erik bedriver. Reglerna skiljer sig därmed åt beroende på vilka typer av försäkringsprodukter som ska distribueras och vilken personalkategori den anställde tillhör.

En anställd måste vidare ha kompetens för att korrekt kunna fullgöra sina arbetsuppgifter och uppdrag som är hänförliga till försäkringsdistribution enligt de krav som gäller för den aktuella verksamheten. Lämplig praktisk erfarenhet uppfylls genom att den anställde antingen tidigare har arbetat med relevanta arbetsuppgifter hos försäkringsdistributör eller utför sina arbetsuppgifter hos S:t Erik under övervakning av en annan person som uppfyller kraven på kunskap och kompetens och som tar fullt ansvar för att uppgifterna utförs korrekt.

I bilaga till dessa riktlinjer finns en sammanställning av relevanta utbildningsområden avseende lämplig kunskap och kompetens och fortbildning och yrkesutveckling avseende verksamheten i S:t Erik. Sammanställningen gäller för de personalkategorier som omfattas av riktlinjerna. För VD och övrig ledning hänvisas till riktlinjer för lämplighetsbedömning.

3.3 Särskilda krav för den som ingår i ledningen (eller ersättare)

Den som ingår i ledningen ska ha den insikt och erfarenhet som behövs för uppgiften, vara allmänt lämplig och får inte förekomma belastningsregistret avseende allvarliga förmögenhetsbrott eller viss allvarlig ekonomisk brottslighet samt ska ha visat skötsamhet i ekonomiska angelägenheter..

Av bolagets Riktlinje för lämplighetsprövning framgår de för bolaget anpassade kraven.

Dokumentation sker vid anställning samt löpande vid utbildning m.m. (belastningsregistret kontrolleras efter anställningen endast på förekommen anledning).

3.4 Ersättning

S:t Eriks personal har endast fast lön i enlighet med bolagets Ersättningspolicy.

3.5 Utbildning

S:t Eriks personal erbjuds regelbundet utbildning inom relevanta områden för att kunna vidmakthålla och utveckla sina kunskaper inom försäkringsområdet . Utbildning tas upp i de utvecklingssamtal som hålls och då dokumenteras även genomförda utbildningar.

Utbildningen kommer framförallt att ske i form av regelbunden intern utbildning då utbildningsansvaret primärt delas upp mellan S:t Erik och S:t Eriks funktioner för regelefterlevnad samt riskhantering. Anställda kommer också att ges möjlighet att genom externa kurser fortlöpande bilda sig och utveckla sin yrkeskompetens. Vid externa kurser krävs att kursdeltagare erhåller kursintyg som kan verifieras av S:t Erik. Utbildningstillfällena

kommer att vara spridda under året så att alla anställda som omfattas av riktlinjerna ges möjlighet att delta i 15 timmars fortbildning per år.

En inledande utbildning kommer att genomföras för varje ny anställd. Denna kommer att verifieras genom kunskapstest som visar att de grundläggande kraven för verksamheten och försäkringsprodukten är uppfyllda. Testet tillhandahålls av S:t Erik och granskas även av Funktionen för regelefterlevnad. Ett uppföljande test av mindre omfattning kommer att genomföras varje år.

S:t Erik kommer att dokumentera de åtgärder som Bolaget vidtar för att uppfylla kraven som ställs i lag och föreskrifter. Detta kommer dels att ske genom förande av register vid gentemot varje enskild medarbetare samt i protokoll vid planering inför interna utbildningstillfällen.

4 Information

Som framgår enligt 2.1 upprättas en sammanställd redovisning för S.t Eriks kund tillika ägare. Således omfattas inte S:t Erik av reglerna om information avseende egendoms- och ansvarsförsäkringen.

I de fall fråga om information aktualiseras (kollektiv olycksfallsförsäkring) ska information lämnas enligt 5 kap. 1, 9, 13§§ lagen om försäkringsdistribution. Information lämnas innan, vid förändringar och förnyelse (om behov föreligger).

Information lämnas kostnadsfritt i pappershandling, eller på annat varaktigt medium eller för kunden tillgänglig webbplats om kunden själv valt att få informationen på annat varaktigt medium än papper. Vid skadeförsäkring ska särskilt standardiserat produktblad i form av papper eller annat varaktigt medium användas. (se EIOPA/FI).

Informationen ska vara klar och koncis samt lämnas på svenska eller annat officiellt språk inom EES där risken är belägen, där åtagandet görs eller efter överenskommelse med kunden.

BILAGA

Kunskap/Kompetens	Innehåll	Kunskapsnivå
Regelverken	- Lagen (2018:1219) om försäkringsdistribution, - Förordningen (2018:1231) om försäkringsdistribution, - Föreskrifter och allmänna råd från Finansinspektionen som är tillämpliga för verksamhet med försäkringsdistribution, - EU-förordningar och riktlinjer som är tillämpliga för verksamhet med försäkringsdistribution,	God kunskap
Affärsstrategi etc.	- Kunskap om S:t Erik Försäkrings AB - Interna regler för verksamheten med försäkringsdistribution - Hantering av klagomål och intressekonflikter	God kunskap
Försäkringsprodukten	- Bolagets försäkringar och tilläggsrisker - Villkor - Skadereglering	Mycket god kunskap
Försäkringsmarknaden	- Kunskaper om marknaden för att förstå bolagets förutsättningar för affären	Övergripande kunskap

Försäkringskompetens	- Kunskap och erfarenhet av försäkring, och återförsäkring för att förstå förutsättningarna för produkten - Affärsetiska normer och bedömning av kundernas behov	God kunskap
Finansmarknaden	- Skuldtäckning och solvenskrav och hur det påverkas av och begränsar försäkringars omfattning.	Övergripande kunskap
Risk	- Kunskap om riskhantering, riskkontroll och riskrapportering för att förstå de samlade riskerna i bolaget och för kunderna.	Övergripande kunskap

RIKTLINJER FÖR HANTERING AV INTRESSEKONFLIKTER I S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna är föremål för revidering årligen och skall fastställas av styrelsen för S:t Erik Försäkrings AB.

2 Riktlinjer

Den som handlägger eller beslutar i ett ärende är jävig om det finns omständigheter som kan rubba förtroendet för hans eller hennes opartiskhet. Dessa riktlinjer är avsedda att ge vägledning för styrelsen, VD och anställda i bolaget i samband med hanteringen av ärenden där det finns risk för sådana intressekonflikter.

Styrelsen, VD, anställd, annan ställföreträdare för bolaget eller person som utför uppdrag för bolaget genom uppdragsavtal får inte företa rättshandlingar eller andra åtgärder som är ägnade att bereda otillbörliga fördelar åt aktieägare, anställda i bolaget, försäkringstagare eller andra till nackdel för bolaget eller dess ägare.

En styrelseledamot, VD eller anställd får därför inte handlägga eller besluta om en fråga om avtal eller annat rättsförhållande

1. mellan bolaget och någon av styrelseledamöterna, VD eller de anställda
2. mellan bolaget och en tredje man, om styrelseledamot, VD eller anställd i frågan har ett egenintresse i frågan, eller
3. mellan bolaget och en juridisk person som styrelseledamot, VD eller anställd ensam eller tillsammans med någon annan får företräda.

En person får inte heller handlägga eller besluta om en fråga om avtal eller annat rättsförhållande mellan bolaget och annan enligt punkten 1-3 ovan om denna är eller har varit gift, sambo eller registrerad partner med eller i rätt upp- eller nedstigande led släkt med eller är i svågerlag med eller är syskon eller på motsvarande sätt är närstående.

I första hand är det den berörde som självmant skall avstå från att delta i handläggning och/eller beslutsfattande i sådana frågor där intressekonflikt har uppstått eller skulle kunna uppstå. Är personen ifråga osäker på om en intressekonflikt föreligger skall anställd vända sig till VD, VD och styrelseledamot till styrelseordföranden och diskutera saken. Om tveksamhet huruvida intressekonflikt föreligger skall sådan anses föreligga. Frågan skall vid intressekonflikt delegeras till någon annan person för vilken intressekonflikt inte föreligger.

Avtal mellan aktieägaren och bolaget som inte avser löpande affärstransaktioner på sedvanliga villkor ska antecknas i eller fogas till styrelsens protokoll.

Ersättningsprogram, resultatdelningssystem eller motsvarande till bolagsledning eller andra anställda i bolaget får inte förekomma.

3 Informationsplikt

För att undvika misstankar om intressekonflikter skall samtliga styrelseledamöter, VD och anställda skriftligen informera bolaget och styrelsen om samtliga uppdrag, sidoverksamheter

eller företag som man eller närstående har intressen i och som kan innebära en framtida intressekonflikt.

4 Identifiering och kontroll av intressekonflikter

4.1 Allmänt

S:t Erik Försäkring ingår i koncernen Stockholm Stadshus AB som i sin tur ägs av Stockholm stad. Bolaget försäkrar endast Stockholm stad och dess bolag.

Nedan följer en beskrivning över de intressekonflikter som bolaget identifierat kan finnas i verksamheten och hur dessa risker behandlas.

4.2 Organisation och ansvar

Styrelsen ansvarar för:

- uppdatering av dessa riktlinjer
- en årlig identifiering av intressekonflikter enligt 4.3
- att vidta erforderliga åtgärder pga. identifierade intressekonflikter

VD ansvarar för:

- en årlig identifiering av intressekonflikter enligt 4.4
- en årlig identifiering av personalens intressekonflikter enligt 4.5
- att vidta erforderliga åtgärder pga. identifierade intressekonflikter
- att redovisa identifiering av intressekonflikter och åtgärder enligt dessa punkter till styrelsen vid första ordinarie styrelsemötet

Bolagets jurist ansvarar för att:

- tillställa styrelseledamöterna bilaga 1, sammanställa dessa samt VD:s till det första ordinarie styrelsemötet

4.3 Styrelsen

Bolagets styrelse består utav tjänstemän inom Stockholm stad och Stadshus AB, dvs utgörs av ägarna och försäkringstagarna.

Risk kan föreligga att styrelseledamot deltar i beslut där denne eller närstående har ett ekonomiskt eller annat intresse. Vidare kan det föreligga en risk för att olika bolag/förvaltningar inom koncernen har avtal med varandra, vilket kan påverka objektiviteten i beslut och avtal.

För att minimera risken skall styrelseledamöterna till det första ordinarie styrelsemötet redovisa enligt bilaga 1. Denna utsänds av bolagets jurist som sammanställer och redovisar denna och VD:s rapport avseende personalen i styrelsen. Redovisningen skall protokollföras.

Styrelsen skall vid en jävsituation eller intressekonflikt bedöma allvarligheten i den och fatta beslut om huruvida det är tillräckligt att ledamot ej deltar vid beslut eller om det är nödvändigt att ägarna tar ställning till om ledamot skall avgå ur styrelsen.

4.4 Bolagets ledning

Bolagets ledning består utav VD som innehar denna position i både bolaget och S:t Erik Livförsäkring AB. Bolagen köper tjänster av varandra.

Risk kan föreligga att VD deltar i beslut där denne eller närstående har ett ekonomiskt eller annat intresse. Vidare innebär de dubbla rollerna att det i avtal eller kostnadsfördelning mellan bolagen är viktigt att det ena bolaget inte gynnas på det andras bekostnad och att regler finns för hur VD prioriterar sitt arbete.

För att minska riskerna får endast styrelsen fatta beslut om avtal mellan bolagen. Vidare skall VD varje månad redovisa för lönefunktionen hur mycket arbete som nedlagts i vardera bolaget samt till vart styrelsemöte redovisa detta samt ange hur arbetet planeras för de två bolagen. VD skall till första ordinarie styrelsemötet tillställa styrelsens sekreterare bilaga 1.

4.5 Anställda

Risk kan föreligga att anställd handlägger frågor som denne eller närstående har ett ekonomiskt eller annat intresse i.

Vid nyanställning skall VD tillse att sökande redovisar enligt bilaga 1 och dokumentera detta i anställningshandlingarna. VD skall i det löpande arbetet vidta de åtgärder som behövs för att personal inte hanterar frågor där jäv eller intressekonflikter kan uppstå. Vidare skall VD årligen tillse att all personal redovisar enligt bilaga 1 och redovisa detta och eventuellt vidtagna åtgärder vid första ordinarie styrelsemötet.

4.6 Kontorsgemenskap

Bolaget och S:t Erik Livförsäkring har kontorsgemenskap och delar kostnaderna för lokaler och kontorsmateriel.

Risk finns att kostnadsfördelning gynnar ett av bolagen på bekostnad av det andra.

För att undvika felaktig kostnadsfördelning sker denna efter antalet anställda.

4.7 Outsourcing

De intressekonflikter som kan vara förknippade med outsourcing finns reglerade i bolagets Riktlinjer för uppdragsavtal.

Bilaga 1

Checklista för eventuella intressekonflikter.

Med närstående menas den som man är eller har varit gift, sambo eller registrerad partner med eller i rätt upp- eller nedstigande led släkt med eller är i svågerlag med eller är syskon eller på motsvarande sätt är närstående.

1. I vilka bolag är du styrelsemedlem, VD eller innehar annan ledande befattning? (Ange bolag och befattning)

2. Är du medveten om några interna intressekonflikter med din roll i bolaget (Outsourcing, avtal inom koncernen etc)

3. Är du medveten om några externa intressekonflikter som påverkar din roll i bolaget (Ex uppdrag eller anställning i andra bolag där man inte är ägare)

4. I vilka bolag är närstående styrelsemedlem, VD eller innehar ledande befattning? (Ange bolag och befattning)

5. Äger du aktier/del av bolag med vilket S:t Erik Försäkring konkurrerar eller samarbetar? (Ange bolag och ägarandel)

6. Äger närstående aktier/del i bolag med vilket S:t Erik Försäkring konkurrerar eller samarbetar? (Ange bolag och ägarandel)

RIKTLINJER FÖR HANTERING AV KLAGOMÅL I S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna revideras löpande och skall fastställas årligen av styrelsen.

Riktlinjerna skall distribueras till samtliga anställda på S:t Erik Försäkring och utbildning av de som träffas av instruktionen ska ske löpande.

Syftet med riktlinjerna är att bolaget ska ha en funktion för klagomålshantering dit kunderna kan vända sig och som kontinuerligt sammanställer, dokumenterar och utvärderar klagomål.

I de fall klagomålsansvarig person ej är utsedd ansvarar istället VD för funktionen. VD har rätt att utse klagomålsansvarig i sitt ställe.

2 Klagomålshantering

2.1 Information till kund

Kunder skall informeras om S:t Erik Försäkrings hantering av klagomål och om vem som är klagomålsansvarig. Av informationen skall framgå hur kunden framställer ett klagomål och denna information skall även framgå av S:t Erik Försäkrings hemsida.

2.2 Ta emot klagomål

Med klagomål avses att en kund i ett enskilt ärende framför konkret missnöje med hanteringen av en tjänst eller produkt. Allmänna synpunkter och generella missnöjesyttringar är i detta sammanhang inte klagomål.

Samtliga klagomål uttryckt i skriftlig form som tas emot av anställd på S:t Erik Försäkring ska omedelbart vidarebefordras till klagomålsansvarig för registrering i bolagets klagomålsregister och bemötas av denne. Klagomål uttryckt i muntlig form som kan betraktas som konkret nog att kräva någon form av åtgärd från S:t Erik Försäkring ska likaledes omedelbart vidarebefordras till klagomålsansvarig och dokumenteras.

2.3 Handläggning av klagomålsärenden

Alla klagomålsärenden som vidarebefordras till klagomålsansvarige ska bemötas snarast, sakligt, rättvist och korrekt efter fullständig utredning. Klaganden ska få ett svar senast 14 dagar efter att klagomålet inkommit till S:t Erik Försäkring. Svaret ska vara i skriftlig form, och i de fall klagomålet avvisas, innehålla en motivering samt information om möjligheten att driva ärendet vidare i allmänna domstolar och, i förekommande fall, i Allmänna reklamationsnämnden,. I tillämpliga fall skall den klagande även upplysas om möjligheten att erhålla rådgivning från Konsumenternas Försäkringsbyrå, Konsumenternas Bank- och finansbyrå samt genom den kommunala konsumentvägledningen.

Om klagomålet inte kan bemötas inom 14 dagar ska klaganden istället få ett skriftligt meddelande om att S:t Erik Försäkring har tagit emot klagomålet med en uppgift varför ärendet försenats och med angivande av en tidsrymd inom vilken klagomålet kommer att bemötas.

2.4 Beslut om åtgärd i klagomålsärenden

För klagomål i okomplicerade ärenden eller ärenden av mindre allvarlig natur ska klagomålsansvarig person i samråd med berörd funktionsansvarig för den eller de tjänster som klagomålet gäller besluta om åtgärd. När beslut fattas skall klaganden informeras om beslutet enligt p 2.3.

För klagomål i komplicerade ärenden eller ärenden av allvarlig natur skall klagomålsansvarig person lämna över ansvaret att ta beslut om åtgärd till VD. VD kan vid behov konsultera bolagets jurist och skall informera regelansvarig. Innan VD tar beslut om åtgärd ska han eller hon informera styrelsens ordförande om ärendet. När beslut fattas skall klaganden informeras om beslutet enligt p 2.3.

Om klaganden genom att upprepa sitt klagomål i samma ärende visar att denne inte godtar det beslut om åtgärd som tagits av klagomålsansvarig, och ingen ny information framkommit som motiverar en förändring av beslutet, ska VD skriftligen informera klaganden om att beslutet är slutgiltigt från S:t Erik Försäkrings sida och hänvisa klaganden till extern myndighet för att få ärendet avgjort.

3 Dokumentation och arkivering

Klagomålsansvarig person är ansvarig för att dokumentera och arkivera information om hanteringen av ärendet i centralt register. I de ärenden VD tagit över ansvaret som klagomålsansvarig ska denne dokumentera information om hanteringen av ärendet och vidarebefordra till klagomålsansvarig person för arkivering. Alla dokument som är relevanta i ärendet ska sparas och arkiveras. Klagomålsansvarig ska bedöma hur länge dokumenten ska bevaras utifrån ärendets karaktär, behovet av dokumentation samt enligt stadens arkivregler.

4 Information och uppföljning

Klagomålsansvarig person är ansvarig för att informera styrelsen och berörda personer på S:t Erik Försäkring om utgången av klagomålsärenden. Vid varje ordinarie styrelsemöte ska VD eller klagomålsansvarig rapportera om eventuella klagomålsärenden mot S:t Erik Försäkring samt vilka åtgärder som vidtagits i dessa ärenden.

Klagomålsansvarig person är också ansvarig för att följa upp samtliga klagomålsärenden och, när så är motiverat, se till att lämpliga förändringar görs i interna rutiner eller produkter och åtföljs av interna informationsinsatser för att liknande klagomål inte ska uppstå på nytt.

5 Information till Finansinspektionen

S:t Erik Försäkring skall underrätta Finansinspektionen om vem som är ansvarig för klagomålshantering och vid förändring härav snarast anmäla förändringen till Finans-inspektionen.

RIKTLINJER FÖR S:T ERIK FÖRSÄKRINGS AB:s HANTERING AV PERSONUPPGIFTER

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Denna instruktion har upprättats mot bakgrund av de regler om behandling av personuppgifter som anges i Förordning (EU) 2016/679 och Dataskyddslagen.

Riktlinjerna revideras löpande och skall fastställas minst årligen av styrelsen.

Syftet med instruktionen är att klargöra vilka regler som gäller för bolagets hantering av personuppgifter och uppnå laglighet, korrekthet, öppenhet, ändamålsbegränsning, uppgiftsminimering, lagringsminimering integritet och konfidentialitet vid bolaget hantering av personuppgifter och därmed uppfylla bolagets ansvarsskyldighet.

2 Ansvar

2.1 Bolaget (Personuppgiftsansvarig)

Bolaget är personuppgiftsansvarig för sin egen behandling och kan vara gemensamt ansvarig om bolaget och annat subjekt tillsammans fastställer ändamålen med och metoderna för behandlingen.

I de fall bolaget handhar uppgifter för annat subjekts räkning är bolaget personuppgiftsbiträde.

Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med gällande rätt. Dessa åtgärder ska ses över och uppdateras vid behov.

Vidare ansvarar personuppgiftsansvarig för vad som stadgas nedan 2.2.3 avseende dataskyddsombudets oberoende och resurser.

VD har att, inom ramen för förvaltningsåtgärder, tillse att personuppgifter hanteras korrekt av bolaget och kan därvid delegera uppgifter internt och externt.

2.2 Dataskyddsombud

Bolaget hanterar en stor mängd personuppgifter i sin skadehantering och vid uppfyllande av försäkringsavtal. Dessa uppgifter hör till viss del till särskilda kategorier (känsliga) av personuppgifter. Av den anledningen ska bolaget utse ett dataskyddsombud.

2.2.1 Kompetens

Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i Artikel 39.

2.2.2 Uppgifter

Ombudets roll är att kontrollera att dataskyddsförordningen följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser. Dataskyddsombudet ska även vara en kontaktpunkt för tillsynsmyndigheten och de registrerade.

Dataskyddsombudet ska vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.

Dataskyddsombudet ska:

- Informera, utbilda och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar personuppgifter om deras skyldigheter enligt gällande regelverk.

- Övervaka bolagets, anställdas och personuppgiftsbiträdens efterlevnad av gällande rätt, ansvarstilldelning och utbildning.

- Övervaka personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

- På begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den.

- Samarbeta med tillsynsmyndigheten och utgöra kontaktpunkt i frågor som rör behandling, inbegripet förhandssamråd, och vid behov samråda i alla andra frågor.

- Tillse att det finns en registerförteckning.

- Tillse att det finns en mall för personuppgiftsbiträdesavtal.

- Rapportera till styrelsen enligt p 13.

2.2.3 Oberoende

- Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

- Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsombudet i utförandet av dennes uppgifter genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

- Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av dessa uppgifter. Han eller hon får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter.

- Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå.

- Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.

- Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

- Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt. Bolaget har riktlinjer för intressekonflikter som därvid ska följas.

Rättsinformation:
- *Artikel 37-39*
- *Skäl 97*
- *Artikel 29-gruppen, Riktlinjer om dataskyddsombud*

2.2.4 Tystnadsplikt
Dataskyddsombudet får inte obehörigen röja det som ombudet har fått kännedom om vid fullgörandet av sin uppgift. I det allmännas verksamhet tillämpas offentlighet- och sekretesslagen i stället för första stycket.

Rättsinformation:
- Dataskyddslag 1 kap. 8§.

2.3 Anställda
Anställda ansvarar för att deras behandling av personuppgifter följer gällande rätt och dessa riktlinjer och ska bl.a.:

- Ansvara för att dataskyddsfrågorna beaktas i de system, upphandlingar eller avtal som den anställde ansvarar för.

- Endast behandla personuppgifter om detta är nödvändigt för ett lagligt ändamål, är säkert och då minimera dessa uppgifter.

- Att registrerad fått den information som krävs enligt gällande rätt.

- Upprätta dokument (om sådant inte redan finns upprättat för behandlingen) avseende behandlingen för att utreda och dokumentera om behandlingen kan ske, om konsekvensbedömning är aktuellt samt meddela dataskyddsombudet detta.

- Upprätta personbiträdesavtal inom sitt ansvarsområde.

- Informera dataskyddsombudet i god tid om sådant som kan beröra behandling, ex:
    - Ny eller ändrad behandling
    - Ändringar av de personuppgifter som behandlas

- Ändringar i IT-system som påverkar personuppgifterna, ex. avseende säkerhet, loggning, backupper, möjligheter till utsökning av information, m.m.
- Inför upphandling av IT-system eller ändringar av avtal

- Vid behov fråga dataskyddsombudet om råd, särskilt vid konsekvensbedömning.

2.4 Personuppgiftsbiträde

Personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning och som således finns utanför den personuppgiftsansvariges organisation.

Personuppgiftsbiträdet tillgodoser någon annans intressen, måste följa instruktioner och kan således inte bestämma ändamålet med behandlingen.

2.4.1 Anlitande eller antagande av uppdrag som personuppgiftsbiträde/underbiträde

Om bolaget anlitar ett personuppgiftsbiträde eller själv utgör biträde åt annan personuppgifts-ansvarig ska uppdraget hanteras som följer.

- Personuppgiftsbiträde får endast anlitas, eller bolaget anta sådant uppdrag, om biträdet kan garantera lämpliga tekniska och organisatoriska åtgärder på sådant sätt att behandlingen uppfyller gällande rätt och säkerställer att den registrerades rättigheter skyddas.

- Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgifts-ansvarige.

  Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgifts-biträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

  I de fall där ett personuppgiftsbiträde anlitar ett underbiträde ska denne genom avtal, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller mellan den personuppgiftsansvarige och personuppgiftsbiträdet och ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller gällande rätt.

  Om det andra underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarig gentemot den personuppgiftsansvarige för utförandet av underbiträdets skyldigheter.

- Personuppgiftsbiträdet ska föra en registerförteckning över sin behandling.

- Skriftligt avtal ska upprättas enligt nedan såvida inte gällande rätt stadgar annat.

2.4.2 Personuppgiftbiträdesavtal

Ett personuppgiftsbiträdesavtal ska vara skriftligt, eller utgöra en del av annat skriftligt avtal, och reglera att:

- föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges.

- biträdet endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgifts-biträdet omfattas av, och i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt.

- biträdet säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

- biträdet vidtar alla säkerhetsåtgärder enligt nedan.

- biträdet ska respektera de villkor som stadgas i 2.4.1 för anlitandet av ett annat personuppgiftsbiträde (underbiträde)

- biträdet med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter.

- biträdet ska bistå den personuppgiftsansvarige med att se till att säkerhet i samband med behandlingen, hantering av personuppgiftsincidenter, konsekvensbedömning av dataskydd och förhandssamråd med tillsynsmyndigheten kan ske (med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå).

- biträdet beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt.

- biträdet ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som avser personuppgiftsbiträden och anlitande av dessa har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

Rättsinformation:
- *Artikel 4.8, 28-29*
- *Skäl 81*

3 Process

Behandling av personuppgifter sker på olika nivåer och i olika syften. Det är i den första linjen, verksamheten, som den faktiska behandlingen sker och även där som laglighet och kontroller sker.

Dataskyddsombudet har en övervakande, rådgivande och kontrollerande roll i andra linjen.

Varje typ av ny behandling utreds av den aktuella handläggaren och en till person hos den personuppgiftsansvarige. Utredningen dokumenteras, registerförteckningen uppdateras och information lämnas till dataskyddsombudet (vid konsekvensbedömning ska dataskyddsombudet rådfrågas). Detta innebär att bolagets register byggs upp succesivt och att de behandlingstyper som bolaget har finns dokumenterade.

När samma typ av behandling ska utföras finns således en genomförd kontroll och handläggaren behöver då inte genomföra en utredning igen, såvida inget har ändrats avseende uppgifter och ändamål. Detta ska i sådana fall hanteras som en ny behandling.

Vid upphandling (outsourcing) tillser den som ansvarar för upphandlingen att krav ställs på uppdragstagaren att redovisa sin process för personuppgiftshantering inklusive dataskydd samt att det upprättas personuppgiftsbiträdesavtal som en del av förfrågningsunderlaget. Vidare svarar den ansvariga som en del av sin kontraktsuppföljning att kontroll sker av biträdet. Dataskyddsombudet övervakar att krav ställs och att uppföljning sker av biträdet.

Dataskyddsombudet tillser att personalen utbildas och genomför såväl stickprover som årlig sammanställning till styrelsen.

Vid incidenter meddelas riskhanteringsansvarig, VD och dataskyddsombud. Dataskyddsombudet handhar sedan frågan och samtliga inblandade deltar i den utredning som sker.

4 Personuppgift, särskilda kategorier, brott, personnummer

Med personuppgift avses all information som direkt eller indirekt kan hänföras till en fysisk person som är i livet t.ex. namn, personnummer, adress, e-postadress, nätidentifierare, nummerskylt, bilder, kundnummer, lägenhetsnummer m.m.

Avidentifierade, avlidna eller juridiska personer utgör således inte personuppgifter.

En del personuppgifter är s.k. särskilda kategorier av personuppgifter (känsliga personuppgifter) för vilka särskilda regler gäller. Dessa uppgifter är:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- behandling av genetiska uppgifter
- biometriska uppgifter
- uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

Vidare finns särskilda regler för:

- personuppgifter som rör fällande domar i brottmål samt överträdelser
- personnummer

Rättsinformation:
- *Artikel 4.13-4.15, 9, 10, 87*
- *Skäl 34, 35, 51*

5 Behandling av personuppgifter

Med behandling avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Behandlingen kan således vara helt automatiserad (allt sker elektroniskt), delvis automatiserad (manuell insamling och automatiserad behandling) eller manuell (om det utgör en del av ett register, ex. ett sökbart kartotek).

Rättsinformation:
- *Artikel 2.1, 4.1-4.2*
- *Skäl 15, 26-30*

5.1 Allmänna krav på behandling

All behandling av personuppgifter måste uppfylla de grundläggande principer som anges i dataskyddsförordningen.

Laglighet, korrekthet och öppenhet
Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Kravet på att behandlingen av personuppgifter ska vara laglig innebär bland annat att det måste finnas en rättslig grund för behandlingen.

Att personuppgifter ska behandlas på ett öppet sätt i förhållande till den registrerade innebär bland annat att det ska vara klart och tydligt för denne hur hans eller hennes personuppgifter samlas in och i övrigt behandlas. De registrerade måste därför få information om behandlingen som är både lättillgänglig och formuleras med ett klart och tydligt språk.

Med korrekthet menas att personuppgifterna ska vara korrekta och uppdaterade samt ska rättas eller raderas om de är felaktiga.

Rättsinformation:
- *Artikel 5.1a*
- *Skäl 39, 58, 60*

Ändamålsbegränsning

Personuppgifter ska bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Det innebär att den som ska behandla personuppgifter måste ha ändamålen klara för sig redan innan insamlingen av personuppgifter börjar. Personuppgifterna får sedan inte behandlas på ett sätt som är oförenligt med dessa ändamål. De på förhand fastställda ändamålen är med andra ord det som sätter ramarna för behandlingen. Ändamålen ska dokumenteras skriftligt och den registrerade ska få information om ändamålen både när uppgifterna samlas in och annars när denne begär det. Om de insamlade personuppgifterna senare ska behandlas för andra ändamål som är förenliga med de ursprungliga ändamålen måste de registrerade också informeras om detta.

De insamlade personuppgifterna får behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål utan att det anses oförenligt med de ursprungliga ändamålen om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.

Rättsinformation:
- *Artikel 5.1b, 6.4, 13.3, 14.4, 89.1.*
- *Skäl 39 och 50.*

Uppgiftsminimering
Principen om uppgiftsminimering innebär att personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov. Insamlade personuppgifter får inte heller behandlas om de till exempel är så gamla att de inte längre är relevanta för de ursprungliga ändamålen.

Lagringsminimering
Personuppgifter får inte sparas, det vill säga. förvaras i en form som möjliggör identifiering av den registrerade, under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

När personuppgifterna inte längre behövs för de ändamålen ska de raderas eller avidentifieras. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den som behandlar personuppgifter införa tidsfrister och rutiner för radering eller avidentifiering.

De insamlade personuppgifterna får lagras under längre tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.

Rättsinformation:
- *Artikel 5.1e*
- *Skäl 39*

Integritet och konfidentialitet
Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Den som behandlar personuppgifter ska därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

Rättsinformation:
- *Artikel 5.1f*

- *Artikel 32*
- *Skäl 39 och 83*

Ansvarsskyldighet
Den som behandlar personuppgifter ansvarar för att principerna om personuppgiftsbehandling följs och måste kunna visa på vilket sätt man följer dem. Det finns flera sätt att visa detta, till exempel genom att ha tydlig information till de registrerade, att dokumentera de behandlingar som pågår i organisationen och de överväganden man har gjort samt att ha dokumenterade interna riktlinjer för dataskyddet (en dataskyddspolicy). Att utse ett dataskyddsombud som bidrar till organisationens efterlevnad av förordningen och de interna riktlinjerna kan också vara ett sätt att uppfylla kravet på ansvarsskyldighet.

Rättsinformation:
- *Artikel 5.2*
- *Skäl 82*

5.2 Rättslig grund för behandling
För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett stöd i dataskyddsförordningen, en så kallad rättslig grund. En sådan rättslig grund är t.ex. samtycke från den registrerade, nödvändig för att fullgöra ett avtal med den registrerade, fullgöra en rättslig förpliktelse, skydda den registrerades grundläggande intressen, fullgöra en uppgift av allmänt intresse, samt efter en intresseavvägning.

Förutom kravet på rättslig grund måste behandlingen också uppfylla övriga bestämmelser i förordningen. Kom ihåg att möjligheten att behandla personuppgifter begränsas av de grundläggande principerna för behandling av personuppgifter och de ytterligare krav som tillkommer för vissa typer av personuppgifter, till exempel känsliga personuppgifter och uppgifter om lagöverträdelser.

För särskilda kategorier av personuppgifter (känsliga uppgifter), domar avseende brottmål, personnummer samt barn finns särskilda krav, se nedan.

5.2.1 Vanliga personuppgifter
En behandling av ”vanliga personuppgifter” är laglig om den följer vad som stadgas i Förordningens Artikel 6. Där räknas ett antal grunder upp varav de nedan är aktuella för bolaget med hänsyn tagen till dess verksamhet.

- Den registrerade har lämnat sitt samtycke.

- Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

- Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller

grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

- Arkivändamål

Rättsinformation:
- *Artikel 6*
- *Skäl 40-49*
- *Dataskyddslagen 2 kap 1-4§§*

5.2.2 Särskilda kategorier (känsliga) personuppgifter

Behandling av särskilda kategorier av personuppgifter är som utgångspunkt förbjudna, men får dock ske enligt Förordningens Artikel 9, varav följande är aktuella för bolaget med hänsyn tagen till dess verksamhet.

- Den registrerade har uttryckligen lämnat sitt samtycke (får inte ske konkludent).

- Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

- Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

- Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.

- Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.

- Behandlingen är nödvändig för arkivändamål av allmänt intresse.

Rättsinformation:
- *Artikel 9*
- *Skäl 34, 35, 51-56.*
- *Dataskyddslagen 3 kap. 1-7§§*

5.2.3 Personuppgifter som rör fällande domar i brottmål samt överträdelser

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder får endast utföras under kontroll av myndighet

eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Bolaget kan dock hantera personuppgifter avseende brottmål som målsägande avseende skadestånd/regresser. Denna behandling är laglig om den avser:

- rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras,
- en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras,
- behandlingen är nödvändig för att fullgöra en föreskrift på socialtjänstområdet,
- behandlingen avser uppgift i anteckningar som förs i fristående skolors elevvårdande verksamhet eller i motsvarande verksamhet hos enskilda anordnare av högskoleutbildning,
- behandlingen är nödvändig för kontroll av att jävssituation inte föreligger i advokatverksamhet eller annan juridisk verksamhet, eller
- uppgifterna avser personer i nyckelpositioner eller ledande ställning inom det egna bolaget eller koncernen och det är sakligt motiverat att behandla uppgifterna i särskilt inrättade rapporteringskanaler för att utreda om personen ifråga varit delaktig i allvarliga oegentligheter som rör bokföring, intern bokföringskontroll, revision, bekämpande av mutor, brottslighet inom bank- och finansväsen, eller andra allvarliga oegentligheter som rör organisationens vitala intressen eller enskildas liv och hälsa.

Rättsinformation:
- *Artikel 10*
- *Dataskyddslagen 3 kap. 8-9 §§*
- *Förordning 2018:219 §§ 5-6*
- *DIFS 2018:2*

5.2.4 Identifikationsnummer (personnummer)

Användning av personnummer får endast ske i följande fall:

- Den registrerade har samtyckt
- När det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av säker identifiering eller annat beaktansvärt skäl.

För bolagets del torde det i första hand röra sig om vikten av säker identifiering vid skadereglering av personskador, hantering av arbetstagare, skadelidande vid ansvarsskador m.m. Om ett ärende kan hanteras utan användande av personnummer ska så ske.

Rättsinformation:
- *Artikel 87*
- *Dataskyddslagen §§10-11*

5.3 Samtycke

Med samtycke avses varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Frivillighet
Ett frivilligt samtycke innebär att den registrerade har en genuin eller fri valmöjlighet, kan vägra eller ta tillbaka samtycke. Således får man inte göra ett avtal eller tjänst beroende av samtycke om behandling av personuppgifter om inte detta är nödvändigt för avtalet eller tjänsten.

Specifik
Samtycket måste vara specifikt för ett visst ändamål som är uttryckligt angivet, berättigat i förhållande till ändamålet, vara begränsat och inte generellt samt ha gjorts uppenbar innan behandlingen inleds.

Informerat
För att samtycket ska vara informerat ska den registrerade ha fått information enligt XX nedan samt ha informerats om följderna av att inte ge samtycke. Informationen ska lämnas innan behandling sker samt även vid ändrad behandling.

Informationen ska vara klar och tydlig, den ska särskiljas från andra frågor och inte vara invävd i annan information, vara begriplig, lättillgänglig och anpassad efter mottagaren. Således får inte informationen ex. vara en hänvisning till allmänna villkor som inte tillhandahålls vid tillfället för samtycke och där den registrerade inte kan välja att godta villkoren eller inte.

Otvetydig viljeyttring
Med en otvetydig viljeyttring avses en aktiv handling från den registrerade, muntlig, skriftlig, elektronisk eller konkludent (dvs genom sitt handlande, ex ansöker om skadeersättning och därvid lämnar uppgifter, OBS GÄLLER EJ KÄNSLIGA UPPGIFTER, se ovan).

En aktiv handling är ex:

- Samtycke på pappersblankett
- Kryssa i ruta på papper eller elektroniskt
- Klicka på länk online
- Välja mellan tydliga ja/nej alternativ
- Välja tekniska inställningar
- Svara på e-postmeddelande
- Svara på muntlig begäran
- Att aktivt ansöka eller efterfråga något och då lämna personuppgifter

Handlingar som inte är aktiva är ex:

- Tysta samtycken (om du inte säger nej så godkänner du)
- Hypotetiska samtycken (X vill nog för det är bra….)
- Förkryssade rutor
- Standardinställningar

För att det ska vara en otvetydig viljeyttring måste den registrerade faktiskt förstå att det handlar om ett samtycke, varför bolaget måste ta hänsyn till behandlingens art, ändamål, kategori av personuppgifter och vem som är registrerad (ålder, mental förmåga att förstå).

Bolaget ska sträva efter skriftligt samtycke i möjligaste mån, genom egna skadeanmälnings-blanketter eller genom dokumentering av konkludenta handlingar av registrerade, ex spara mail, spontananmälningar, förfrågningar m.m.

Rättsinformation:
- *Artikel 7 och 8.*
- *Skäl 32, 42 och 43.*

5.3.1 Återkallelse

Den registrerade har rätt att när som helst återkalla sitt samtycke, lika lätt och i samma form som de lämnades.

Efter ett återkallande får inte ytterligare personuppgifter samlas in eller behandlas, redan insamlade uppgifter inte uppdateras eller kompletteras.

Behandling får dock fortsatt ske med de personuppgifter som lämnats för samma ändamål.

Rättsinformation:
- *Artikel 7.3*

5.3.2 Barns samtycke avseende informationssamhällets tjänster

Med informationssamhällets tjänster avses alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535. Det rör sig om bland annat olika sociala medier, såsom till exempel bloggar, internetforum, webbplatser för videoklipp, chattprogram och sociala nätverk. Även onlinespel och olika applikationer (appar) med spel eller annat innehåll kan omfattasav definitionen.

När det gäller personuppgiftsbehandling som inte sker i samband med att informations-samhällets tjänster erbjuds får en bedömning, liksom tidigare, göras i varje enskilt fall av den registrerades förmåga att förstå innebörden av ett lämnat samtycke.

Vid erbjudande av informationssamhällets tjänster direkt till ett barn är behandling av personuppgifter som rör ett barn tillåten om barnet är minst 13 år.

Om barnet är under 13 år sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Med hänsyn till bolagets verksamhet torde inte några informationssamhällets tjänster bli aktuella för vår handläggning.

Rättsinformation:
- *Artikel 8*
- *Skäl 32, 38, 42-43.*
- *Dataskyddslag 2 kap 4§*

5.3.3 Dokumentation av samtycke

Den som behandlar personuppgifter med stöd av ett samtycke måste kunna visa att ett giltigt samtycke har lämnats av den registrerade. Personuppgiftsansvarig ska dokumentera samtycket för att kunna visa att det uppfyller de krav som gällande rätt kräver genom ett verifierbart bevis:

- Vem har samtyckt (t.ex namn, e-postadress, sessions id)
- När gavs samtycket (kopia av daterat dok, loggar m tidsangivelse etc)
- Vilken information lämnades (kopia på informationstext, policy m.m.)
- Hur samtycket lämnades (t.ex uppgifter i formulär)
- Om samtycket återkallats (t.ex. tidpunkt för återkallelse)

Rättsinformation:
- *Artikel 5*
- *Skäl 42*

6 Rättigheter för den registrerade

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade, eller att få ut eller flytta sina uppgifter. De registrerades rättigheter har utökats, förstärkts och specificerats i dataskyddsförordningen jämfört med personuppgiftslagen. Mer information om rättigheterna finns här nedan.

6.1 Allmänt avseende information och kontakter

Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla information och kommunikation, vilken avser behandling, i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn.

Rättsinformation:
- *Artikel 12*
- *Skäl 58-64*

6.1.1 Form av utlämnande och kontakt

Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. (Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat).

Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

6.1.2 Tid för utlämnande och kontakt (eller vägran att utlämna)

Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål, senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt nedan. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden.

Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen.

Om den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning.

6.1.3 Kostnader

Information som tillhandahålls och all kommunikation och samtliga åtgärder som vidtas ska tillhandahållas kostnadsfritt.

Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen:

- ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller

- vägra att tillmötesgå begäran.

Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig. Detta ska dokumenteras.

6.1.4 Kontroll av identitet

Identiteten fastställs genom de uppgifter som lämnas i ansökan, e-mail, eller muntligt. Om muntlig info ska ske skickas brev till folkbokföringsadressen med kodord eller så baseras det på information från tidigare kontakter som är unika i ärendet och som endast registrerad vet om (ex vad som står i skadeanmälan).

Bolaget skickar f.n. brev eller usb till folkbokföringsadressen vid lämnande av information eller registerutdrag, alternativt kan krypterad epost användas (se stadens regler för epost och kryptering)

6.1.5 Offentlighet samt begränsning av information

Reglerna om offentliga handlingar och sekretess (OSL) har företräde före de avseende dataskyddsreglerna, varför en begäran om offentlig handling ska handhas enligt OSL. Skyldigheten att lämna ut handlingar gäller dock inte elektronisk form, varför dataskyddsreglerna gäller för sådana handlingar.

Vid begäran om offentlig handling informeras dataskyddsombudet och ärendet lämnas till bolagsjuristen.

Bolaget informerar i färdiga texter om att behandling kan ske för OSL och registrerad behöver därför inte meddelas när någon begär ut offentliga handlingar.

Får man inte lämna ut handlingar pga sekretess gäller detta före förordningen.,

Rättsinformation:

- *Dataskyddslagen 1 kap 7§, 5 kap.*

6.2 Information

Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

Då bolaget endast handhar personuppgifter för handläggning av administration, skadereglering och försäkringar så finns färdiga texter på hemsidan, i skadeanmälnings-dokument samt i e-post. De är i dessa fall direkt nåbara för registrerad och någon särskild information behöver inte skickas ut. I andra fall samt vid begäran från registrerad och registerutdrag tillämpas reglerna nedan.

6.2.1 Information insamlad från den registrerade

Information från den registrerade ska vara skriftligt, elektroniskt eller muntligt på registrerads begäran (endast om identiteten kan fastställas) och ska lämnas när den samlas in. Information som den registrerade redan har behöver inte lämnas ut.

Följande information ska lämnas:

- Identitet och kontaktuppgifter för den personuppgiftsansvarige
- Kontaktuppgifter för dataskyddsombudet
- Ändamålen med behandlingen
- Den rättsliga grunden för behandlingen.
- Mottagarna eller kategorier av mottagare

- Eventuella överföringar av personuppgifter till ett tredjeland, huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

- Registrerads rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.

- Rätt att återkalla samtycke utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
- Rätten att inge klagomål till en tillsynsmyndighet

- Förekomsten av automatiserat beslutsfattande

Rättsinformation:
- *Artikel 13*
- *Skäl 58-64*
- *Artikel 29-gruppen, Riktlinje om automatiserat och individuellt beslutsfattande och begreppet profilering.*

6.2.2 Information insamlad från annan registrerade

Information från den registrerade ska vara skriftligt, elektroniskt eller muntligt på registrerads begäran (endast om identiteten kan fastställas, se dock OSL).

Bolaget skickar f.n. brev eller usb till folkbokföringsadressen vid lämnande av information eller registerutdrag, alternativt kan krypterad epost användas (se stadens regler för epost och kryptering)

Informationen ska lämnas ut:

- inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad

- om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade

- om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut för första gången.

Undantag från utlämnande av information:

- Information som den registrerade redan har behöver inte lämnas ut.

- Om det är omöjligt eller är en oproportionerlig ansträngning

- Omöjliggör eller allvarligt försvårar målen med behandlingen (ex. utredning om bedrägeri)

- Lagstadgad tystnadsplikt

Följande information ska lämnas:

- Identitet och kontaktuppgifter för den personuppgiftsansvarige

- Kontaktuppgifter för dataskyddsombudet

- Ändamålen med behandlingen

- Den rättsliga grunden för behandlingen.

- Kategorier av personuppgifter*

- Mottagarna eller kategorier av mottagare

- Eventuella överföringar av personuppgifter till ett tredjeland, huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
- Registrerads rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.

- Rätt att återkalla samtycke utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.

- Rätten att inge klagomål till en tillsynsmyndighet

- Personuppgifternas ursprung*

- Förekomsten av automatiserat beslutsfattande

Rättsinformation:
- *Artikel 14*
- *Skäl 58-64*

6.2.3 Registerutdrag – information på begäran av registrerad

Den registrerade har rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna samt information enligt nedan. (Se även Dataportabilitet nedan.)

Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna.

Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.

Bolaget skickar f.n. brev eller usb till folkbokföringsadressen. Om muntlig info ska ske skickas brev till folkbokföringsadressen med kodord som kvitteras i samtalet.

Information kan även skickas via e-post om den bifogade filen är krypterad genom Microsoft Office version 2007 eller senare förutsatt att dokumentet sparas i docx-format.

Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen.

Följande information ska lämnas:

- Ändamålen med behandlingen. (Se registerförteckningen)
- De kategorier av personuppgifter som behandlingen gäller. (Se registerförteckningen)
- De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer och rätt till information om de lämpliga skyddsåtgärder som vidtas (Se registerförteckingen)
- Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period. (Se registerförteckningen)
- Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling. (Se information på hemsidan)
- Rätten att inge klagomål till en tillsynsmyndighet. (Se information på hemsidan)
- Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer. (Se registerförteckningen)
- Förekomsten av automatiserat beslutsfattande.

Rättsinformation:

- *Artikel 15*
- *Skäl 58-64*

6.3 Rättelse

Registrerad har rätt att utan dröjsmål få felaktiga uppgifter rättade och kompletterade. Personuppgiftsansvarig ska kontrollera identiteten och dokumentera ändringen eller kompletteringen.

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Rättsinformation:

- *Artikel 16,19.*
- *Skäl 65*

6.4 Radering

Registrerad har rätt att utan dröjsmål få sina personuppgifter raderade på de grunder som anges nedan med beaktande av undantagen. Om uppgifterna offentliggjorts ska den personuppgiftsansvarige underrätta andra personuppgiftsansvariga/biträden att radera eventuella länkar till, eller kopior eller reproduktioner av dessa personuppgifter.

Med anledning av att bolaget omfattas av offentlighets- och sekretesslagen samt arkivlagen ska radering alltid diskuteras med och utredas av dataskyddsombudet samt stadens generella och bolagets specifika bevarandehandling/gallringsbeslut kontrolleras.

Personuppgiftsansvarig ska kontrollera identiteten och dokumentera raderingen.

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om radering av personuppgifter om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Grunder för radering:

- Uppgifterna är inte längre nödvändiga för de ändamål för vilka de samlats in
- Samtycke återkallas och det inte finns någon annan rättslig grund
- Olaglig behandling
- Rättslig förpliktelse
- Insamling har skett i samband med erbjudande av informationssamhällets tjänster till barn.

Undantag från radering:

- Utövande av yttrande- och informationsfrihet
- Rättslig förpliktelse
- Arkivändamål
- Fastställa, göra gällande eller försvara rättsliga anspråk.

Rättsinformation:
- *Artikel 17,19*
- *Skäl 65-66*

6.5 Begränsning av behandling

Registrerad har rätt att kräva begränsning av behandlingen om:

- Registrerad bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige en möjlighet att kontrollera om personuppgifterna är korrekta.
- Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.
- Den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
- Den registrerade har invänt mot behandling genom berättigat intresse, direkt marknadsföring i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

Om behandlingen har begränsats får sådana personuppgifter, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

En registrerad som har fått behandling begränsad ska underrättas av den personuppgifts-ansvarige innan begränsningen av behandlingen upphör.

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om begränsningar av behandling som om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Personuppgiftsansvarig ska kontrollera identiteten och dokumentera ändringen eller kompletteringen.

Rättsinformation:

- *Artikel 4.3, 18, 19*
- *Skäl 67*

6.6 Dataportabilitet

Den registrerade har i vissa fall rätt att få ut de personuppgifter som rör honom eller henne i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig (direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt).

Personuppgiftsansvarig ska kontrollera identiteten och dokumentera.

F.n. utges personuppgifterna genom att usb sänds till folkbokföringsadressen i word, excel eller excelformat, alternativt krypterat via epost (se stadens regelverk avseende epost).

Förutsättningar för dataportabilitet:

- Avser endast personuppgift som den registrerade har tillhandahållit den personuppgiftsansvarige

- Behandlingen grundas på samtycke

- Behandlingen är automatiserad

- Dataportabilitet får inte påverka andras rättigheter på ett ogynnsamt sätt.

Rättsinformation:
- *Artikel 20*
- *Skäl 68*
- *Artikel 29-gruppen, Riktlinjer om rätten till dataportabilitet*

6.7 Invändningar

Invändningar av den registrerade mot behandling av personuppgifter får ske enligt nedan.

Personuppgiftsansvarig ska kontrollera identiteten och dokumentera hanteringen i skadeakt/system.

Rättsinformation:
- *Artikel 21*
- *Skäl 69-70*

6.7.1 Behandling pga. allmänt intresse eller intresseavvägning

Den registrerade har rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på allmänt intresse eller berättigat intresse (se laglighet ovan) inbegripet profilering som grundar sig på dessa bestämmelser.

Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa:

- Tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter

- Fastställande, utövande eller försvar av rättsliga anspråk.

6.7.2 Direkt marknadsföring

Om personuppgifterna behandlas för direkt marknadsföring har registrerade rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

Senast vid den första kommunikationen med den registrerade ska den rätt som avses ovan uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information.

6.7.3 Informationssamhällets tjänster

När det gäller användningen av informationssamhällets tjänster får den registrerade utöva sin rätt att göra invändningar på automatiserat sätt med användning av tekniska specifikationer.

6.7.4 Behandling pga. vetenskapliga, historiska eller statistiska ändamål

Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål har den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

6.8 Automatiserat individuellt beslutsfattande

Den registrerade har rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling. Behandlingen får dock ske om det är nödvändigt för ingående eller fullgörande av avtal, samtycke eller enligt gällande rätt. För särskilda kategorier av personuppgifter får automatiserat beslutsfattande endast ske efter registrerads samtycke.

Den personuppgiftsansvarige ska genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna utrycka sin åsikt och bestrida beslutet.

Rättsinformation:
- *Artikel 22, 13.2 f, 14.2g,*
- *Skäl 71,72*

7 Registerförteckning

Personuppgiftsansvarig och personuppgiftsbiträde ska föra skriftligt/elektroniskt register över behandling som utförs av dem.

Bolaget har ett register för all sina behandlingar under G/2Verksamhetsstöd/2.5 Kommunicera/PUL.

Rättsinformation:

- *Artikel 30*
- *Skäl 82*

7.1 Registerförteckning personuppgiftsansvarig

Följande uppgifter ska finnas i registret:

- Namn och kontaktuppgifter på personuppgiftsansvariga och dataskyddsombud
- Ändamålen med behandlingen
- Kategorier av registrerade
- Kategorier av personuppgifter
- Kategorier av mottagare
- Överföringar till tredjeland och vidtagna säkerhetsåtgärder
- Tidsfrister för radering av uppgifter
- Beskrivning av tekniska och organisatoriska säkerhetsåtgärder

7.2 Registerförteckning personuppgiftsbiträde

Följande uppgifter ska finnas i registret:

- Namn och kontaktuppgift för personuppgiftsbiträdena och personuppgiftsansvarig samt dataskyddsombud
- Kategorier av behandling som utförs
- Överföringar till tredje land och skyddsåtgärder
- Beskrivning av tekniska och organisatoriska säkerhetsåtgärder

8 Säkerhet

8.1 Dataskydd

Inbyggt dataskydd (privacy by design) innebär att man tar hänsyn till integritetsskydds-reglerna redan när man utformar it-system och rutiner. Det är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas.

Kravet på dataskydd som standard (privacy by default) innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst för sociala media är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas.

Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder.

Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

Exempel på åtgärder är:

- Pseudonymisering och kryptering
- Backup
- Regelbundna tester/undersökningar av teknik och organisation
- Säkerhetsnivå baserad på risken för oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst.
- Biträden och andra endast behandlar personuppgifter efter personuppgiftsansvarigs instruktion.

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Bolagets principer för dataskydd framgår av Stockholm stads allmänna regler för dataskydd där krav ställs på åtkomst, loggning, rutiner, backup, kryptering, hantering m.m.:

- Riktlinje för informationssäkerhet
- Handbok för informationsklassificering.
- Kryptorekommendationer

Rättsinformation:
- *Artikel 25, 32,*
- *Skäl 78, 83*

8.2 Skyddade personuppgifter

Skyddade personuppgifter hanteras i enlighet med Stockholm stads riktlinje ”Stadsövergripande policy om skyddade personuppgifter”.

8.3 Personuppgiftsincident

Med personuppgiftsincident avses en incident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

Vid personuppgiftsincident ska riskhanteringsansvarig och dataskyddsombudet informeras och incidenten dokumenteras, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Personuppgiftsbiträden ska utan onödigt dröjsmål informera personuppgiftsansvarig efter att ha fått vetskap om en personuppgiftsincident och därvid bistå personuppgiftsansvarig på alla sätt.

Dokumentering sker i bolagets incidentrapporteringssystem IA där även kopior på anmälningar och information ska biläggas.

Dataskyddsombudet beslutar i samråd med riskhanteringsansvarig och handläggare huruvida anmälan ska ske till tillsynsmyndigheten eller inte samt om registrerade ska informeras.

Rättsinformation:

- *Artikel 33,34.*
- *Skäl 85-88*

8.3.1 Anmälan till tillsynsmyndigheten

Incidenter ska anmälas till tillsynsmyndigheten såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter

Vid incident ska personuppgiftsansvarig anmäla incidenten till tillsynsmyndigheten utan onödigt dröjsmål, och om möjligt, inte senare än 72 timmar efter vetskap om incidenten. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

I anmälan till tillsynsmyndigheten ska följande information ingå:

- Incidentens art
- Kategorier av och antalet registrerade som berörs
- Kategorier av och antalet personuppgiftsposter som berörs
- Namn och kontaktuppgifter till dataskyddsombudet samt andra relevant kontakter
- Konsekvensbedömning av incidenten
- Åtgärder som vidtagits eller kommer att vidtas för att åtgärda incidenten

- Åtgärder för att mildra incidentens potentiellt negativa effekter

8.3.2 Information till den registrerade

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

Registrerad behöver inte informeras om något av följande uppfylls:

- Lämpliga tekniska och organisatoriska skyddsåtgärder vidtagits
- Åtgärder vidtagits som innebär att den ev höga risken inte uppstår
- Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

Den information som ska lämnas är densamma som till tillsynsmyndigheten, men ska var särskilt tydlig och klar.

9 Konsekvensbedömning av dataskydd

I vissa fall måste personuppgiftsansvarig genomföra en konsekvensbedömning innan behandling sker samt, om hög risk föreligger, samråda med tillsynsmyndigheten.

Konsekvensbedömningen ska dokumenteras under G/.

9.1 Konsekvensbedömning

Om en typ av behandling (särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål) sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

Konsekvensbedömning ska särskilt ske i följande fall:

- Systematisk och omfattande bedömning av fysiska personers personliga aspekter
- Behandling i stor omfattning av särskilda kategorier av uppgifter
- Behandling av personuppgifter fällande domar i brottmål eller överträdelser
- Systematisk övervakning av allmän plats i stor omfattning

Den personuppgiftsansvarige ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförande av en konsekvensbedömning avseende dataskydd.

Konsekvensbedömningen ska minst innehålla:

- Systematisk beskrivning av behandlingen
- Behandlingens syften
- Personuppgiftsansvariges berättigade intresse
- Bedömning av behovet och proportionaliteten med behandlingen
- Utvärdering av riskerna för de registrerades rättigheter och friheter
- Åtgärder för att hanteras riskerna (ex. skyddsåtgärder, säkerhetsåtgärder, rutiner)
- (om lämpligt inhämta registrerades synpunkter eller förklara varför så inte skett)

Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Rättsinformation:
- *Artikel 35*
- *Skäl 89-95*
- *Artikel 29-gruppen, Riktlinjer för konsekvensbedömning*

9.2 Förhandssamråd

Den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.

Vid samråd ska följande information lämnas till tillsynsmyndigheten:

- i tillämpliga fall de respektive ansvarsområdena för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden
- ändamålen med och medlen för den avsedda behandlingen
- de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,
- i tillämpliga fall kontaktuppgifter till dataskyddsombudet
- konsekvensbedömningen avseende dataskydd
- all annan information som begärs av tillsynsmyndigheten.

Rättsinformation:
- *Artikel 36*
- *Skäl 89-95*

10 Överföring till tredje land

Som huvudprincip är överföring av personuppgifter utanför EU/EES förbjuden. Överföring får dock ske om någon av följande förutsättningar föreligger:

- EU-kommissionen har beslutat att ett land har adekvat skyddsnivå
- Personuppgiftsansvarig/biträde har vidtagit lämpliga skyddsåtgärder
- Särskilda situationer

För bolagets del kan detta vara aktuellt om t.ex. servrar/backup finns i land utanför EU/EES.

Personuppgiftsansvarig ska rådfråga dataskyddsombudet innan behandling sker och utredningen ska dokumenteras som behandlingar i övrigt.

Rättsinformation:
- *Artikel 44-50*
- *Skäl 101-116, 169.*

10.1 Godkända länder

Se ”Commission decisions on the adequacy of the protection of personal data in third countries”

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

10.2 Lämpliga skyddsåtgärder

I avsaknad av ett beslut om godkännande av ett land från EU-kommissionen kan personuppgiftsansvarig/biträde vidta nedan nämnda skyddsåtgärder, varvid överföring är tillåten.

Märka att en dator eller mobil som tas med utanför EU/EES utgör en tredjelandsöverföring.

Utan tillstånd från tillsynsmyndigheten:

- rättsligt bindande och verkställbart instrument mellan offentliga myndigheter
- bindande företagsbestämmelser (standarsklausuler BCR:s ska ha antagits eller godkänts av EU-kommissionen eller av en tillsynsmyndighet. Det behövs däremot inget särskilt tillstånd av tillsynsmyndighet för varje överföring.)
- standardiserade dataskyddsbestämmelser som antas av kommissionen
- standardiserade dataskyddsbestämmelser som antagits av en tillsynsmyndighet och godkänts av kommissionen
- godkänd uppförandekod
- godkänd certifieringsmekanism

Med tillstånd från tillsynsmyndigheten

- avtalsklausuler med personuppgiftsansvarig/biträde i tredjeland
- bestämmelser i administrativa överenskommelser mellan offentliga myndigheter

10.3 Särskilda situationer

I vissa situationer får personuppgifter överföras till tredjeland:

- Samtycke
- Fullgöra avtal eller åtgärder som föregår avtal på den registrerades begäran
- Fullgöra avtal eller åtgärder som föregår avtal i den registrerades intresse
- Allmänt intresse
- Nödvändig för rättsliga anspråk
- Intresseavvägning i enstaka fall (visst förfarande och dokumentation enligt Förordningen Artikel 49)

11 Outsourcing

Vid outsourcing ska krav på redovisning av hur personuppgifter behandlas finns i upphandlingsunderlaget. Det skall särskilt beaktas om motparten eller underleverantör behandlar data utanför EU/EES.

Upphandlingsunderlaget ska vidare innehålla krav på personuppgiftsbiträdet enligt 2.4 ovan.

Ansvarig för upphandlingen/ansvarig kontrollerar inom ramen för kontraktsuppföljning biträdets hantering av personuppgifter.

12 Dokumentation

Dokumentation av utredning, register, konsekvensbedömning, kontakter med tillsynsmyndigheten, personuppgiftsincidenter etc sker under

12.1 Utredning inför behandling

Utredning sparas under G/

12.2 Registerförteckning

Sparas under G/

12.3 Konsekvensbedömning

Sparas under G/

12.4 Incidenter
Sparas i IA samt kopia under G/

12.5 Utbildning
Sparas under G/

12.6 Intresseavvägning och godkännanden vid tredjelandsöverföring
Sparas under G/

12.7 Personuppgiftsbiträdesavtal m.m.
Sparas under G/ samt i avtalsdatabasen G/2/2.4/2.4.3/Avtal

Biträdets registerförteckningar sparas på samma sätt.

12.8 Dataportabilitet
Begäran och sändkvitto eller motsvarande sparas under G/

12.9 Samtycke
Sparas i den form den inkommit i det ärende den tillhör, ex. skadeakt.

12.10 Information
Sparas i den form den utgivits i det ärende den tillhör, ex skadeakt. Allmänna informationsskrifter för bolaget sparas under G/.

12.11 Registerutdrag
Begäran sparas i den form den inkom tillsammans med registerutdraget och bevis för utskick under G/.

12.12 Rättelse, radering, begränsning, invändningar
Begäran och åtgärd sparas under G/.

12.13 Rapporter
Sparas under G/.

13 Rapportering
Incidenter rapporteras av respektive handläggare till Riskhanteringsansvarig, Dataskyddsombud ,VD samt noteras i IA. Om en incident innebär att anmälan sker till tillsynsmyndigheten eller att registrerad informeras ska detta meddelas styrelsen av dataskyddsombudet.

Dataskyddsombudet ska årligen utfärda en rapport till VD och styrelse avseende bolagets personuppgiftsbehandling. I denna rapport ska följande redovisas:

- Bolagets behandlingar av personuppgifter (registerförteckningen)
- Genomförda kontroller
- Sammanställning över eventuella incidenter och hur dessa hanterats

- Rekommendationer som lämnats till verksamheten
- Eventuella konsekvensbedömningar som genomförts

14 Utbildning

Samtlig personal ska utbildas av dataskyddsombudet eller annan med erforderliga kunskaper i dessa riktlinjer och den process som gäller för företaget.

Utbildningen ska dokumenteras och ange när och var den ägts rum, vad den avsett, vilka som deltagit samt ska undertecknas av utbildare och deltagare.

Dokumentation sker under G/

15 Kontroll

Handläggare ansvarar för att kontroll enligt 2.3 ovan sker innan behandling utförs och av personuppgiftsbiträdens behandlingar och datasäkerhet samt riktlinjer inom ramen för kontraktsuppföljning.

Dataskyddsombudet kontrollerar att uppföljning sker av personuppgiftsbiträden, att tillgång till system är begränsat till de som behöver dem for sin handläggning, att regler kring personuppgifter finns vid upphandling, att system har informationsklassats och åtgärder vidtagits för datasäkerhet.

16 Klagomål

Den som anser att någon behandlar uppgifter om honom eller henne i strid med dataskyddsförordningen kan lämna in ett klagomål till Datainspektionen.

Datainspektionen tar del av alla klagomål och bedömer om tillsyn ska inledas och lämnar därefter besked till den som fört fram klagomålet. Datainspektionen måste meddela om tillsyn ska inledas eller inte inom tre månader efter att ha tagit emot klagomålet. Om den klagande inte får besked inom den tiden, kan han eller hon vända sig till domstol för att begära besked.

Bolaget har även en intern Riktlinje för hantering av klagomål” enligt regelverket för Solvens 2.

17 Lagring och gallring

Personuppgifter ska inte lagras längre eller i större omfattning än vad som är nödvändigt för ändamålet med behandlingen.

Som offentligt ägt bolag omfattas S:t Erik av arkivlagen. Regler för arkivering finns således i arkivlagen, arkivregler för Stockholms stad, riktlinjer för arkivregler i Stockholms stad samt att värdera och gallra information i Stockholms stad. Med ledning av dessa har bolaget en hanteringsanvisning under G/.

Generellt anpassar bolaget sin lagring/gallring som följer.

Försäkringsavtal	tills försäkringen upphör samt preskriptionstid (10 år från avtalets upphörande)

Skadereglering	preskriptionstid (10 år efterförsäkringsfall)
Bokföring	bokföringslagen, normalt 7 år
Avtal	preskriptionslagen (normalt 10 år)

S:T ERIK FÖRSÄKRINGS AB:S RIKTLINJER FÖR INTERN STYRNING OCH KONTROLL

FASTÄLLD AV STYRELSEN 2022-05-23

Innehållsförteckning

1. Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna är föremål för revidering och skall fastställas årligen av styrelsen för bolaget.

1.1 Syfte med riktlinjerna

Syftet med dessa riktlinjer är att på ett åskådligt och övergripande plan:

- ge mål och riktlinjer för bolagets interna styrning och kontroll,
- ange hur ansvaret för den interna styrningen och kontrollen fördelas,
- beskriva hur bolagets interna styrning och kontroll är organiserad.

1.2 Generella principer för intern styrning och kontroll inom S:t Erik Försäkrings AB

Styrelsen och den VD skall verka för att en god styrning och kontroll präglar organisationen och driften av företagets verksamhet.

1.3 Uppdatering av riktlinjerna

VD ansvarar för att riktlinjerna löpande hålls uppdaterad.

2. Bolagets strategi för god intern kontroll

2.2 Allmänt

Styrelsen måste ha klara och tydliga regler för hur verksamheten skall organiseras och hur verksamheten skall förvaltas genom att upprätta instruktioner och styrdokument. Bolagets VD har i sin tur ansvaret för den löpande förvaltningen. Detta kräver att VD delegerar ansvaret vidare till bolagets anställda genom tydliga befattningsbeskrivningar och arbetsinstruktioner. I de fall verksamheten är utlagd på extern part måste klara och tydliga uppdragsavtal upprättas.

Samtliga styrdokument måste hållas löpande uppdaterade.

2.3 Fördela ansvar och arbete

Det är viktigt att styrelsen och VD fördelar ansvar och arbete på ett sådant sätt att intressekonflikter undviks.

2.4 Dela på handläggning av ärenden

För att minska risken för rena handläggningsfel och avsteg från fastställda instruktioner är det viktigt att samtliga arbetsinstruktioner upprättas så att det alltid är fler än en befattningshavare som handlägger ett ärende genom hela behandlingskedjan.

2.5 Verksamhetsuppföljning

För att kunna bedriva verksamheten på ett effektivt sätt krävs att verksamheten följs upp löpande och på ett ändamålsenligt sätt som en del av bolagets processer.

2.6 Informations- och rapporteringssystem skall innehåll aktuell och relevant information

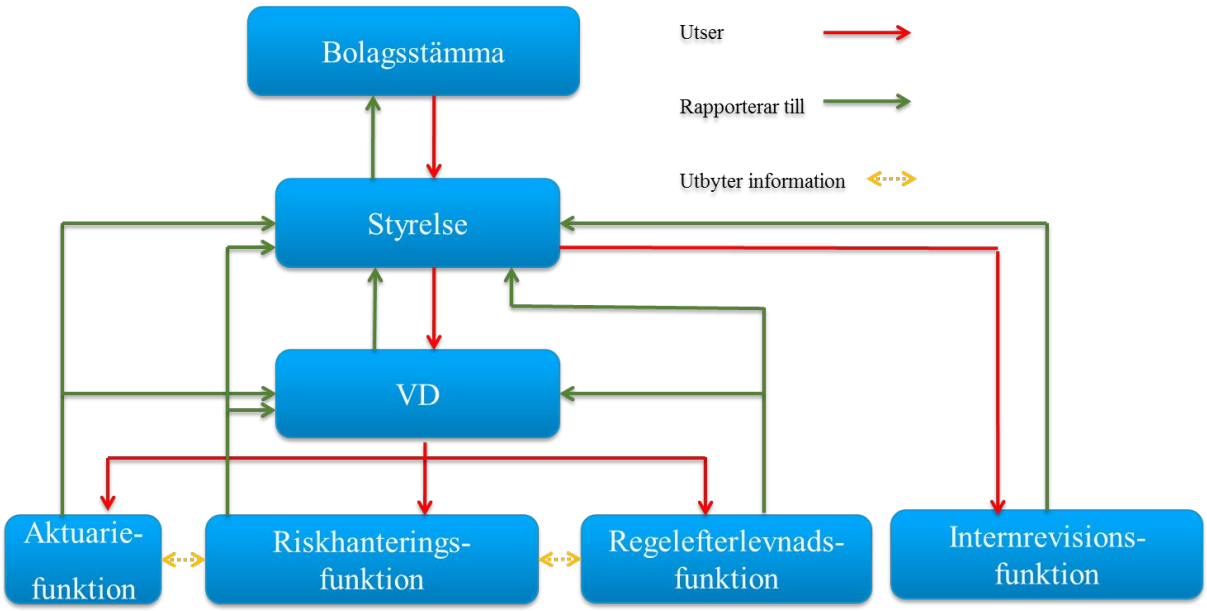
En stor risk i samband med beslutsfattande är att beslutsunderlaget inte stämmer överens med verkligheten vilket i sin tur leder fram till felaktiga beslut. Av det skälet är det mycket viktigt att bolagets informations- och rapporteringssystem innehåller aktuell och relevant information och att processer utarbetas för att så kan ske.

3. Organisation, ansvar och rutiner för intern styrning och kontroll

3.1 Rutiner för intern styrning och kontroll

Intern styrning och kontroll finns definierat i en mängd dokument på verksamhetsnivå, processbeskrivningar, Riktlinjer för rapportering m.fl. Av de dokumenten framgår de kontroller och beslut som fattas i allt från kontroll av upphandlingsunderlag till beslut av styrelsen avseende rapportering av SCR.

Detta dokument ger en översiktlig beskrivning av den interna styrningen.



Figuren visar S:t Erik Försäkrings AB:s organisation för riskhantering och intern kontroll

3.2 Ansvarsfördelning

3.2.1 Ägarens ansvar

- Att fastställa bolagets bolagsordning
- Att fatta beslut på bolagsstämman

3.2.2 Styrelsen i bolagets ansvar

Styrelsen är ytterst ansvarig för bolagets verksamhet. Styrelsen skall årligen fastställa de mål och strategier som skall gälla för verksamheten. Styrelsen skall tillse att erforderliga regler avseende intern styrning och kontroll föreligger och fatta övergripande beslut i enlighet med gällande regelverk.

3.2.3 VD:n i bolagets ansvar

VD svarar för att verksamheten i bolaget bedrivs i enlighet med ägarens och styrelsens fastställda instruktioner samt gällande regler i övrigt för verksamheten. VD svarar också för att verksamheten bedrivs inom de riskmandat styrelsen fastslagit i sina policydokument för respektive riskområde/riskslag. VD utser funktionsansvariga har det yttersta ansvaret för att kontraktsuppföljning sker samt att kontroller görs löpande i verksamheten.

3.2.4 Internrevision

Internrevision tillsätts av styrelsen och har i uppdrag att utföra oberoende granskning av verksamheten med avseende på bland annat tillförlitlighet och effektivitet i organisationen. Därutöver inbegriper uppdraget granskning av den interna kontrollen samt bolagets andra centrala funktioner.

För att säkerställa att den oberoende granskningsfunktionen verkligen är oberoende gentemot de delar av den operativa verksamheten som den är satt att granska, ska ansvarig för internrevision rapportera direkt till styrelsen.

Funktionens uppdrag regleras av bolagets instruktion för internrevision.

3.2.5 Regelefterlevnadsfunktionen

Regelefterlevnadsfunktionen ansvarar för att kontrollera och informera verksamheten (första linjen), företagsledning och styrelsen om regelefterlevnadsrisker, ex. lagstiftning, god affärssed, etiska regler, och rekommendationer från branschorganisationer samt interna regler. Detta kan även t.ex. innebära en viss kontroll av information från andra funktioner till den del dessa ingår som en del av bolagets rapportering till Finansinspektionen, att funktionerna har upprättats och anmälts till Finansinspektionen m.m., men inte en generell kontroll av dessa funktioners tillförlitlighet eller effektivitet. Detta åligger internrevisionen, se 3.2.4.

Funktionen ansvarar inte för finansiella risker, civilrättsliga, skatterättsliga, redovisningsrättsliga, konkurrensrättsliga frågor eller frågor som rör hantering av personuppgifter eller säkerställande av det numeriska underlaget för bolagets kapitaltäckning.) Detta hanteras av andra funktioner i bolaget.

Funktionens uppdrag regleras av bolagets riktlinjer för funktionen för regelefterlevnad.

3.2.6 Riskhanteringsfunktionen

Riskhanteringsfunktionen övervakar bolagets samlade riskexponering (riskprofil) och verkar för att effektivisera riskhanteringssystemet. Funktionen ska informera bolagets styrelse och ledning om bolagets risker i en samlad form.

Riskhanteringsfunktionen ska ge en samlad, allsidig och saklig bild av bolagets väsentliga risker och ska analysera och övervaka riskutvecklingen, särskilt ska funktionen bevaka och rapportera framväxande risker. Funktionen ska i analysen väga in och bedöma all information eller rapporter som är relevanta för utvärderingen av riskprofil och riskhanteringssystem. Det innefattar information även från ekonomi-, aktuarie- och regelefterlevnadsfunktionerna. Riskhanteringsfunktionen ska särskilt samarbeta nära med aktuarien.

Funktionen ansvarar för att genom riskregistret kontrollera att varje väsentlig risk har en riskägare samt att följa upp att risken hanteras av verksamheten och därvid rapportera avvikelser till verksamheten, styrelsen och VD.

Riskhanteringsfunktionen ansvarar för att kontrollera att incidenter rapporteras korrekt och att beslutade åtgärder föranledda av incidenter genomförs. Funktionen kontrollerar även att verksamheten genomför riskanalyser inför outsourcing och affärsbeslut.

Funktionens uppdrag regleras av bolagets instruktion för riskhanteringsfunktionen och av styrelsen beslutad årsplan.

3.2.8 De anställdas och underleverantörernas ansvar

De anställda skall utföra sitt arbete i enlighet med fastställda instruktioner och befattningsbeskrivningar samt fastställda tariffer och försäkringsplan. Samtliga anställda har också skyldighet att informera VD och andra berörda funktioner om incidenter, risker och händelser av väsentlig betydelse.

Verksamheten äger riskerna och de aktiviteter som behövs för att hantera dem samt utför löpande kontroller enligt ett dualistiskt synsätt. Underleverantörerna skall utföra sitt arbete i enlighet med upprättade uppdragsavtal.

3.2.9 Aktuarie

Kontrollen av bolagets försäkringsrisker som kan beräknas med statistiska metoder (ex IBNR) ska utföras och rapporteras fortlöpande av bolagets aktuarie till verksamheten och styrelsen. Aktuarien lämnar information till riskhanteringsfunktionen om försäkringsrisker. Aktuarien uttalar sig även om kvalitén på den information som finns i bolagets IT-system och som används av aktuarien.

Funktionens uppdrag regleras av gällande aktuarieinstruktion.

4. Återrapportering och uppföljning

4.1 Rutiner för återrapportering

Återrapporteringen i bolaget skall vara utformad så att samtliga berörda enheter, inklusive ägare och styrelse, dels får sådan saklig, utförlig och relevant information som behövs för att kunna fatta väl underbyggda beslut, dels att löpande informeras om utvecklingen av företagets verksamheter.

4.2 Rapportering

4.2.1 Från verksamheten

Samtliga anställda som får kännedom om en incident, risk eller händelse av väsentlig betydelse skall genast informera VD och berörd funktion om händelsen. Genom bolagets IT-system får VD även kännedom om tecknade försäkringar, inträffade skador samt ekonomiskt utfall.

4.2.2 Från funktionen för regelefterlevnad

Funktionen för regelefterlevnad skall informera styrelse, företagsledning och anställda om ändrad lagstiftning, god affärssed, etiska regler och rekommendationer från branschorganisationer, samt interna regler. Rapportering sker i enlighet med av styrelsen beslutad instruktion.

4.2.3 Från internrevision

Internrevisionen skall minst en gång om året utvärdera och rapportera statusen på den interna kontrollen inom bolaget och rekommendera åtgärder till företagsledningen för att komma tillrätta med brister.

4.2.4 Från funktionen för riskhantering

Riskhanteringsfunktionen ska, med av styrelsen i årsplanen beslutat intervall samt vid behov, sammanställa en skriftlig sammanfattande riskrapport. Riskrapporten beaktar samtliga övriga funktioners rapporter och ger en detaljerad, allsidig och saklig bild av bolagets samtliga väsentliga risker inklusive deras förändring och eventuella framväxande risker.

Funktionen avger en årlig incidentrapport med en samlad analys av inträffade incidenter, uppföljning av vidtagna åtgärder analys och förslag till ytterligare förbättringsförslagförbättringar. Funktionen avger också en årsrapport som beskriver hur de övriga kontroller som funktionen ansvarar för genomförts.

Rapportering sker enligt gällande instruktion för riskhanteringsfunktionen.

4.2.6 Från VD

VD skall för styrelsen presentera budget och långsiktig strategisk inriktning, kvartalsrapporter med prognoser samt årsbokslut i enlighet med ”instruktion för rapportering av bolagets ekonomiska situation m.m.”

Vid behov skall VD även ge förslag på ändrade instruktioner och riktlinjer. I särskilda fall skall VD även lägga fram en ”särskild riskrapport”.

VD skall även årligen redovisa genomgång av kontraktsuppföljning och internkontrollplan.

4.2.7 Från Styrelsen

Bolagets styrelse ansvara för att det upprättas årsredovisning och revisionsberättelse till ägarna.

4.2.8 Från aktuarie

Aktuarien skall, till berörda funktioner, löpande tillhandahålla underlag för den aktuariella delen av rapporteringen, årligen lämna aktuarieutlåtande och försäkringsteknisk utredning till bolagets styrelse samt, på styrelsens begäran, medverka vid styrelsemöten.

RIKTLINJER FÖR S:T ERIK FÖRSÄKRINGS INTERNREVISION

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna skall revideras årligen och fastställas av styrelsen.

2 Internrevisionens oberoende

För att säkerställa att den oberoende granskningsfunktionen verkligen är oberoende gentemot de delar av den operativa verksamheten som den är satt att granska, ska ansvarig för granskningsfunktionen rapportera direkt till styrelsen. Utöver riktlinjerna i detta dokument skall den oberoende granskningsfunktionen fritt bestämma över sitt eget arbete.

3 Syfte och ansvarsfördelning

Internrevisionen inom S:t Erik Försäkring ska vara en resurs för styrelsen att utföra oberoende granskning av verksamheten i enlighet med p 4 nedan.

Den oberoende granskningsfunktionens arbete gränsar till den externa granskning som utförs av företagets externa auktoriserade revisor. Som gränsdragning i granskningsarbetet ska då gälla att den oberoende granskningsfunktionen inriktar sig på den interna kontrollen, medan den externa granskningen inriktar sig på företagets redovisning och årsbokslut. Den person som leder den oberoende granskningsfunktionen är ansvarig för att samordna granskning- och revisionsarbetet så att inget område hamnar utanför granskningen eller utsätts för dubbel granskning.

Företagsledningen är ansvarig för att utveckla och underhålla strukturer för intern kontroll och genomföra de åtgärder som styrelsen beslutar med aneldning av funktionens rekommendationer.

Styrelsen ansvarar för att besluta om revisionsplan, vilka åtgärder som vidtas med anledning av funktionens rekommendationer och att åtgärderna genomförs.

Anställda är ansvariga inom sitt arbetsområde för efterlevnaden av de riktlinjer, instruktioner och rutiner som finns på plats för att åstadkomma en god intern kontroll.

Den granskning som utförs av den oberoende granskningsfunktionen befriar inte någon del av organisationen från dess delegerade ansvar för intern kontroll.

4 Omfattning av granskning

Internrevisionen är ansvarig för att:

- utvärdera systemet för internkontroll
- utvärdera andra delar av företagsstyrningssystemet
- rapportera resultat och lämna rekommendationer till företagets styrelse och ledning
- kontrollera verkställande av beslut baserade på funktionens rekommendationer
- minst årligen upprätta en riskbaserad revisionsplan för granskning de kommande åren

Internrevisionen har rätt till obegränsad tillgång till all verksamhetsrelaterad information inom bolaget.

5 Granskningsprocessen

Internrevisionen ska planera sitt arbete väl i förväg genom att bedöma var i verksamheten det kan vara störst risk för brister och årligen upprätta en riskbaserad revisionsplan som föreläggs styrelsen för beslut.

Funktionen ska i övrigt arbeta systematiskt och noggrant med rekommendationer och åtgärder.

6 Rapportering och uppföljning

Internrevisionen ska rapportera skriftligen minst en gång per år till styrelsen och VD samt skall närvara vid styrelsemöte då rapporten behandlas. Rapporten ska presenteras snarast möjligt efter avslutad granskningsprocess. Om det har upptäckts allvarliga brister ska detta rapporteras snarast till VD respektive styrelsen.

Rapporten ska innehålla rekommendationer, vem som ansvarar för en åtgärds genomförande och tidsschema för detta och för åtgärdernas genomförande. Samråd ska ske med verksamheten.

Internrevisionen skall följa upp åtgärder så snart de är utförda och sedan återkommande vid nästa granskning.

Riktlinjer för hantering och rapportering av händelser av väsentlig betydelse i S:t Erik Försäkrings AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

Innehåll

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Instruktionerna är föremål för revidering och skall fastställas årligen av styrelsen för S:t Erik Försäkring AB, nedan Bolaget.

Syftet med instruktionen är att bolaget ska ha en organisation och beredskap att meddela väsentliga händelser till Finansinspektionen. De händelser som anges är inte uttömmande.

2 Definition av händelse av väsentlig betydelse

Med händelser av väsentlig betydelse avses sådana händelser som kan äventyra Bolagets stabilitet eller skyddet för kundernas tillgångar och som skall rapporteras till Finansinspektionen enligt nedan.

Händelser av väsentlig betydelse som skall rapporteras så snart som möjligt till Finansinspektionen är sådana som kan medföra att:

A. -de ekonomiska förutsättningarna ändras, så att företaget inte kan uppfylla sina åtaganden mot kunder

B. -ett större antal försäkringstagare eller andra ersättningsberättigade orsakas betydande ekonomisk skada

   -en väsentlig ryktesförlust för företaget uppkommer

   Exempel på sådana händelser:

   -information i samband med kundtransaktioner är felaktig eller bristfällig

   -kundtransaktioner haneteras på ett felaktigt eller bristfälligt sätt

   -fel uppstår i tekniska system

   -interna eller externa regler överträds

C. – om Bolaget inte uppfyller solvenskapitalkravet eller om det finns risk för detta under de närmaste tre månaderna

D. -om en revisor vidtar åtgärder som anges i 9 kap 43-44 §§ ABL
(revisorns skyldighet att anmäla misstänkt brottslighet till styrelse och åklagare)

E. –händelser som kan medföra väsentliga förändringar av bolagets:
   a. Verksamhet och resultat
   b. Riskprofil
   c. Företagsstyrningssystem

Händelser där bolagets ska utvärdera om behov av rapportering av väsentliga händelser föreligger:

F. –förändring av affärstrategi

G. -förändring av organisation

H. –krav till följd av rättsliga processer

I. –fel eller brister i bolagets styrning och kontroll av verksamheten

J. Fel eller brister i processer, rutiner och tekniska system

Redogörelse på begäran av Finansinspektionen:

- Bolaget ska på begäran av Finansinspektionen upprätta och inlämna en redogörelse avseende Bolagets förmåga att hantera händelser eller förändringar av ekonomiska förhållanden som skulle kunna påverka företagets finansiella ställning negativt.

3 Handlingsplan

En anställd på Bolaget som får kännedom om en händelse av väsentlig betydelse ska genast informera VD och regelansvarig. VD skall informera regelansvarig om så inte skett samt styrelseordföranden och sammankalla till ett extra styrelsemöte så snart som möjligt. VD skall i samarbete med regelansvarig person genast samla in all tillgänglig information om händelsen. Informationen skall sammanställas i en rapport som snarast ska lämnas till styrelsen och Finansinspektionen. Rapporten ska innehålla

- Information om den anställdes tjänsteställning om någon anställd hos Bolaget är berörd.

- Beskrivning av händelsen. Av beskrivningen bör framgå förfaringssättet och övriga omständigheter av betydelse.

- Den ekonomiska omfattningen (beloppets storlek) samt en bedömning av den skada händelsen har förorsakat eller kan komma att förorsaka Bolagets eller dess kunder.

- Tidpunkt för upptäckten och uppgift om hur länge händelsen har pågått innan den upptäcktes.

- Omständigheter kring händelsens upptäckt, t.ex. den interna granskningsfunktionens roll. Det bör framgå om det har förekommit brister i Bolagets interna kontroll och i så fall vilka brister.

Vid det extra styrelsemötet ska VD redogöra för rapporten. Styrelsen har därefter att besluta om åtgärder. Om Bolaget har utsatts för ett misstänkt eller konstaterat brott bör VD eller styrelsen göra en anmälan till polis- eller åklagarmyndighet.

VD ska därefter, i samarbete med regelansvarig person, komplettera sin rapport med följande information:

- Beskrivning av vilka åtgärder som har vidtagits eller kommer att vidtas med anledning av händelsen beträffande t.ex. interna instruktioner, ansvars- och arbetsfördelning från kontrollsynpunkt, informations- och rapportsystem, kontroller för IT-säkerhet, kontroller inom ekonomisystem, redovisningsprinciper, information till drabbade kunder m.m.

- Vidtagna eller planerade disciplinära åtgärder.

- Tidpunkt för anmälan till polismyndighet.

VD ska därefter utan dröjsmål lämna den nya rapporten till Finansinspektionen och meddela regelansvarig person att så skett.

4 Intern information

VD bör skriva ett internt meddelande till samtliga medarbetare. Om anmälan har gjorts eller kommer att göras till polismyndighet bör särskild hänsyn till detta tas vid bedömningen av vilken information om berörda personer som ska inkluderas i meddelandet.

5 Extern information

Alla kontakter med media sköts av VD eller av företagsledningen utsedd talesperson, dock med beaktande av anställds lagliga rätt att yttra sig i media.

RIKTLINJER FÖR RISKHANTERING I S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt
Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Dokumentet revideras vid behov och fastställs årligen av styrelsen.

2 Inledning
Risker i företagets verksamhet utgörs huvudsakligen av försäkringsrisker, finansiella risker och operativa risker.

3 Syfte
Syftet med S:t Erik Försäkrings riktlinjer för riskhantering är att säkerställa att bolagets samtliga risker blir löpande identifierade, bedömda, prioriterade och hanterade på ett enhetligt sätt för att uppnå bolagets fastlagda mål.

Vidare skall det framgå vilka ramar och riktlinjer som gäller för S:t Erik Försäkrings verksamhet när det gäller risker, ansvar och befogenheter.

Ytterst är målet att säkerställa en fortlöpande uthållig verksamhet genom att skydda bolagets anställda, dess tillgångar och åtaganden samt ytterst dess anseende och förtroende.

4 Övergripande mål och principer
Huvudmålet för S:t Erik Försäkrings verksamhet är att svara för att det finns en effektiv riskfinansiering av anläggningar och verksamheter ägda av Stockholms stad och närstående bolag genom ökad konkurrensutsättning. S:t Erik Försäkring ska förmedla försäkringslösningar, minimera försäkringskostnaderna och förbättra riskhanteringen för samtliga berörda enheter inom kommunkoncernen. S:t Erik Försäkrings AB ska vara det bästa och mest kostnadseffektiva alternativet för stadens nämnder och bolag. Samtliga sakförsäkringar som stadens nämnder och bolagsstyrelser har behov av ska tecknas med bolagets medverkan. Bolaget ska optimera den försäkringsrisk som bolaget själv tar, i förhållande till storleken på det egna kapitalet och fastslagen risknivå.

De överordnade målen med bolagets riskhanteringsprocess är att
- förebygga händelser som kan äventyra verksamheten eller allvarligt skada organisationens varumärke,
- förbättra bolagets måluppfyllelse och säkerställa dess framtida utveckling

5 Ansvarsområden och ansvarsfördelning

5.1 Styrelsen
Styrelsen har det yttersta ansvaret för att säkerställa att S:t Erik Försäkrings riskhanteringssystem är effektivt genom att fastställa företagets riskaptit och samlade risktolerans, samt godkänna huvudsakliga strategier och styrdokument för riskhantering. Styrelsen ansvara för att riktlinjer följs och fortlöpande prova om de behöver ändras. Styrelsen ska även anta finanspolicyn för Stockholms Stadshus AB årligen och säkerställa att den efterlevs av bolaget.

Styrelsens uppdrag regleras av bolagsordningen.

5.2 VD

VD svarar för att verksamheten i bolaget bedrivs i enlighet med ägarens och styrelsens fastställda instruktioner samt gällande regler i övrigt för verksamheten. VD svarar också för att verksamheten bedrivs inom de riskmandat styrelsen fastslagit i sina policydokument för respektive riskområde/riskslag. VD utser ansvarig för bolagets riskhanteringsfunktion och regelefterlevnadsfunktion, ansvarar för att kontraktsuppföljning sker samt att kontroller görs enligt internkontrollplan och löpande i verksamheten. VD ska tillse att sakbolagets finansiella tillgångar placeras i enlighet med riktlinjer för placeringar. Då det gäller placeringsriktlinjer ska samråd ske med internbanken inom Stockholms stad inför revidering och fastställande.

VD ansvarar för kontroller och risker som inte delegerats till annan funktion.

VD:s uppdrag regleras av ”Instruktion för arbetsfördelning mellan styrelse och VD”.

5.3 Anställda

De anställda ansvarar för att utföra sitt arbete i enlighet med fastställda riktlinjer, instruktioner och befattningsbeskrivningar. Anställda ska rapportera incidenter i enlighet med Stockholms Stads riktlinjer för incidentrapportering. Incidenter som ska rapporteras inkluderar de som kan få påverkan på S:t Erik Försäkrings affärsverksamhet.

Verksamheten äger riskerna och de aktiviteter som behövs för att hantera dem samt utför löpande kontroller enligt ett dualistisk (fler än en befattningshavare som handlägger ett ärende) synsätt.

5.4 Funktionen för regelefterlevnad

Funktionen för regelefterlevnad ska identifiera och bedöma regelefterlevnadsrisker (ej finansiella risker, civilrättsliga, skatterättsliga, redovisningsrättsliga, konkurrensrättsliga frågor eller frågor som rör hantering av personuppgifter eller säkerställande av det numeriska underlaget för bolagets kapitaltäckning) t ex vid framtagandet av nya produkter och tjänster, samt löpande informera om risker som kan uppkomma till följd av bristande regelefterlevnad till verksamheten, styrelsen, VD och riskhanteringsfunktionen.

Funktionens uppdrag regleras av bolagets riktlinjer för funktionen och uppdragsavtalet.

5.5 Funktionen för riskhantering

Riskhanteringsfunktionen övervakar bolagets samlade riskexponering (riskprofil) och verkar för att effektivisera riskhanteringssystemet. Funktionen ska informera bolagets styrelse och ledning om bolagets risker i en samlad form.

Riskhanteringsfunktionen ska ge en samlad, allsidig och saklig bild av bolagets väsentliga risker och ska analysera och övervaka riskutvecklingen, särskilt ska funktionen bevaka och rapportera framväxande risker. Funktionen ska i analysen väga in och bedöma all information eller rapporter som är relevanta för utvärderingen av riskprofil och riskhanteringssystem. Det innefattar information även från ekonomi-, aktuarie- och regelefterlevnadsfunktionerna. Riskhanteringsfunktionen ska särskilt samarbeta nära med aktuarien.

Riskhanteringsfunktionen ska även vara rådgivande till styrelse, VD och verksamheten i riskhanteringsfrågor inbegripet när det gäller utformning av strategi, förändringar i verksamhetens inriktning och vid beslut om större projekt eller investeringar. Riskhanteringsfunktionen ska vid behov föreslå förändringar i riskhanteringssystemet.

Funktionens uppdrag regleras av bolagets instruktion för riskhanteringsfunktionen och av styrelsen fastställd arbetsplan.

5.6 Aktuarie

Kontrollen av bolagets försäkringsrisker som kan beräknas med statistiska metoder (t.ex IBNR) ska utföras och rapporteras fortlöpande av bolagets aktuarie. Funktionens uppdrag regleras av de försäkringstekniska riktlinjerna, gällande uppdragsavtal och aktuarieinstruktion. Aktuarien lämnar information till riskhanteringsfunktionen om försäkringsrisker. Aktuarien uttalar sig även om kvalitén på den information som finns i bolagets IT-system och som används av aktuarien.

6 Riskhanteringssystemet

Riskhantering understryker behovet att förstå alla risker som kan påverka ett företag och därmed dess intressenter. Denna process syftar till att skapa en riskkultur som genomsyrar bolagets hela verksamhet. Avsikten är att de risker som tas ska vara medvetna och väl förstådda. En god riskhantering kan inte enbart baseras på matematiska modeller utan måste även innefatta nyfikenhet, kritisk analys och sunt förnuft.

Med risk menas i detta sammanhang en negativ variation från ett förväntat resultat. En risks storlek och omfattning beror på hur stora variationer som är möjliga, och hur stora sannolikheterna för dessa variationer är. Bolaget måste i många sammanhang ta eller acceptera risker för att uppnå vissa mål, men dessa risker får samtidigt inte vara så stora att de hotar bolagets övergripande måluppfyllelse.

Genom en välfungerande riskhanteringsprocess ska bolaget vid varje tillfälle vara i stånd att identifiera, värdera, övervaka, hantera och rapportera samtliga de risker som kan hindra bolaget från att uppnå sina verksamhetsmål eller efterleva gällande lagar och regler. De risker som tas är en följd av medvetna beslut, de är väl analyserade och bedöms inte hota verksamhetens mål.

Bolagets riskhanteringssystem består av följande huvudsakliga delar:

- Ett *kapitalmål* vilket anger bolagets målsättning i fråga om det eller de mest relevanta kapitaliseringsmåtten för bolaget. Kapitalmålet kompletterar riskaptiten per riskområde genom att ange bolagets övergripande riskaptit och -tolerans.
- En *riskhanteringsprocess* övergripande och för respektive riskområde eller delområde. Utformningen av riskhanteringsprocessen för enskilda områden varierar med områdets beskaffenhet.
- En *riskfilosofi* vilken utgör en bakgrund till riskhanteringssystemet. Riskfilosofin innefattar en konceptuell uppdelning av riskerna i riskgrupper och en kategorisering för bolagets inställning till enskilda riskområden som önskvärda, nödvändiga eller ej önskvärda
- En *riskaptit* vilken kompletterar bolagets inställning enligt riskfilosofin genom att, antingen kvalitativt eller kvantitativt, ange vilken tolerans bolaget har mot respektive riskområde eller delområde

6.1 Kapitalmålet

Kapitalmålet anger bolagets övergripande riskaptit och -tolerans och utgörs av en målsättning för bolagets kapitalisering i fråga om det eller de mest relevanta kapitaliseringsmåtten för bolaget. För respektive kapitaliseringsmått kan målnivåer anges som en lägsta tolererad nivå,

ett önskvärt intervall eller en kombination av dessa två. Kapitalmålet kan innefatta åtgärder om målet inte uppnås.

Kapitalmålet antas av styrelsen och anges i denna riktlinje.

6.2 Riskhanteringsprocessen

För varje riskområde ska en riskhanteringsprocess definieras. Den ska innefatta minst följande element:

1. Identifiering och beskrivning av risker
2. Riskvärdering inklusive definitioner av riskmått
3. Fastställande av riskaptit och toleransnivåer
4. Riktlinjer och rutiner för riskreducering
5. Rutiner för mätning och rapportering av riskexponering

Identifiering, värdering och fastställande av riskaptit utgör viktiga delar av bolagets strategiarbete och ska därmed även vara integrerade med den årliga verksamhetsplaneringen och med ORSA-processen (ORSA och scenarier regleras i bolagets Policy för ORSA). Riskhanteringssystemet ska täcka samtliga risker bolaget är exponerade mot, och omfatta både interna och externa processer. Analys av påverkan på riskexponeringen ska göras vid varje betydande förändring i verksamhetens processer, organisation eller inriktning (inklusive vid outsourcing).

Varje identifierad risk skall ha en *riskägare*, d.v.s. en person som är ansvarig för att övervaka riskens utveckling och kontrollera att beslutade åtgärder efterlevs. Bolaget ska föra ett *riskregister* som utgör en sammanställning av alla väsentliga riskgrupper och undergrupper, med angivande av vem som är riskägare, riskaptit, ytterligare risklimiter samt i vilka styrdokument relevanta element i riskhanteringssystemet framgår för respektive riskgrupp eller undergrupp.

Övergripande riktlinjer för ovan element i riskhanteringssystemet fastställs av styrelsen i detta eller andra styrdokument vilka kompletteras med rutiner och instruktioner inom bolaget. De mest betydande riskerna, aktuell nivå för dessa samt förändringen över tid ska regelbundet avrapporteras till styrelsen.

6.3 Riskfilosofin

Bolaget kategoriserar risker som *önskvärda*, *nödvändiga* eller *icke önskvärda*. Kategoriseringen följer på bolagets uppdrag och strategi.

Önskvärda risker är de risker som bolagets exponerar sig mot i direkt syfte att uppfylla bolagets uppdrag och leverera mervärde till ägarna tillika försäkringstagarna. Önskvärda risker ska hållas på en medveten och kontrollerad nivå så att bolagets värdeskapande maximeras utan att åtagandena mot försäkringstagarna äventyras.

Nödvändiga risker är risker som inte direkt bidrar till bolagets värdeskapande men som inte kan undvikas vid bedrivandet av verksamheten. Nödvändiga risker ska hållas på en begränsad nivå och reduceras i den mån det är kostnadseffektivt.

Ej önskvärda risker är risker vars negativa påverkan på bolagets möjligheter till värdeskapande överskrider värdet av att tillåta exponering mot sådana risker. Ej önskvärda risker ska om möjligt undvikas. Identifierade exponeringar mot sådana risker ska minimeras.

S:t Erik Försäkrings risker delas in i följande huvudgrupper

- Försäkringsrisker
- Finansiella risker
- Operativa risker
- Affärsrisker

Definitioner och ytterligare indelning i undergrupper samt bolagets inställning och aptit redogörs för per riskgrupp nedan. I denna riktlinje anges även övriga element i riskhanteringssystemet för affärsrisker och operativa risker, medan det för försäkrings-respektive finansiella risker hänvisas till andra styrdokument (försäkringstekniska riktlinjer respektive finanspolicy).

6.4 Riskaptiten

Riskaptiten utgörs av en beskrivning av risknivåer som bolaget är villigt att exponera sig mot i syfte att nå sina affärsmål, per riskgrupp eller undergrupp. Aptiten ska uttryckas i form av en övergripande inställning till risken i en kvalitativ skala (låg – måttlig – hög) och om möjligt även kvantitativt i form av de mest centrala toleransnivåerna. Riskaptiten kan vid behov kompletteras med detaljerade limiter för berörda riskgrupper, sådana limiter är dock inte en del av riskaptiten i sig utan snarare av riskhanteringsprocessen.

Styrelsen antar i dessa riktlinjer en riskaptit i form av bolagets övergripande risktoleranser vid sidan av kapitalmålet. Riskaptiten ska uttryckas för varje väsentlig riskgrupp eller undergrupp.

7 Kapitalmålet

S:t Erik Försäkrings kapitalmål och tillika samlade risktolerans är att solvenskapitalkvoten (SCR-kvoten) inte bör understiga 150%. Om SCR-kvoten går under 150% så ska styrelsen utan dröjsmål besluta om nödvändiga åtgärder för att återställa SCR-kvoten till minst 150% inom ett år.

8 Försäkringsrisker

Försäkringsrisk (teckningsrisker) innebär att kostnaden för inträffade försäkringsfall blir större än förväntat.

8.1 Indelning av försäkringsrisk

De undergrupper inom försäkringsrisk som är aktuella för bolaget är reservrisk, premierisk och katastrofrisk inom skadeförsäkring:

- Premierisk är risken att premierna är otillräckliga för att täcka framtida skador inom tecknade försäkringar, exempelvis kan förluster uppstå genom att frekvens eller genomsnittlig skada blir högre än estimerat.
- Reservsättningsrisk är risk för kostnader för redan inträffade skador blir högre än vad som reservsatts, oavsett om det gäller rapporterade eller ännu ej rapporterade skador.
- Katastrofrisk är risk för förluster till följd av beror på extrema eller oregelbundna händelser, exempelvis naturkatastrofer, epidemier, extrema väderförhållanden eller katastrofer orsakade av mänskliga aktiviteter.

8.2 Kategorisering av försäkringsrisk

Bolaget anser att skadeförsäkringsrisker i form av premierisk, reservrisk och katastrofrisk inom ramen bolagets uppdrag är önskvärda risker. Andra försäkringsrisker är ej önskvärda risker och ska inte förekomma.

Bolaget använder sig återförsäkring och avger försäkringsrisker till återförsäkringsmotparter. Bolaget tar dock inte emot återförsäkring, försäkringsrisker från indirekt försäkring är ej önskvärda och ska ej förekomma.

8.3 Riskaptit för försäkringsrisk

Bolagets aptit för försäkringsrisk uttrycks efter beaktande av avgiven återförsäkring, det vill säga netto (för egen räkning). Motpartsrisker från avgiven återförsäkring behandlas finansiella risker.

Bolagets aptit för de önskvärda försäkringsriskerna netto är stor. Kapitalmålet enbart sätter en den övre gränsen för risktoleransen för försäkringsrisker. Processen för hantering av försäkringsrisker, bland annat i fråga om villkorsutformning, premiesättning och val av självbehåll i återförsäkringen, ska utformas så att riskerna hålls på en medveten och kontrollerad nivå. Ytterligare limiter för försäkringsrisker anges i *Instruktion för tecknings- och återförsäkringsrisker.*

8.4 Riskhanteringsprocess för försäkringsrisk

Riskhanteringsprocessen för försäkringsrisker ska närmare beskrivas i S:t Erik Försäkrings *Försäkringstekniska riktlinjer, Instruktion för tecknings- och återförsäkringsrisker* samt *Instruktion för hantering av reservsättningsrisker.*

9 Finansiella risker

Finansiella risker består av risken för förluster från likviditets-, marknads- och motpartsrisker inklusive bristande matchning mellan tillgångar och skulder samt koncentrationsrisker.

För motpartsrisker från avgiven återförsäkring anges processen för hantering i *Instruktion för tecknings- och återförsäkringsrisker.* För övriga finansiella risker, i de fall de överhuvudtaget får förekomma, anges processen för hanteringen i *Placeringsriktlinjer*. De metoder för hantering, inklusive limiter, som anges i de styrdokumenten ska reflektera den inställning och aptit som uttrycks här.

9.1 Likviditetsrisker

Likviditetsrisk avser risken att egna betalningsåtaganden inte kan fullgöras på grund av brist på likvida medel.

Likviditetsrisk är en nödvändig risk för bolaget, men då den värdeskapande effekten att ta likviditetsrisk är liten är också bolagets riskaptit låg.

9.2 Marknadsrisker

Marknadsrisk avser risken för förluster som direkt eller indirekt orsakas av ändringar, i nivå eller volatilitet, i marknadspriser för tillgångar, skulder och finansiella instrument inklusive förluster orsakade av brister i matchningen mellan tillgångar och skulder. Den enda typ av marknadsrisk som bolaget inte undviker helt är *Ränterisk* vilket avser risken för förluster till följd av ändringar av marknadsräntor.

Bolaget placeringstillgångar ska uteslutande vara placerade på koncernkonto hos Stockholms stad. Riskerna från dessa hänförs till motpartsrisker. Valutarisker är ej önskvärda och ska undvikas genom att belopp för tecknade försäkringar, avgiven återförsäkring och placeringstillgångar uteslutande ska vara uttryckta i SEK.

Marknadsrisk i form av ränterisk är en nödvändig risk, och uppstår främst från omvärderingseffekter vid ränteförändringar på tillgångar och försäkringstekniska avsättningar. För ränterisk har bolaget en låg aptit, men accepterar risken upp till den nivå som resulterar från att tillgångarna uteslutande hålls till rörlig ränta. Risker från längre räntebindningstider i tillgångar än i skulder är ej önskvärda.

9.3 Motpartsrisker

Motpartsrisker avser risken för förluster till följd av att motparter inte fullgör sina åtaganden och att eventuella säkerheter inte täcker fordran. Följande typer av motpartsrisk skulle kunna vara aktuella för bolaget:

- Motpartsrisk i finansiella derivat avser risken för förluster till följd av att motparter i finansiella derivat inte fullgör sina åtaganden och att eventuella säkerheter inte täcker fordran.
- Motpartsrisk i avgiven återförsäkring avser risken för förluster till följd av att återförsäkringsgivare inte fullgör sina åtaganden och att eventuella säker-heter inte täcker fordran.
- Motpartsrisk i mottagen försäkring, från premiefordringar eller återkrav samt klientmedelskonton avser risken att kunder och leverantörer inom försäkringsrörelsen inte fullgör sina åtaganden
- Kreditrisk i finansiella tillgångar, från utlåning, insättningar och obligationer avser risken för förluster för att motparten inte fullgör sina åtaganden

Motpartsrisk från finansiella derivat ska inte förekomma.

Motpartsrisk i avgiven återförsäkring uppstår som en naturlig följd av bolagets uppdrag. Dessa är därför önskvärda i fråga om beloppens storlek, men snarare nödvändig i fråga om motparternas kreditvärdighet. Bolaget har en hög aptit för beloppen där kapitalmålet enbart sätter en den övre gränsen för risktoleransen, men där aptiten för motparternas bidrag är måttlig. I den aspekten ska riskerna begränsas genom att endast motparter med god kreditvärdighet ska vara aktuella och att utestående fordringar avtalsmässigt ska kunna regleras utan onödigt dröjsmål.

Motpartsrisk i mottagen försäkring är en nödvändig risk, riskaptiten är låg. Riskerna ska hållas på en mycket begränsad nivå genom att premier begärs in i förskott, att leverantörer med god betalnings- och leveransförmåga väljs och att klientmedlen hålls begränsade.

Kreditrisk i finansiella tillgångar är en ej önskvärd risk som ska undvikas så långt det är möjligt. Medel på koncernkonto hos Stockholms stad anses ej bidra till riskens storlek, och utgör den enda tillåtna formen av placeringstillgång för bolaget. Om det av driftsskäl inte kan undvikas att medel hålls på bankkonto kan det accepteras under förutsättning att kontobehållningen inte överstiger det nödvändiga.

9.4 Koncentrationsrisker

Koncentrationsrisker avser risken att en enskild exponering, en grupp av likartade exponeringar eller en specifik händelse leder till förluster i större utsträckning än om verksamheten vore väl diversifierad.

Koncentrationsrisker inom tecknad försäkring utgör inte en egen undergrupp inom bolagets riskhanteringssystem utan ingår i försäkringsriskerna netto.

Koncentrationsrisker inom placeringstillgångarna anses inte föreligga utifrån bolagets syn på Stockholms stad.

Koncentrationsrisker inom motpartsexponeringarna från avgiven återförsäkring är en nödvändig risk. Bolaget anger inte någon specifik aptit eller övre toleransnivå för denna risk utan accepterar den inom motpartsriskerna i syfte att underlätta upphandlingsförfarandet för återförsäkring och minimera kostnaden för densamma.

10 Operativ risk

Med operativ risk avses risken för förluster till följd av icke ändamålsenliga eller fallerade processer, människor, system eller yttre händelser, inbegripet legala risker och compliancerisker.

10.1 Indelning av operativa risker

De former av operativ risk som är aktuella för bolaget är produkt- och processrisker, personalrisker, legala risker, IT-risker och säkerhetsrisker:

- *Produkt och processrisker* avser risken för förluster till följd av att fastställda arbetsprocesser inte fungerar, inte är kända eller är icke-ändamålsenliga. Risktypen kan exempelvis utmynna i fel i hanteringen av produkter, transaktioner eller rapportering.
- *Personalrisker* avser risken för förluster till följd av otydlighet i ansvarsområde, otillräcklig kompetens i förhållande till arbetsuppgift eller att det inte finns tillräckligt med personal i förhållande till arbetsuppgifterna. Andra risker kan innebära intressekonflikt för personalen samt avsteg från lagstadgad tystnadsplikt. Risktypen kan exempelvis utmynna i att arbetsuppgifter inte kan utföras på ett korrekt sätt eller tidsenligt.
- *Säkerhetsrisker* avser risken för förluster till följd av att företaget utsätts för externa brott eller interna oegentligheter. Risktypen kan exempelvis utmynna i ekonomiska förluster eller varumärkesrisker.
- *IT-risker* avser risken för förluster till följd av IT-system inte är tillgängliga i beslutad omfattning eller inte är tillräckligt säkra. Risktypen kan exempelvis utmynna i att kunduppdrag inte kan utföras eller att information blir tillgänglig för obehöriga.
- *Legala risker och Compliancerisker* avser risken att bolaget inte efterlever lagar, förordningar samt föreskrifter, allmänna råd från FI och europeiska myndigheter eller andra relevanta regleringar och rekommendationer för den tillståndspliktiga verksamheten samt inte efterlever interna regler, god sed eller god standard för den tillståndspliktiga verksamheten och därigenom utsätts för risken att drabbas av sanktioner eller andra påpekanden från myndigheter, negativ publicitet i media och/eller ett minskat förtroende från kunder eller övriga intressenter

10.2 Kategorisering av operativa risker

Operativ risk kan aldrig till fullo kan undvikas och ofta är kostnaden för ytterligare reducering betydande. Operativa risker är som huvudregel att betrakta som nödvändiga risker.

Följande operativa risker är dock ej önskvärda:

- Säkerhetsrisker
- Personalrisker relaterade till hälsa och personlig integritet
- Produkt- och produktrisker med risk för skadereglering till nackdel för fysiska personer
- IT-risker relaterade till personlig integritet
- Compliancerisker relaterade till bolagets tillstånd att bedriva verksamhet

10.3 Riskaptit för operativ risk

Bolaget har en låg aptit för ovan ej önskvärda operativa risker. För sådana risker ska interna processer utformas i syfte att minimera dem.

För övriga operativa risker har bolaget en måttlig aptit, där kostnaden för bolaget om risken materialiseras ska beaktas vid val av åtgärder för att reducera risken. Under alla omständigheter ska dock riskerna hållas på en begränsad nivå.

10.4 Riskhanteringsprocess för operativ risk

Operativa risker ska identifieras genom att riskanalyser genomförs inom alla verksamhetsområden. Riskanalyser ska genomföras vid väsentligt förändrad verksamhet och annars minst vartannat år. De identifierade specifika operativa riskerna kompletterar riskregistret.

Identifierade risker ska värderas i fråga om (i) sannolikheten att en händelse inträffar och (ii) konsekvensen om den inträffar. Sannolikhet respektive konsekvens kan värderas enligt kvalitativ skala (ex. låg-medel-hög) eller kvantitativ skala (procent resp. kronor i kostnad) beroende på vad som är lämpligt. För risker som till sin storlek överstiger riskaptiten ska åtgärder vidtas.

Följande typer av åtgärder kan vara aktuella för att reducera operativa risker, ensamt eller i kombination:

- Införa dokumenterad kontroll
- Införa dokumenterat krav på dualitet
- Genomföra utbildning
- Förändra process, riktlinje eller rutinbeskrivning
- Ökade resurser

Bolagets riskhanteringsfunktion ska delta i riskanalyserna och kontrollera identifiering och bedömning av risker som utförs av verksamheten.

Bolagets största operativa risker med tillhörande åtgärdsplaner och deras status ska rapporteras till styrelsen.

11 Affärsrisker

Affärsrisker är risker för förluster till följd av effekter av strategiska beslut, en sämre intjäning eller rykten.

11.1 Indelning av affärsrisker

Affärsrisker indelas enligt följande:

- Strategisk risk är risken för förluster till följd av affärsstrategier och affärsbeslut som visar sig vara missriktade, omvärldsförändringar och institutionella förändringar
- Intjäningsrisk är risken för förluster till följd av en oväntad nedgång i intäkter från exempelvis volymminskningar eller från en oväntad ökning av kostnader från exempelvis svag arbetsproduktivitet
- Ryktesrisk är risken för förlorat anseende hos kunder, ägare, anställda, myndigheter etc., vilket kan leda till minskade intäkter och ett försämrat värde av varumärket

11.2 Kategorisering av affärsrisker

Bolagets uppdrag innefattar att hantera affärsrisker relaterade till att tillhandahålla försäkringslösningar för kommunkoncernens räkning. Affärsrisker är därför önskvärda risker.

11.3 Aptit för affärsrisker

Bolagets aptit för affärsrisker är måttlig. Processen för att hantera riskerna ska säkerställa att de hålls på en begränsad nivå.

11.4 Riskhanteringsprocess för affärsrisker

Affärsrisker ska identifieras genom att riskanalys genomförs inom ORSA- och affärsplaneringsprocessen och vid strategiska förändringar av verksamheten. De identifierade specifika affärsriskerna kompletterar riskregistret. Styrelsen ska vara delaktig i att kvalitetssäkra riskanalysen.

Identifierade risker ska värderas i fråga om (i) sannolikheten att en händelse inträffar och (ii) konsekvensen om den inträffar. Sannolikhet respektive konsekvens kan värderas enligt kvalitativ skala (ex. låg-medel-hög) eller kvantitativ skala (procent resp. kronor i kostnad) beroende på vad som är lämpligt.

Ett centralt moment i identifiering av affärsriskerna är en god omvärldsanalys, den viktigaste åtgärden för att kunna reducera enskilda risker är att upprätthålla en förmåga att anpassa bolaget till förändringar i förutsättningarna att bedriva verksamhet. För risker som till sin storlek överstiger riskaptiten ska åtgärder medtas i affärsplanen och genomföras i verkställandet av denna.

För de affärsrisker som bedömts nödvändiga att hantera ska avrapporteringen av status för åtgärdsplanerna ingå i den löpande rapporteringen från Vd till styrelsen.

S:T ERIK FÖRSÄKRINGS AB:S RIKTLINJER FÖR SKADE-REGLERING, REGRESSHANTERING OCH UTREDNING VID MISSTANKE OM FÖRSÄKRINGSBEDRÄGERI I

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna har fastställts av styrelsen för S:t Erik Försäkrings AB och skall revideras årligen.

Ansvarig för revidering av dessa riktlinjer är VD.

Nedan angivna riktlinjer skall följas av bolagets anställda och uppdragstagare.

2 Skadereglering

Riktlinjerna anger vad som skall iakttas vid varje skadetyp.

2.1 Aktiv service

Försäkringsbolaget skall lämna aktiv service och utredningen skall utföras så snabbt som möjligt.

2.2 Råd och anvisningar

Råd och anvisningar skall lämnas om vilka åtgärder som skall vidtagas för att begränsa en skadas verkningar.

2.3 Information om åtgärder och beslut

Kunden skall på ett enkelt och lättfattligt sätt informeras om sina rättigheter och skyldigheter samt om bolagets åtgärder och beslut

2.4 Fullständig utredning

Bolaget skall i samarbete med kunden tillse att utredningen blir så fullständig som möjligt.

2.5 Information om fördröjning

Om ett skadeärende fördröjs är det viktigt att upplysa kunden om anledningen. Beror dröjsmålet på kunden, skall han informeras om att den fortsatta handläggningen är beroende av hans åtgärder.

2.6 Lyhördhet och sekretess

Handläggningen skall ske smidigt och med lyhördhet för kundens individuella förhållanden.

Gällande sekretessbestämmelser skall iakttas.

2.7 Bolag skall komma överens

Om flera försäkringsbolag berörs av samma skada, skall bolagen komma överens om handläggningen så att skaderegleringen inte fördröjs

2.8 Konsekvent skadereglering

Skaderegleringen skall vara konsekvent, enhetlig och rättvis.

2.9 Rätt ersättning

Ersättningen skall bestämmas med tillämpning av försäkringsavtalets bestämmelser, skaderegleringspraxis och gällande rättsregler.

Kunden skall ha den ersättning han är berättigad till, även om han på grund av otillräckliga kunskaper om ersättningsregler eller av andra skäl begär mindre.

2.10 Försäkringskollektivets intressen

Om det finns anledning anta att kunden inte agerar korrekt skall bolaget sträva efter att skydda samtliga försäkringstagares intressen.

2.11 Beslut

Beslut skall motiveras.

2.12 Hot och påtryckningar

Det är nödvändigt att inta en fast hållning mot hot och otillbörliga påtryckningar

2.13 Felbedömningar

Om det visar sig att ett ärende blivit felbedömt, skall kunden omedelbart informeras härom och ändring ske snarast.

2.14 Information om prövning av beslut

Om ersättning inte lämnas eller om den reduceras, skall bolaget lämna kunden upplysning om de möjligheter till prövning av bolagets beslut som finns.

3 Regress

Enligt kommunallagen, som gäller båda för de kommunala förvaltningarna och bolagen, får kommuner ha hand om sådana angelägenheter av allmänt intresse som har anknytning till kommunens område eller deras medlemmar och som inte skall handhas av någon annan. En kommun får således inte gynna enskilda utan särskilt lagstöd. I detta ligger också att en kommun eller ett kommunalt bolag inte får efterge en rätt som man har.

Om S:t Erik Försäkring, efter en noggrann juridisk analys, kommer fram till att bolaget har en fordran på en enskild som t ex har förorsakat en brand i en byggnad eller vållat en vattenskada, är bolaget skyldigt att kräva in denna fordran. Om så erfordras måste bolaget väcka tala vid domstol för att driva in sin fordran.

I bedömningen om kravet skall drivas mot enskild bör även beaktas vad som anges i reglerna om ekonomisk förvaltning: ”Indrivning av en fordran får avbrytas om ytterligare indrivningsförsök är utsiktslösa eller inte är försvarliga med hänsyn till kostnaderna och inte krävs från allmän synpunkt.”

Återkrav av utgiven ersättning skall ske från den som är ansvarig för skadan och vid dubbelförsäkring (där en och samma risk är försäkrad hos två eller flera bolag) hos det eller de bolag där försäkring finns för den aktuella risken.

4 Misstanke om försäkringsbedrägeri m m

Försäkringsidén bygger på ett ömsesidigt förtroende mellan försäkringstagaren och försäkringsbolaget, där bolaget vid skaderegleringen bör kunna utgå från att försäkringstagarens uppgifter är riktiga.

Bolaget skall beakta försäkringstagarkollektivets intresse av att inte en enskild försäkrad gynnas otillbörligt.

Målet för bolagets utredning är att skaffa ett tillräckligt underlag för beslut i ersättningsfrågan. Det ska dock understrykas att det inte ankommer på försäkringsbolagen att utreda och beivra brott. Ansvaret för detta ligger på polis och åklagare.

Förevarande riktlinjer anger hur utredningar inom bolaget skall gå till. De är tillämpliga på utredning av skador inom samtliga försäkringstyper. Riktlinjerna ska vara en garanti för att försäkringstagare inte utsätts för misstankar om brott på felaktiga grunder. De ska även säkerställa att bolaget inte betalar ut ersättning till följd av felaktiga uppgifter från den försäkrade.

I den mån bolaget uppdrar åt någon utomstående att fullgöra viss utredningsverksamhet, åligger det bolaget att säkerställa att riktlinjerna tillämpas även i detta fall.

4.1 Utredning

Vid misstanke om oriktiga krav eller bedrägeri beslutar VD om en särskild utredning ska göras för att få misstanken undanröjd eller bekräftad. VD beslutar även vem som skall utföra utredningen. Utredningens syfte är att skapa ett underlag för ett riktigt beslut i ersättnings-frågan.

Den försäkrade bör snarast underrättas när utredning görs i syfte att skapa klarhet i ersättningsfrågan om sådan underrättelse inte kan antas vara till men för utredningen. Bolaget bör också ge den försäkrade möjlighet att förklara oklara omständigheter.

4.2 Resultat av utredningen

Utredningen kan i princip ge följande tre resultat:

1. Stöd för misstanke om brott föreligger inte. Skadeärendet regleras i normal ordning.

2. Försäkringsfall är inte visat eller ersättningsbart försäkringsfall föreligger inte, men tillräckligt underlag för en polisanmälan saknas. Ersättning utbetalas inte och den försäkrade erinras om sin rätt att få ärendet prövat vid allmän domstol.

3. Stöd för misstanke om försäkringsbedrägeri eller försök därtill föreligger. Ersättning utbetalas inte och ev polisanmälan görs.

Om bolagets beslut innebär att den försäkrade inte får någon ersättning eller endast en del av begärd ersättning, ska denne så snart som möjligt skriftligen meddelas bolagets slutliga ställningstagande. Skälen till bolagets beslut ska härvid redovisas samt även resultatet av utredningen i lämplig sammanfattning. Det ska stå klart för den försäkrade varför bolaget inte betalar.

Det kan finnas skäl att inte lämna ut hela utredningsmaterialet, t ex om polisutredning pågår eller av hänsyn till enskild uppgiftslämnare.

Det bör av bolagets information framgå att beslutet är slutligt samt att den försäkrade har rätt att få ärendet prövat vid allmän domstol genom att väcka talan mot försäkringsbolaget.

4.3 Sekretess

Utredningen tillförs ofta material som innehåller känsliga och förtroliga uppgifter angående såväl den försäkrade som andra personer vilka berörs av utredningen. Detta material ska omfattas av hög sekretess och hanteras med stor varsamhet.

Bolaget skall vid varje tillfälle beakta gällande offentlighets- och sekretesslagstiftning. Vid tveksamhet skall Stockholms stads juridiska avdelning konsulteras.

4.4 Kontakt med polis och åklagare

Polisanmälan sker genom beslut av VD i samråd med Stockholms stads juridiska avdelning.

RIKTLINJER FÖR UPPDRAGSAVTAL I S:T ERIK FÖRSÄKRING AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

INNEHÅLLSFÖRTECKNING

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler” och har fastställts av styrelsen för S:t Erik Försäkring AB.

Riktlinjerna är föremål för revidering och skall fastställas årligen av styrelsen.

2 Syftet med riktlinjerna

Riktlinjerna har till syfte att reglera vilken typ av verksamhet i bolaget som får läggas ut på uppdragsavtal samt under vilka förutsättningar detta får ske.

Ett uppdragsavtal får inte avse operativ verksamhet eller funktioner som är av väsentlig betydelse, om det kan leda till att:

- kvaliteten i företagsstyrningssystemet försämras väsentligt,
- den operativa risken i företaget ökar väsentligt,
- Finansinspektionens möjlighet att utöva tillsyn försämras, eller,
- försäkringstagarnas möjlighet till tillfredsställande och fortlöpande service inte kan upprätthållas.

3 Ansvarsfördelning

Styrelsen ansvarar ytterst för den verksamhet som utförs på uppdragsavtal.

Styrelsen ska fastställa huruvida en funktion eller aktivitet är kritisk eller viktig för företagets verksamhet och godkänna att sådan verksamhet får utföras genom uppdragsavtal. Beslutet skall föregås av en riskanalys enligt kap 5.

För uppdragsavtal avseende molntjänster ska EIOPA:s Riktlinjer om uppdragsavtal med molntjänstleverantörer (EIOPA 20-002) riktlinje 1 och 2 beaktas.

VD ansvarar för:

- att bolaget utövar sitt beställaransvar genom att på bolaget utse en ansvarig för den utlagda verksamheten och att ansvarig har tillräckliga kunskaper för att kunna leda och kontrollera tjänsteleverantören. Kraven på ansvarig person framgår av bolagets Riktlinjer för lämplighet av styrelse, ledning och nyckelfunktioner.
- att minimikraven för outsourcing i kap 7 är uppfyllda,
- att styrelsen tillställs en riskanalys inför beslut om outsourcing avseende kritiska eller viktiga funktioner,
- att avtal upprättas med extern part i enlighet med LOU (avtal mellan S:t Erik Försäkring och S:t Erik Livförsäkring upprättas av styrelsen i enlighet med gällande firmateckningsrätt)
- att uppföljning sker av den verksamhet som utförs på uppdragsavtal

- att de som utför verksamheten på uppdragsavtal får del av och följer de riktlinjer och policys som antagits av styrelsen

- att godkänna upphandlingsunderlaget och tillställa detta till styrelsen för godkännande avseende kritiska eller viktiga funktioner

- att årligen rapportera utfallet (kontraktsuppföljning) av outsourcad verksamhet till styrelsen.

- att Finansinspektionen informeras om planerad eller förändrad outsourcing och ansvarig person

Av VD delegerad ansvarig person för den outsourcade verksamheten skall, med hänsyn till verksamhetens art och omfattning, löpande, följa upp uppdragstagarens arbete och ska minst årligen genomföra en dokumenterad utvärdering av verksamheten och rapportera den till VD.

Riskhanteringsfunktionen ansvarar för att på verksamhetens begäran bistå verksamheten i riskanalys vid kritiska eller viktiga funktioner.

Regelefterlevnadsfunktionen ansvarar för att på verksamhetens begäran bistå verksamheten i bedömningen av om ett uppdragsavtal, avseende kritiska eller viktiga, funktioner följer gällande regelverk eller inte.

Informationssäkerhetssamordnaren ansvarar för att på verksamhetens begäran bistå verksamheten i bedömningen av om ett uppdragsavtal, särskilt avseende IT system eller molntjänster, följer regelverket för informationssäkerhet och de krav eller åtgärder som erfordras.

4 Kritiska eller viktiga operativa funktioner och aktiviteter

En funktion eller aktivitet anses vara kritisk eller viktig om den är nödvändig för att bolaget ska kunna tillhandahålla tjänster i bolagets kärnverksamhet åt försäkringstagarna.

Vid en bedömning av om en funktion är kritisk eller viktig kan ledning hämtas från EBA:s riktlinje GL/2019/02.

För uppdragsavtal avseende molntjänster bör ledning hämtas från EIOPAS Riktlinjer om uppdragsavtal med molnleverantör (EIOPA 20-002) riktlinje 7.

Styrelsen har identifierat följande funktioner och aktiviteter som kritiska:

- VD

- aktuariella tjänster,

- IT

- oberoende granskare

- regelefterlevnad
- skadereglering
- försäkringshantering
- riskhantering
- ekonomi

5 Riskanalys

Riskanalys skall genomföras av bolaget och, avseende kritiska eller viktiga funktioner, vara ett underlag för styrelsens beslut om outsourcing. Vid förnyad outsourcing ska ny riskanalys genomföras om riskerna har ändrats.

Riskanalysen ska innehålla en beskrivning av:

- funktionen eller aktiviteten som uppdragsavtalet avser,
- beställaransvarig och erforderlig kompetens,
- hur minimikraven nedan säkerställs
- beredskapsplan för att avsluta uppdragsavtalet (skrivs in i bolagets krisplan),
- risken att minimikraven inte uppnås

Riskanalys utförs i enlighet med bilaga 1. För uppdragsavtal avseende molntjänster av kritiskt eller viktig funktion ska även EIOPA 20-002 riktlinje 8 och 9 beaktas.

6 Verksamheter som idag bedrivs på uppdragsavtal

Verksamhet som idag bedrivs på uppdragsavtal är:

- aktuariella tjänster,
- IT
-
- internrevision
- regelefterlevnadsfunktionen
- riskhanteringsfunktionen
- skadereglering
- ekonomi

7 Minimikrav som ska vara uppfyllda för att verksamhet ska få bedrivas av extern part genom uppdragsavtal

För att en verksamhet ska få läggas ut på uppdragsavtal krävs det att:

- tillräcklig beställarkompetens finns inom bolaget för att kunna upphandla och kontrollera den utlagda verksamheten,
- leverantören är ”fit” genom att ha tillräcklig kompetens för att långsiktigt utföra uppdraget med god kvalitet och med väl fungerande internkontroll,
- leverantören är ”proper” genom att kraven på lämplighet i LOU uppfylls,
- bolaget kan styra, följa upp och revidera uppdraget i tillräcklig omfattning,
- det kan säkerställas att gällande sekretesskydd kan vidmakthållas och regler avseende personuppgifter kan följas,
- bolaget och leverantören upprättar och vidmakthåller en beredskapsplan för den aktuella verksamheten i syfte att om möjligt mildra effekterna av oförutsedda händelser, övergång av verksamheten till annan leverantör eller bolaget,
- Finansinspektionens möjlighet att bedriva tillsyn av den aktuella verksamheten vidmakthålls och att uppdragstagaren samarbetar med Finansinspektionen gällande de funktioner eller verksamhet som omfattas av uppdragsavtalet samt på begäran ger Finansinspektionen faktiskt tillträde till dess lokaler,
- bolaget fortsatt kan tillgodose samtliga sina skyldigheter mot sina intressenter inklusive Finansinspektionen och samtliga kunder,
- uppdragstagaren ger försäkringsföretaget, dess revisorer och Finansinspektionen tillgång till uppgifter som rör de funktioner eller verksamhet som omfattas av uppdragsavtalet
- frågor kring jäv och intressekonflikter identifieras och utreds,
- att reglerna om offentlig upphandling följs,
- att gällande rätt följs i övrigt,
- den utlagda verksamheten regleras i ett skriftligt avtal där parternas samtliga rättigheter och skyldigheter regleras,
- kvaliteten i bolagets försäkringsstyrningssystem inte försämras väsentligt,
- den operativa risken i bolaget inte ökar väsentligt,
- försäkringstagarnas möjlighet till tillfredsställande och fortlöpande service kan upprätthållas

- verksamhetens övriga riktlinjer kan följas, särskilt avseende informationssäkerhet och personuppgifter

- För molntjänster av ska även EIOPA 20-002 riktlinje 2,6, 12 och 15 beaktas.

8 Uppdragsavtalets innehåll

I avtal med extern part skall nedanstående punkter regleras. För molntjänster ska även EIOAP 20-002 riktlinje 10-13 och 15 beaktas.

- krav på tjänsten/varan – omfattning

- krav på leverantörens kompetens, kvalité och internkontroll

- avtalsperiod

- kontaktperson hos leverantören som är ansvarig för uppdraget

- partsoberoende (intressekonflikter)- riktlinjer avseende jäv och intressekonflikter och hur dessa kontrolleras

- riktlinjer för styrning, uppföljning och revidering av uppdraget

- ersättning, mervärdesskatt, prisjustering, fakturering och betalningsvillkor

- skatter och avgifter

- underleverantörer
    - samma ansvar som leverantören
    - efter Beställarens godkännande/anmälan till Beställaren

- personal - kompetens, förändringar

- marknadsföring

- rättigheter till material

- rättsintrång

- fel

- försening och brister i tillgänglighet

- sekretess

- information mellan parterna (inkluderar även att bolaget ska kunna ta del av leverantörens resultat om det är väsentligt för bolaget att få uppgift om detta)

- ansvar mellan parterna

- försäkring
- säkerhet
- force majeure
- ändringar och tillägg
- överlåtelse av avtal, rättigheter och skyldigheter
- uppsägning
- tillämplig lag och tvistefora
- leverantören ska följa bolagets riktlinjer och policys
- personuppgifter
- särskilda kontraktsvillkor, bl a. antidiskrimineringsklausul
- beredskapsplan för oförutsedda händelser och återgång av verksamheten
- leverantörens medverkan vid upphandling och återgång och behjälplighet med eventuell överföring av uppdraget och uppgifter till en ny leverantör
- möjlighet för Beställaren och Finansinspektionen att bedriva tillsyn av den outsourcade verksamheten (detta inkluderar också att Beställarens interna och externa revisorer får tillgång till uppgifter om den utlagda verksamheten)

9 Uppföljning

Uppföljning av uppdragsavtal sker riskbaserat utifrån bolagets Instruktion för kontraktsuppföljning.

För molntjänster ska även EIOPA 20-002 riktlinje 11 och 14 beaktas.

10 Anmälan till Finansinspektionen

VD eller delegerad ansvarar för att anmälan till Finansinspektionen sker av:

- Ansvarig för verksamheten/funktionen på företaget
- Verksamhet som avser operativ verksamhet eller funktioner av väsentlig betydelse ska anmälas in innan avtalet börjar gälla samt snarast vid förändringar av densamma.

Vid uppdragsavtal som avser väsentliga funktioner ska en ansvarig för funktionen på företaget utses av VD och anmälas till Finansinspektionen.

För molntjänster ska EIOPA 20-002 riktlinje 4 beaktas.

11 Dokumentation

Upphandling och dokumentation sker i bolagets upphandlings/avtalssystem samt under G/2.4 i bolagets databas beroende på typ av avtal.

För molntjänster ska även dokumentation enligt EIOPA 20-002 riktlinje 5 beaktas i tillämpliga delar.

Bilaga 1 – Riskanalys outsourcing, (ex)

Avtal:

Intern/extern outsourcing:

1. Är syftet med outsourcingen att minimera system och/eller personalkostnader och införa en mer effektiv verksamhet?

2. Kan företaget försäkra att aktiviteterna som genomförs av en tredje part (Uppdragstagare) utförs under övervakade och säkra omständigheter?

3. Är det säkert att den externa uppdraget inte leder till en materiellt lägre kvalitet av företagets internkontroll eller FI:s möjlighet att övervaka företagets regelefterlevnad?

4. Om avtalet är mellan företag i gruppen: har frågor om intressekonflikter blivit speciellt belysta?

5. Är rättigheterna och skyldigheterna för det egna bolaget och Uppdragstagare dokumenterade i ett skriftligt avtal?

6. Finns det ett SLA-kontrakt (Service Level Agreement) eller motsvarande?

7. Specificerar avtalet att om uppdragstagaren skulle delegera till en annan aktör att utföra delar av det avtalade uppdraget så skall den detta uppdrag också innefattas av samma villkor och regler som det ursprungliga avtalet?

8. Specificerar avtalet alla aktörer som genomför uppdraget inte får vidarebefordra uppdraget till en annan aktör utan att detta har blivit skriftligt godkänt av företaget?

9. I de fall som uppdragsavtalet är relaterat till genomförandet av aktiviteter som avser tillståndspliktig verksamhet, ska det godkännas genom VD, avdelningschef eller företagschef. Är det så med aktuellt uppdrag?

10. Innehåller SLA-kontraktet villkor som säkrar att serviceavtalet kan avslutas utan att det påverkar kontinuiteten och kvaliteten på uppdraget som tillhandahålls till företagets kunder?

11. Säkerhetställer SLA-villkoren att uppdragstagaren sammarbetar med Finansinspektionen i relation till den outsourcade verksamheten?

12. Säkerhetsäller SLA-villkoren att uppdragstagaren har en lämplig kontinuitetsplan (BCP)?

13. Säkerhetställer SLA-villkoren att företaget dess revisorer, och FI ska ha aktuell och omdelbar tillgång till information som rör företagsaktiviter som är outsourcade och tillgång till lokalerna till uppdragstagaren?

14. Innehåller SLA-villkoren metoder som ska etableras för att bedöma hur väl uppdragstagaren genomför sina åtaganden?

15. Innehåller SLA-villkoren det som behövs för att ändamålsenliga åtgärder vidtas om uppdragstagaren misslyckas med att genomföra uppdraget effektivt och bryter mot regelefterlevnaden?

16. Finns det en utnämnd en ansvarig person (i de flesta fall områdeschef eller motsvarande) för uppdraget/avtalet. Har den ansvariga personen den nödvändiga kunskapen som behövs för effektivt övervaka verksamheten som är outsourcad på uppdragstagaren, och att övervaka risken i förhållande till uppdraget?

17. Är det definierat i företagets kontinuitetsplan (BCP) hur uppdraget kan avslutas och tas tillbaka till verksamheten utan större avbrott i verksamheten?

18. Innehåller BCP-planen en krisplan som ska testas regelbundet?

19. Om personuppgifter eller konfidentiella uppgifter behandlas: kan företaget intyga att lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter finns hos uppdragstagaren?

20. Har företaget tillräckliga resurser för att utföra tjänsten ?

RIKTLINJER OM MUTOR OCH REPRESENTATION INOM S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Som S:t Erik Försäkrings AB:s riktlinjer gäller bilaga 1, Stockholm stads riktlinjer avseende mutor och representation, samt därutöver bilaga 2, Institutet mot mutors Näringslivskod.

Riktlinjerna ska prövas årligen av styrelsen och revideras vid behov.

2 Implementering

VD ansvarar för att genomgång av riktlinjerna och överlämnande av desamma sker enligt följande:

- vid nyanställning,
- årligen med samtliga anställda,
- vid outsourcing, med entreprenören.

RIKTLINJER OM MUTOR OCH REPRESENTATION (reviderade år 2015)

En förutsättning för att stockholmarna ska ha förtroende för oss som arbetar inom staden är att vi utför vårt arbete med omdöme och att vi följer gällande lagar och regler. Det är viktigt att vi har en god etik och hög moral.

Dessa riktlinjer har utformats utifrån detta förhållningssätt. Riktlinjerna skall vara ett stöd för oss i vårt arbete och i vår relation med andra som vi kommer i kontakt med i tjänsten. Riktlinjerna gäller för alla förtroendevalda och anställda i staden och i stadens bolag.

Riktlinjerna är uppdaterade med hänsyn till ändringar i lagstiftning m.m. som trätt i kraft fram till den 1 september 2015. Vissa tillägg och justeringar har också skett mot bakgrund av senaste versionen av den s.k. Näringslivskoden (reviderad den 20 november 2014). Se mer om koden nedan på s. 5.

REPRESENTATION

Dessa riktlinjer anger den norm som bör gälla för representation, uppvaktningar och gåvor inom staden. Utgångspunkten är att vår representation ska kännetecknas av måttfullhet. De belopp som anges nedan är hämtade från Skatteverkets allmänna råd. De allmänna råden uppdateras löpande och man bör därför alltid kontrollera att man har de aktuella gränsvärdena.

REPRESENTATION I FORM AV MÅLTIDER M.M.

Extern representation

Extern representation riktar sig mot utomstående organisationer, företag och enskilda personer.

Staden hanterar stockholmarnas pengar. Redan på grund härav ska all representation utgå från en restriktiv inriktning. Att helt förbjuda extern representation är dock inte en realistisk utgångspunkt. T ex måste staden kunna arbeta med marknadsföringsinsatser som turiststad och allmänt främja näringslivet i Stockholm. Att dra en skarp gräns när representation inte ska ske är omöjligt.

Representationen ska alltid ha ett omedelbart samband med och direkt värde för verksamheten. Det gäller både tidpunkt och plats för representationen samt de personer mot vilka representationen riktar sig.

Vi ska vara restriktiva med representation. Detta gäller särskilt i samband med myndighetsutövning, inköp och upphandling, där det i princip inte får förekomma.

Återkommande representation med en och samma person eller grupp av personer bör inte förekomma.

Det bör inte vara fler deltagare från staden än utomstående gäster.

Representation i hemmet ska inte förekomma annat än i rena undantagsfall och fordrar förvaltningschefs eller VDs godkännande. För de sistnämnda gäller godkännande av nämndordförande eller styrelseordförande.

Vid representationsmåltider bör vi iaktta måttfullhet. Särskilt gäller detta bruk av alkohol. Lyxbetonad representation, såsom t.ex. särskilt arrangerade resor eller specialarrangerad underhållning, bör inte förekomma. I speciella situationer, t.ex. vid utländska besök, kan särskilda former av representation förekomma. Dessa undantag ska beslutas av förvaltningschef eller VD.

Starksprit ska inte förekomma vid representation. Undantag kan göras när sedvänja eller kutym kräver det. Undantag från normalregeln ska beslutas av förvaltningschef eller VD.

Intern representation

Med intern representation avses personalfester, informationsmöten, interna kurser och planeringskonferenser. Annan intern representation ska inte förekomma eftersom deltagarna då riskerar att beskattas för förmånen.

Arbetsgivaren kan alltså inte bjuda på t ex idrotts- eller underhållningsevenemang utan att deltagarna riskerar att bli beskattade för förmånen. Undantag kan medges efter beslut av styrelse/nämnd för klart angivna evenemang och i den omfattning som fordras för att den berörde ska kunna fullgöra sitt uppdrag.

Personalfester får endast förekomma två gånger per år. Detta ansluter till de regler som gäller för rätten att göra skatteavdrag.

Stor måttfullhet bör iakttas i synnerhet vad gäller bruk av alkohol. Förvaltningar och bolag ska aldrig bekosta starksprit vid intern representation. Som huvudregel bekostas inte heller andra alkoholhaltiga drycker än lättöl och motsvarande. Undantag från huvudregeln kan göras vid speciella tillfällen och förutsätter att samråd med överordnad chef har skett i förväg.

Måltider i samband med bolagsstämmor, styrelsesammanträden m.m. är inte avdragsgilla. Avdrag medges endast för enklare förtäring.

GÅVOR OCH UPPVAKTNINGAR FRÅN ARBETSGIVAREN

I inkomstskattelagen regleras vilka förmåner som är skattefria respektive skattepliktiga för mottagaren. Inkomstskattelagens regler om skattefria förmåner utgör den övre gränsen för värdet av gåvor m.m. och ska inte överskridas.

Gåvor till anställda

Regler om gåvor bör vara utformade så att de avser samtliga anställda inom förvaltningen eller bolaget. Andra gåvor än de som skattelagstiftningen accepterar som avdragsgilla kan medföra skatteplikt för den anställde. Grundtanken är att en anställd aldrig ska erhålla en gåva, eller annan förmån, som skulle kunna medföra skatteplikt för henne eller honom.

Gåva till anställd får inte förekomma med undantag av:

- Julgåva. Skatteverket har i sina allmänna råd angivit gränsvärde för julgåva och gränsvärdet är för närvarande 450 kr inklusive mervärdesskatt (SKV A 2014:33). Inom staden bör återhållsamhet iakttas och värdet på eventuella julgåvor klart understiga detta gränsvärde. Julgåva ska avse samtliga anställda inom förvaltningen eller bolaget.
- Minnesgåva efter 30 års anställning i form av stadens hedersbelöning.
- Minnesgåva vid pensionsavgång eller vid anställningens upphörande, i båda fallen efter minst 6 års anställning. Enligt inkomstskattelagen är 15 000 kr inklusive mervärdesskatt det högsta värde en sådan gåva får ha utan att vara skattepliktig för den anställde. Även här bör återhållsamhet iakttas och förvaltningar eller bolag som eventuellt delar ut sådan gåva bör tillämpa en mycket lägre beloppsgräns. Förekommer minnesgåvor ska alla anställda omfattas och principer fastställas. Minnesgåva ska, förutom utdelandet av hedersbelöningen, inte ges vid annat tillfälle än vid anställningens upphörande.
- Sedvanlig jubileumsgåva då förvaltningen eller bolaget firar 25-, 50-, 75-årsjubileum eller liknande. Skatteverket har i sina allmänna råd angivit gränsvärde för jubileumsgåvor och gränsvärdet är 1 350 kr inklusive mervärdesskatt (SKV A 2014:33). Även här bör värdet vara klart lägre än så och ansluta till värdet på eventuella julgåvor.
- Uppvaktningar och gåvor vid högtidsdagar, t ex 40, 50 eller 60-årsdag. Även här bör värdet ansluta till värdet på julgåvor.

Enklare reklamgåvor får förekomma om det avser artiklar av närmast obetydligt värde som antingen har direkt anknytning till givarens sortiment eller tillverkning eller utgörs av enklare presentartiklar. För att

en gåva ska klassas som reklamgåva bör den lämnas till ett större antal personer och sakna inslag av personlig karaktär. Sådan gåva ska vara försedd med den givande förvaltningens eller bolagets namn, märke eller dylikt.

Gåvor i form av pengar eller andra kontanta medel t.ex. presentkort medför alltid att mottagaren ska beskattas och ska därför inte förekomma.

Förmåner av mindre värde som avser att skapa trivsel i arbetet, s.k. personalvårds-förmåner, är skattefria och får förekomma. Förmånerna ska normalt vara tillgängliga för all personal och i regel tillhandahållas på arbetsplatsen. Exempel på personalvårdsförmån är förfriskningar och annan enklare förtäring som inte anses som måltid samt enklare motion och annan friskvård. Även klädutrustning av mindre värde och enklare slag, som t.ex. t-shirts och träningsoveraller för den anställdes personliga bruk, och som är försett med arbetsgivarens reklamtryck, får förekomma.

Gåvor till externa (representationsgåvor)

Representationsgåvor förekommer i kommersiella sammanhang och lämnas till representant för det företag man för diskussioner med. Gåvan är avsedd att bidra till goda förbindelser mellan företagen. Representationsgåvor får endast förekomma då det är fråga om att inleda eller bibehålla affärsförbindelser eller dylikt. Gåvan ska alltså ha ett omedelbart samband med verksamheten.

Vid studiebesök och t.ex. besök hos andra kommuner och i liknande situationer får representationsgåvor förekomma som tack för visad gästfrihet.

Skatteverket har i sina allmänna råd angivit gränsvärde för avdragsgilla representationsgåvor och gränsvärdet är för närvarande 180 kr exklusive mervärdesskatt, vilket är det belopp som även gäller för staden.

Reklamgåvor får förekomma om det avser artiklar av förhållandevis obetydligt värde som antingen har direkt anknytning till givarens verksamhet eller utgörs av enklare presentartiklar. För att en gåva ska klassas som reklamgåva bör gåvan lämnas till ett större antal personer och sakna inslag av personlig karaktär. Gåvan ska vara försedd med den givande förvaltningens eller bolagets namn, märke eller dylikt.

MUTOR

Vi som är förtroendevalda eller anställda i staden har dagligen kontakt med ett stort antal människor och företag. Vid dessa kontakter riskerar vi att utsättas för otillbörlig påverkan. Vi kanske inte alltid tänker på att erbjudanden och förmåner som vi får från dem vi träffar i tjänsten kan vara olagliga eller olämpliga. För att förhindra korruption finns bestämmelser om mutbrott. Dessa har till syfte att skydda både vår arbetsgivare staden och samhället i stort mot illojalt och felaktigt handlande hos oss förtroendevalda eller anställda.

Mutbrottslagstiftningen ändrades i vissa delar den 1 juli 2012. De flesta ändringarna innebar en modernisering av reglerna utan någon större förändring i sak. Det brott som tidigare hette bestickning kallas nu *givande av muta* och det brott som tidigare hette muta kallas nu *tagande av muta*. Man införde också ett nytt brott som kallas *handel med inflytande*. Straffbestämmelsen *handel med inflytande* täcker bland annat in den situationen att en arbetskamrat eller närstående (t ex make eller barn) till en beslutsfattare tar emot en otillbörlig förmån för att påverka beslutsfattarens beslut.

I staden finns en fast praxis hur vi ska agera om vi erbjuds förmåner av olika slag från personer och företag som vi har kontakt med i våra arbeten. Målet är att ingen ens ska kunna misstänkas för att ta emot mutor.

Lagen gör i princip ingen skillnad mellan om den som erhåller eller erbjuds en förmån är anställd i ett privat företag eller arbetar i offentlig verksamhet. De rättsfall som finns visar emellertid att det ställs särskilt höga krav på offentligt anställda, och då särskilt på de som ägnar sig åt myndighetsutövning (t ex tillståndsgivning, beslut om rättigheter, inspektion) och på de som arbetar med upphandling och inköp. Även inom omsorgsområdet ställs särskilt höga krav.

Den s.k. Näringslivskoden, *Kod om gåvor, belöningar och andra förmåner i näringslivet*, fastställs av Institutet Mot Mutor (IMM) och är en vägledande uppförandekod till stöd för hur företag, både privat och offentligt ägda, kan förhålla sig till förmåner inom näringslivet och i förhållande till offentliga organ och bolag för att undvika att bryta mot mutlagstiftningen.

Enligt Näringslivskoden är det alltid otillåtet med gåvor, belöningar eller andra förmåner till den som utövar myndighet eller beslutar om offentlig upphandling.

Enligt Näringslivskoden gäller också att det, utöver de som utövar myndighet eller beslutar om offentlig upphandling, finns andra personkategorier där ”förmåner visserligen inte är helt otillåtet men där särskild restriktivitet ändå ska iakttas. Exempel på sådana kategorier är arbets- eller uppdragstagare:

a) vid offentliga organ, även om personen inte deltar i myndighetsutövning eller offentlig upphandling,

b) inom integritetskänsliga verksamheter där särskilda skyddsintressen gör sig gällande, såsom offentligt ägda eller finansierade företag, privatägda banker, finans- och försäkringsföretag samt företag inom certifiering och kontrollerande verksamhet.”

I staden ska vi tillämpa dessa regler. Detta innebär alltså att de av oss som i sitt arbete utövar myndighet eller beslutar om offentlig upphandling aldrig ska ta emot gåvor, belöningar eller andra förmåner. Andra anställda inom stadens olika verksamheter arbetar ju vid offentliga organ och/eller inom integritetskänsliga verksamheter där särskilda skyddsintressen gör

sig gällande och ska därmed iaktta särskild försiktighet när det gäller att ta emot förmåner av olika slag.

Graden av restriktivitet kan dock variera något beroende på t.ex. vilken slags förmån eller värde det är fråga om och vilken slags verksamhet och arbetsuppgifter vi har.

Om man t.ex. arbetar inom omsorgsområdet är utrymmet för att ta emot gåvor mycket litet. Endast undantagsvis kan det accepteras och då bara i form av gåvor av trivselkaraktär t ex en enklare blomma, kakor, choklad eller liknande.

Vad som kan bedömas som otillåten förmån och muta kan variera från fall till fall. Utgångspunkten är att vi inte ska ta emot något som kan anses beteendepåverkande, dvs. påverkar eller riskerar att påverka våra beslut eller vårt sätt att fullgöra våra arbetsuppgifter.

Det kan ibland vara osäkert var gränsen mellan det tillåtna och det otillåtna går. Vid tveksamhet ska vi tacka nej eller rådgöra med vår närmaste chef. Om vi t.ex. erbjuds att delta i en kundträff bör vi informera vår närmaste chef.

Exempel på hur vi ska agera i olika situationer

Nedan följer en katalog på exempel som ska underlätta för oss att avgöra vad som kan vara tillåtet och vad som kan vara straffbart.

Måltider

Vi låter oss inte bjudas på måltider av en leverantör eller entreprenör om måltiden inte har ett naturligt samband med arbetet och är av typen normal arbetslunch eller liknande. Måltiderna får inte förekomma för ofta.

Visning av projekt, projektturer

Om en byggherre eller entreprenör vill visa ett relevant projekt och bjuda på en enklare måltid är detta normalt tillåtet. Om vi måste resa eller bo på hotell för att delta i visningen bekostar staden detta och står för uppehället.

Kundträffar

Om ett företag som staden handlar med bjuder på en kundträff är det normalt tillåtet att delta om syftet med träffen är att utbyta information. Om det vid träffen förekommer viss underhållning och bjuds på enklare förtäring innebär inte det att kundträffen blir en muta. Det är dock viktigt att huvudsyftet är just informationsutbytet, inte nöje, och träffen får inte vara lyxbetonad. Om vi måste resa eller bo på hotell för att delta i kundträffen bekostar staden detta och står för uppehället.

Studieresor, konferenser

Studieresor och konferenser som affärskontakter vill bjuda på tackar vi alltid nej till. Är det en studieresa eller konferens som det är viktigt för oss att delta i för att vi ska kunna fullgöra våra arbetsuppgifter står staden för kostnaderna för konferensen samt resa, hotell och uppehälle. Det är givetvis inte acceptabelt att affärskontakten bekostar t ex uppgradering till

ett dyrare hotellrum. Om det bjuds på enklare förtäring innebär inte det att studieresan eller konferensen blir en muta. På sedvanligt sätt beslutar överordnad chef vem som deltar.

Gåvor

Vi bör inte ta emot gåvor. Gåvor kan vara av många olika slag, inte bara presenter. T ex är biljetter till idrotts- eller underhållningsevenemang naturligtvis också gåvor. Även förmåner utan ekonomiskt värde kan vara otillåtna, t.ex. sådant som har ett affektionsvärde för mottagaren. Om vi får gåvor i samband med högtidsdagar eller jul kan detta accepteras. Gåvorna bör dock inte vara värda mer än 200-300 kronor.

Som angetts ovan ska de som utövar myndighet eller beslutar om offentlig upphandling aldrig ta emot gåvor. Se också vad som angetts beträffande gåvor till de som arbetar t ex inom omsorgsområdet

Rabatter, kontanter, lån

Rabatter riktade till enskilda medarbetare tackar vi nej till. Rabatter riktade till alla anställda i staden eller i en förvaltning kan i vissa fall vara godtagbara. Erbjudanden om pengar och lån ska vi naturligtvis alltid tacka nej till.

Rabatter och förmåner av typen ”flygpoäng”

Vissa flygbolag utger, enligt vedertagen internationell praxis, rabatter eller liknande förmåner för visad kundtrohet.

Alla rabatter som vi får i samband med tjänsteresor ska tillfalla staden.

Erbjudanden på fritiden

Det är inte ovanligt att vi får erbjudanden av affärskontakter om att fritt eller till subventionerat pris delta i olika evenemang på vår fritid. Det kan vara fråga om att resa, att låna en sommarstuga/segelbåt eller om aktiviteter som t.ex. golftävlingar. Detta ska vi alltid tacka nej till. Att erbjudandet gäller under semester eller fritid hindrar inte att det kan betraktas som muta.

Riktlinjerna ovan gäller även om man lär känna en affärskontakt så väl att det blivit fråga om vänskap. Kravet är alltid detsamma, nämligen att vi ska uppträda sakligt och opartiskt.

Vi behöver inte ha blivit påverkade av ett erbjudande för att det ska kunna bli mutbrott. Det räcker att man objektivt sett skulle kunna tänkas bli påverkad av förmånen.

Självfallet ska vi tillämpa samma policy när vi vill bjuda en affärskontakt eller t ex uppvakta någon kollega i en annan kommun.

JÄV

Reglerna om jäv följer av lag. De talar om när vi ska anses ha ett sådant intresse i ett ärende att vår opartiskhet kan ifrågasättas. Om vi är jäviga får

vi inte delta i handläggningen av ärendet. Om någon som är jävig deltar i handläggningen kan beslutet överklagas på grund av jävet.

Det finns en skyldighet enligt lag att självmant anmäla jäv. Om vi känner till någon omständighet som kan antas utgöra jäv ska vi meddela detta. Det kan ibland förekomma situationer som är svåra att bedöma ur jävssynpunkt. I sådana fall bör vi iaktta försiktighet och som förtroendevalda eller anställda avstå från att delta i hanteringen av ärendet. Även här gäller således att vi inte ska kunna misstänkas för något felaktigt agerande.

När föreligger jäv?

För nämndledamöter och anställda föreligger jäv i följande situationer:

- Om saken angår oss själva eller någon närstående eller om ärendets utgång kan väntas medföra synnerlig nytta eller skada för oss själva eller någon närstående.
- Om vi är ställföreträdare – t ex förvaltare, god man eller firmatecknare – för den som saken angår eller för någon som kan vänta synnerlig nytta eller skada av ärendets utgång.
- Om ärendet rör tillsyn över sådan kommunal verksamhet som vi själva är knutna till.
- Om vi har fört talan som ombud eller mot ersättning biträtt någon i saken.
- Om det i övrigt finns någon särskild omständighet som är ägnad att rubba förtroendet för vår opartiskhet i ärendet.

För ledamöter i kommunfullmäktige gäller endast den första punkten vid behandling av ärenden i kommunfullmäktige.

KOD MOT KORRUPTION I NÄRINGSLIVET

INSTITUTET MOT MUTOR

Institutet Mot Mutor
Box 16050, 103 21 Stockholm
Tel: 08 - 555 100 45
E-post: info@institutetmotmutor.se
Webb: www.institutetmotmutor.se

Förord

Institutet Mot Mutor (IMM), som grundades 1923, har sedan sin tillkomst verkat för självreglering som medel att bekämpa korruption i samhället. Genom sina huvudmän har institutet en bred räckvidd både inom näringslivet, kommuner och regioner.

IMM har varit pådrivande i kampen mot mutor och korruption och i att framhålla vikten av kraftfull lagstiftning på området. IMM tog initiativ till den reformering av mutbrottslagstiftningen som skedde 2012 (se proposition 2011/12:79, En reformerad mutbrottslagstiftning). Den första versionen av denna kod togs fram i anslutning till den reformen.

Brottsbalkens regler om mutbrott är dock allmänt hållna och svårtolkade trots den reformering som skett. Tolkningen kan också förändras av samhällsutvecklingen. Denna Kod mot korruption i näringslivet - ”koden”- ska ses som ett komplement till lagstiftningen, den fyller ut och förtydligar straffbestämmelserna, i den meningen att den ger en samlad bild av ett etiskt försvarbart handlingssätt i olika situationer. Men också på det sättet att den ska verka för att förebygga korruption.

Den revidering som nu gjorts har pågått under mer än två års tid och innefattat en omfattande synpunktsinhämtning på såväl den tidigare versionen av koden som på förslag till nya och justerade skrivningar. Efterfrågan på mer ledning i fråga om förebyggande åtgärder samt kontroll av mellanhänder har mötts genom att koden i dessa avseenden väsentligt har utvidgats. Koden har också i fråga om avsnittet om förmåner delvis strukturerats om samtidigt som ett antal praktiska exempel införts för att underlätta förståelsen av reglerna. Namnet har ändrats som en följd av att koden nu även inkluderar krav på åtgärder mot korruption, vilket inte är begränsat till hantering av förmåner.

Koden omfattar hela näringslivet och inte minst relationen mellan näringslivet och offentlig sektor. Frågan om korruption är komplex och ger ofta upphov till svåra gränsdragningar. Den synpunktsinhämtning som skett har mot den bakgrunden varit mycket värdefull. Härigenom har koden också blivit väl förankrad. Förhoppningen är att koden i dess reviderade lydelse ska ge utvidgad och relevant vägledning och stöd för att förebygga och hantera korruptionsrisker.

För en kommentar till mutbrottslagstiftningen och dess tillämpning hänvisas till Thorsten Cars och Natali Engstam Phalén, Mutbrott, 4 uppl., Norstedts juridik, Stockholm 2020.

Koden, som förvaltas av IMM, gäller i sin nya lydelse från denna dag.

Stockholm den 14 augusti 2020.

Fredrik Wersäll

Ordförande

Innehållsförteckning

A. Om koden

1. Varför denna kod?

1.1 Syfte

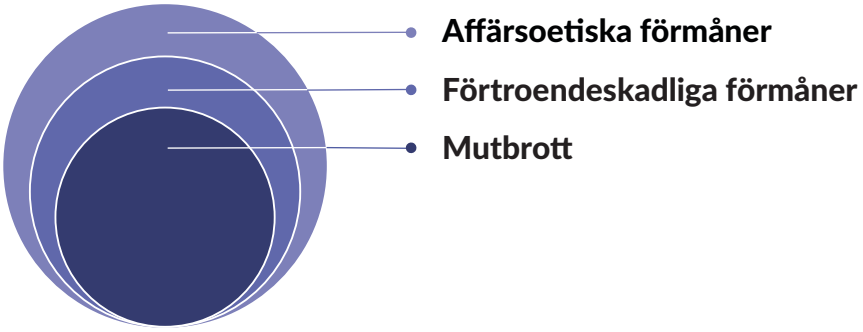
Institutet Mot Mutor (IMM) har som uppgift att motverka korruption och underlätta för samhällets aktörer att hantera korruptionsrisker. IMM har ända sedan sin tillkomst 1923 verkat för självreglering som medel att bekämpa korruption i samhället. Denna kod tillsammans med IMM:s Etiknämnd ger förutsättningar för självreglering i näringslivet på detta område. Med effektiv självreglering kan en trygghet skapas för näringslivet i fråga om vad som är tillåtet, samtidigt som den bidrar till att samhället kan ha förtroende för att näringslivet agerar på en hög etisk nivå.

Syftet med koden är:

- att tillgodose näringslivets intresse av att anställda och uppdragstagare inte låter sig påverkas att agera till nackdel för företaget genom att ge eller ta emot otillåtna förmåner,
- att öka förtroendet för näringslivet, eftersom samhället måste kunna förlita sig på att marknaden fungerar väl ur ett affärsetiskt perspektiv,
- att främja marknadens intresse av effektiv och sund konkurrens på lika villkor.

1.2 Koden som självreglering

Kodens utgångspunkt är brottsbalkens bestämmelser om mutbrott. Ett förfarande som strider mot lagen är inte heller förenligt med koden. Koden syftar också till att förmåner inte ska ges på sådant sätt att det skadar förtroendet för vissa särskilt skyddsvärda aktörer samt att förmåner inte ska ges till andra aktörer på ett sätt som inte är förenligt med den etik som bör gälla i näringslivet. Koden etablerar därmed en etisk standard för dessa situationer som i vissa avseenden ställer andra krav än de straffrättsliga reglerna, se illustration nedan. Genom att ansluta sig till koden åtar sig företagen att handla så att kodens syften främjas.



Koden vägleder företag i fråga om de förebyggande åtgärder som ska vidtas mot korruption.

Koden ska hjälpa företag att bedöma vad som är en tillåten förmån respektive vad som kan utgöra en otillåten förmån. Reglerna är med nödvändighet allmänt hållna och innebörden belyses med exempel. Reglerna kan och bör kompletteras med egna, mer detaljerade regler (se avsnitt C.4). Bedömningen i det enskilda fallet är beroende av de faktiska omständigheterna. Företag kan begära att Etiknämnden uttalar sig i ett enskilt fall.

Koden vägleder också företag i fråga om kontrollåtgärder som behöver vidtas i förhållande till mellanhänder för att mutbrott ska undvikas.

2. Etiknämnden

Etiknämnden inrättades av IMM år 2013. Etiknämnden har till uppgift att genom bl.a. uttalanden verka för god sed inom det område som omfattas av koden. Genom Etiknämndens beslut kan kodens bestämmelser konkretiseras i enskilda fall. Etiknämndens beslut i anonymiserad form samt information om nämnden och kontaktuppgifter till nämnden finns på IMM:s hemsida: www.institutetmotmutor.se/etiknamnden

3. Vem riktar sig koden till?

Koden riktar sig till företag som bedriver näringsverksamhet, oavsett om ägandet är privat eller offentligt, samt till svenska företags filialer och koncernföretag i utlandet.

Koden kan också användas av myndigheter, kommuner och andra aktörer.

4. Internationella förhållanden

Koden är i fråga om förmåner i första hand skriven för svenska förhållanden. De etiska riktlinjer som uttrycks i koden bör normalt vara tillämpliga även i en internationell kontext. Vid bedömning i enskilda fall kan också lokala seder och bruk liksom vedertagna former för internationellt umgänge få betydelse.

B. Gällande bestämmelser

1. Svenska straffbestämmelser

De svenska straffbestämmelserna om mutbrott finns i brottsbalken 10 kap. 5 a–e §§. Brottsbeskrivningarna lyder:

5 a § Den som är arbetstagare eller utövar uppdrag och tar emot, godtar ett löfte om eller begär en otillbörlig förmån för utövningen av anställningen eller uppdraget döms för **tagande av muta** till böter eller fängelse i högst två år. Detsamma gäller den som är deltagare eller funktionär i en tävling som är föremål för allmänt anordnad vadhållning och det är fråga om en otillbörlig förmån för hans eller hennes fullgörande av uppgifter vid tävlingen.

Första stycket gäller även om gärningen har begåtts innan gärningsmannen fått en sådan ställning som avses där eller efter det att den upphört.

För tagande av muta enligt första och andra styckena döms också den som tar emot, godtar ett löfte om eller begär förmånen för någon annan än sig själv.

5 b § Den som lämnar, utlovar eller erbjuder en otillbörlig förmån i fall som avses i 5 a § döms för **givande av muta** till böter eller fängelse i högst två år.

5 d § För **handel med inflytande** döms till böter eller fängelse i högst två år den som i annat fall än som avses i 5 a eller 5 b §

1. tar emot, godtar ett löfte om eller begär en otillbörlig förmån för att påverka annans beslut eller åtgärd vid myndighetsutövning eller offentlig upphandling, eller

2. lämnar, utlovar eller erbjuder någon en otillbörlig förmån för att han eller hon ska påverka annans beslut eller åtgärd vid myndighetsutövning eller offentlig upphandling.

5 e § En näringsidkare som tillhandahåller pengar eller andra tillgångar åt någon som företräder näringsidkaren i en viss angelägenhet och därigenom av grov oaktsamhet främjar givande av muta, grovt givande av muta eller handel med inflytande enligt 5 d § 2 i den angelägenheten döms för **vårdslös finansiering av mutbrott** till böter eller fängelse i högst två år.

Smörjmedelsbetalningar (eng. *facilitation payments*) är inte undantagna från svensk mutlagstiftning. Med smörjmedelsbetalning menas normalt små betalningar till offentliga tjänstemän för att få en tjänst eller för att skynda på en process eller ett beslut.

Den närmare innebörden av straffbestämmelserna framgår av lagförarbeten, domstolsavgöranden och lagkommentarer.

Enligt svensk straffrätt kan enbart fysiska personer begå brott. Straffansvaret för mutbrott är därmed personligt. Om brott har begåtts kan företag dömas att betala en företagsbot om företaget inte i tillräcklig utsträckning har vidtagit åtgärder för att förebygga brottsligheten eller om brottet har begåtts av en person i ledande ställning eller med särskilt ansvar för tillsyn eller kontroll i företaget. Personer och företag kan också få vinster förverkade.

2. Övriga viktiga beaktanden

Företag som verkar utomlands måste också beakta mutlagstiftningen i de länder där företaget är verksamt.

Vissa länders lagstiftning har räckvidd utanför det egna landet och kan behöva beaktas av svenska företag (t.ex. amerikansk och brittisk).

Många branscher har antagit egna regler om förmåner.

C. Förebyggande åtgärder

1. Allmänna utgångspunkter

Företag ska vidta förebyggande åtgärder mot korruption. Åtgärderna ska vara anpassade till företagets storlek och ägarförhållanden, den verksamhet som bedrivs och de korruptionsrisker företaget möter. De förebyggande åtgärderna ska syfta till att skapa en kultur mot korruption och vara utformade på ett effektivt sätt för att undvika korruptionsrisker samt upptäcka korrupta ageranden.

Nedan beskrivs de komponenter som ett förebyggande arbete bör innehålla. Vad gäller de enskilda komponenternas närmare utformning är det varje företags ansvar att anpassa dessa efter sina egna behov. Den centrala frågan för utformningen är vilka risker företaget står inför. De åtgärder som vidtas ska vara proportionella till identifierade risker.

2. Ställningstagande från ledningen

Ledningen har en avgörande roll för ett framgångsrikt antikorruptionsarbete. I företagets regler mot korruption och i övrig intern och extern kommunikation ska tydligt anges ledningens ställningstagande mot korruption.

I ledningens ansvar ingår också att säkerställa att det finns tillräckliga resurser och kompetens för det förebyggande antikorruptionsarbetet samt att styrelsen håller sig löpande informerad om företagets antikorruptionsarbete.

3. Analys av risken för korruption

Företag ska på regelbunden basis genomföra riskanalyser som specifikt avser vilka korruptionsrisker företaget har. Frågor som bör besvaras i riskanalysen är:

- Vilka korruptionsrisker möter företaget och inom vilka delar?
- Vad blir konsekvensen om en risk realiseras?
- Finns brister i hur identifierade korruptionsrisker hanteras i dag?

De övriga förebyggande åtgärderna ska utformas utifrån resultatet av riskanalysen. Riskanalysen ska ses över årligen samt vid behov.

4. Interna regler mot korruption

Företag ska ha skriftliga regler mot korruption. Dessa ska innehålla företagets övergripande ståndpunkt mot korruption samt de konkreta riktlinjer och regler som företaget uppställer för att undvika korruption (detta kan ske genom en allmän policy, eventuellt i kombination med särskilda riktlinjer för olika områden, t.ex. intressekonflikter, representation och sponsring).

Genom de egna reglerna kan de övergripande principer som anges i denna kod i fråga om hantering av förmåner (avsnitt D) konkretiseras och anpassas till det enskilda företaget.

Det ska framgå vem eller vilken avdelning som svarar för företagets regler och till vem företagets anställda kan vända sig för rådgivning.

Det ska anges vad som händer när reglerna överträds.

5. Kommunikation och utbildning

Företag ska offentliggöra sin inställning till korruption.

Företag ska tillse att deras anställda utbildas regelbundet om de interna reglerna mot korruption och om reglernas tillämpning. Även företags mellanhänder och andra tredjeparter kan behöva få sådan utbildning.

6. System för kontroll av mellanhänder och andra tredjeparter

Företag ska ha system för kontroll av mellanhänder enligt vad som anges i avsnitt E i denna kod.

Företag ska ha rutiner för att hantera korruptionsrisker förknippade med andra tredjeparter än mellanhänder.

7. Rapporteringssystem (visselblåsning)

Företag ska säkerställa att det finns möjlighet att rapportera misstankar om korruption utan att den som rapporterar utsätts för negativa konsekvenser.

Företag ska ha rutiner för uppföljning av rapporter.

8. Verktyg för kontroll och uppföljning

Företag ska ha de interna kontrollsystem som krävs för att säkerställa implementeringen av de förebyggande åtgärderna.

De åtgärder som vidtas ska löpande följas upp och utvärderas samt uppdateras vid behov.

D. Förmåner

1. Vad är en förmån?

En förmån ska ha ett materiellt eller immateriellt värde för mottagaren. Förmåner kan ha många olika former såsom kontanter, presentkort, varor, tjänster, rabatter, resor, lån av pengar eller saker, biljetter till evenemang, sponsring, provision, anställning eller uppdrag, förtur i en kö eller en prestigefylld utmärkelse.

För att det ska vara en förmån enligt koden ska den ges till en arbetstagare eller uppdragstagare från någon annan än arbetsgivaren eller uppdragsgivaren.

Exempel: En arbetsgivare har förhandlat fram rabatter hos ett företag för arbetsgivarens anställda. Rabatten utgör inte en förmån enligt denna kod för de anställda.

Det ska också vara något som arbetstagaren eller uppdragstagaren skulle ha stått kostnaden för själv.

Exempel: Ett företag anlitar en representant från en annan verksamhet för att hålla en utbildning på annan ort än där representanten är verksam. Det utgör inte en förmån om företaget betalar normala och nödvändiga resekostnader för den som håller utbildningen.

Givandet av förmånen ska ha samband med utförandet av arbetstagarens arbete eller uppdragstagarens uppdrag (tjänstesamband). Förmåner som ges mellan t.ex. vänner utan att det finns någon koppling till en anställning eller ett uppdrag omfattas alltså inte. För att förmånen ska undantas ska den ha sin grund uteslutande eller i allt väsentligt i något annat förhållande än tjänstesambandet.

Exempel: A och B är barndomsvänner. B arbetar i ett företag som levererar tjänster till A:s arbetsgivare. På grund av vänskapsbandet bjuder B på sin födelsedag A på middag. Middagen är ingen förmån enligt denna kod.

En förmån kan ges direkt till en arbetstagare eller uppdragstagare, men en förmån kan även ges till någon annan eller genom någon annan.

Exempel: A ansvarar för genomförandet av en upphandling. A ber en potentiell anbudsgivare om sponsringspengar till A:s barns idrottslag. Upplägget utgör en förmån till A.

Som förmån räknas inte sådant med obetydligt värde som förekommer vid normalt arbetsrelaterat umgänge, t.ex. kaffe och kaffebröd/frukt i samband med ett arbetsmöte.

I koden används uttrycken ge respektive ta emot en förmån. Är det otillåtet att ge respektive att ta emot en förmån, får förmånen inte heller erbjudas eller utlovas respektive begäras eller accepteras. När uttrycken ge respektive ta emot används i koden avses alla nyss nämnda situationer.

2. Hur kan förmåner ges och tas emot?

2.1 Olika situationer

Bedömningen av om det är tillåtet att ge eller ta emot en förmån skiljer sig beroende på tillfälle och vem som är mottagare.

Koden gör skillnad mellan tre slags situationer som behandlas under olika avsnitt i koden.

2.2 Mottagare vid myndighetsutövning och offentlig upphandling (s. 10)

2.3 Mottagare inom offentlig sektor och inom offentligt finansierad verksamhet i andra fall än vid myndighetsutövning och offentlig upphandling (s. 11)

2.4 Mottagare inom privat sektor (s. 14)

2.2 Mottagare vid myndighetsutövning och offentlig upphandling

Det är förbjudet att ge respektive ta emot en förmån vid myndighetsutövning eller vid genomförande av en offentlig upphandling. Det har ingen betydelse om en förmån ges eller tas emot före eller efter det att ett beslut har fattats. Förbudet att ge eller ta emot förmåner gäller i förhållande till mottagare som direkt fattar beslut om eller har möjlighet att påverka, även indirekt, myndighetsutövningen eller genomförandet av den offentliga upphandlingen.

Exempel: Myndighetsföreträdare genomför inom ramen för ett tillsynsärende ett platsbesök hos ett företag. Ett stort antal handlingar ska gås igenom vid besöket och myndighetsföreträdarna kommer att vara på företaget över lunchtid. Det är inte tillåtet att företaget bjuder myndighetsföreträdarna på ens en enklare lunch.

När förmåner ges till mottagare som arbetar med myndighetsutövning eller offentlig upphandling i situationer som inte har någon koppling till myndighetsutövning eller offentlig upphandling gäller i stället vad som står i avsnitt 2.3.

Exempel: En myndighetsanställd som har bland sina arbetsuppgifter att utöva myndighet har bjudits in av en organisation för att tala på en konferens. Den myndighetsanställde är inte involverad i ett pågående ärende rörande organisationen. Som tack för genomfört talaruppdrag får den myndighetsanställde en blombukett. Blombuketten omfattas inte av förbudet mot förmåner eftersom det saknas samband med myndighetsutövning eller offentlig upphandling. Tillåtligheten att ta emot blombuketten får i stället prövas enligt avsnitt 2.3.

Med myndighetsutövning avses detsamma som i allmänhet enligt lag. Begreppet omfattar beslut om förmåner och skyldigheter som meddelas enligt lag eller förordning och är bindande för enskilda personer och organisationer. Exempel på myndighetsutövning är beslut om serveringstillstånd och bygglov. I de flesta fall meddelas besluten av myndigheter, men privata företag kan genom lag anförtros att utöva myndighet, t.ex. bilbesiktning.

Med offentlig upphandling avses åtgärd enligt lagarna om offentlig upphandling.

2.3 Mottagare inom offentlig sektor och inom offentligt finansierad verksamhet i andra fall än vid myndighetsutövning och offentlig upphandling

2.3.1 Kategorier av mottagare

Anställda och uppdragstagare inom offentlig sektor och offentligt finansierad verksamhet förvaltar ett förtroende från allmänheten. Verksamheten bedrivs i medborgarnas intresse och den ska skyddas mot korruption. Det får inte uppstå tvivel om att beslutsfattandet har skett på sakliga och objektiva grunder. Av domstolsavgöranden framgår att skyddsintresset för mutbrott inom den offentliga sektorn är förvaltningens integritet samt att allmänheten ska kunna förlita sig på att det offentliga bedriver sin verksamhet med absolut hederlighet och opartiskhet. Utgångspunkten är därför att det ska råda försiktighet vad gäller förmåner till denna mottagarkategori.

Med offentlig sektor menas den skatte- och avgiftsfinansierade verksamheten som drivs av det allmänna samt företag som ägs av staten, kommuner eller regioner.

Med offentligt finansierad verksamhet menas sådan verksamhet där det allmänna ger ekonomisk ersättning till själva driften. Exempel på offentligt finansierad verksamhet är verksamhet som bedrivs i privat regi inom vård, skola och omsorg.

Mottagare som arbetar med myndighetsutövning eller offentlig upphandling omfattas av detta avsnitt när avsnitt 2.2 inte gäller.

För att en förmån som ges till eller tas emot av en mottagare i offentlig sektor eller offentligt finansierad verksamhet ska vara tillåten gäller följande.

2.3.2 Otillåtna förmåner

En förmån är otillåten om den påverkar eller riskerar att påverka mottagarens beslut eller sätt att fullgöra sina arbetsuppgifter, t.ex. en gåva av inte obetydligt ekonomiskt eller personligt värde för mottagaren. Bedömningen får göras från fall till fall.

Följande slag av förmåner är på grund av sin beteendepåverkande natur otillåtna:

a. penninggåva och lån av pengar,

b. testamentariska förordnanden,

c. varor och tjänster för privat ändamål och privata rabatter på varor och tjänster,

d. rätt att använda fordon, båt, fritidsbostad eller liknande för privat bruk,

e. nöjes- eller semesterresa,

f. köp av sexuella tjänster eller besök på stripp- och porrklubb, och

g. förmåner som kan medföra att givaren får en hållhake på mottagaren.

Förmåner som inte är otillåtna enligt den här bestämmelsen ska prövas mot kraven på öppenhet och måttfullhet.

2.3.3 Förmåner ska ges öppet

Förmåner ska ges öppet. Det innebär att en förmån ska riktas direkt till mottagarens arbets- eller uppdragsgivare eller vara förenlig med dennes etablerade policy i fråga om förmåner.

Ett godkännande från mottagarens arbetsgivare att ta emot en förmån är inte tillräckligt för att det ska vara tillåtet att ge respektive ta emot förmånen utan förmånen måste också vara måttfull.

2.3.4 Förmåner ska vara måttfulla

Huruvida en förmån är måttfull avgörs i första hand av förmånens ekonomiska eller personliga värde för mottagaren. Om flera förmåner erbjuds till en och samma anställd eller uppdragstagare ska dessa förmåner bedömas i ett sammanhang. En förmån som sedd för sig är måttfull är alltså inte måttfull om den tillsammans med andra förmåner riktade till samma mottagare ökar risken för att mottagaren ska påverkas i sitt arbete eller uppdrag.

När det ska bedömas om en förmån är måttfull ska följande omständigheter beaktas.

— Mottagare

Det är betydelsefullt vilken anställning eller vilket uppdrag mottagaren av förmånen har. Vissa tjänsteställningar har särskilt höga krav på skydd för integriteten. Detta gäller t.ex. personer som arbetar med eller kan fatta beslut rörande myndighetsutövning, offentlig upphandling, inköp och avtalsförvaltning. Även vissa sektorer har särskilt höga krav på skydd för integriteten, t.ex. vård och omsorg.

Mottagarens position i förhållande till givaren är också av betydelse. Det är en varningsflagga om en förmån ges till en mottagare i nära anslutning till beslut som berör givaren.

— Förmånen

Risken för att en förmån ska bedömas som otillåten ökar med förmånens ekonomiska eller personliga värde liksom med antalet förmåner till samma mottagare. I allmänhet ska därför försiktighet iakttas när det gäller förmåner av inte obetydligt värde, förmåner som förekommer frekvent och förmåner med personligt värde.

Exempel: I ett rättsfall har det ansetts utgöra mutbrott att bjuda en offentliganställd på lunch och på café med hänvisning till att det förekommit vid flera tillfällen.

— Arbetskoppling

Risken för att en förmån ska bedömas som otillåten ökar om förmånen är av ett sådant slag att den saknar anknytning till mottagarens arbetsuppgifter. Det är därför av betydelse om förmånen har ett tydligt samband med och ingår som ett naturligt och nyttigt led i mottagarens arbete.

Exempel 1: Det är i allmänhet tillåtet att bjuda på en måltid i samband med ett möte där arbetsrelaterade frågor diskuteras, eller att arrangera en studieresa där arbetsrelaterade programpunkter utgör ett väsentligt inslag.

Exempel 2: Mingel eller annan sammankomst som en bred krets av personer bjuds in till och som anordnas i syfte att skapa kontakt, informera om verksamhet och liknande och där arbetskopplingen är i fokus är i allmänhet tillåtet även om det bjuds på förtäring.

Det är som utgångspunkt inte tillåtet att den anställde eller uppdragstagaren bjuds in till evenemang tillsammans med medföljande, t.ex. en anhörig eller vän. I vissa fall kan dock ett arrangemangs karaktär motivera en annan bedömning.

2.4 Mottagare inom privat sektor

2.4.1 Skyddsintressen

Inom privat sektor är de huvudsakliga skyddsintressena att anställda och uppdragstagare ska agera lojalt mot sin arbets- respektive uppdragsgivare samt att företag ska konkurrera på lika villkor utan användning av förmåner på ett oetiskt sätt. Det finns också ett allmänt intresse av att främja sunda affärsmetoder och i förlängningen ett förtroende från allmänheten gentemot det privata näringslivet.

Vissa aktörer inom privat sektor förvaltar därutöver ett särskilt förtroende från allmänheten som behöver skyddas. Det gäller t.ex. banker, finans- och försäkringsföretag, skiljemän, offentligt utsedda rättsliga biträden och ombud, journalister, revisorer samt företag inom certifiering och kontroll.

För att en förmån som ges till eller tas emot av en mottagare i privat sektor ska vara tillåten gäller följande.

2.4.2 Otillåtna förmåner

En förmån är otillåten om den påverkar eller riskerar att påverka mottagarens beslut eller sätt att fullgöra sina arbetsuppgifter, t.ex. en gåva av högt ekonomiskt eller personligt värde för mottagaren. Bedömningen får göras från fall till fall.

Följande slag av förmåner är på grund av sin beteendepåverkande natur otillåtna:

a. penninggåva och lån av pengar,

b. varor och tjänster för privat ändamål och privata rabatter på varor och tjänster,

c. rätt att använda fordon, båt, fritidsbostad eller liknande för privat bruk,

d. nöjes- eller semesterresa,

e. köp av sexuella tjänster eller besök på stripp- och porrklubb, och

f. förmåner som kan medföra att givaren får en hållhake på mottagaren.

Förmåner som inte är otillåtna enligt den här bestämmelsen ska prövas mot kraven på öppenhet och måttfullhet.

2.4.3 Förmåner ska ges öppet

Förmåner ska ges öppet. Det innebär att en förmån ska riktas direkt till mottagarens arbets- eller uppdragsgivare eller vara godkänd av denne eller vara förenlig med dennes etablerade policy i fråga om förmåner.

2.4.4 Förmåner ska vara måttfulla

Huruvida en förmån är måttfull avgörs i första hand av förmånens ekonomiska eller personliga värde för mottagaren. Om flera förmåner erbjuds till en och samma anställd eller uppdragstagare ska dessa förmåner bedömas i ett sammanhang.

När det ska bedömas om en förmån är måttfull ska följande omständigheter beaktas.

— Mottagare

Det är betydelsefullt vilken anställning eller vilket uppdrag mottagaren av förmånen har. I fråga om mottagare hos aktörer som enligt ovan förvaltar ett särskilt förtroende från allmänheten ska förmåner ges respektive tas emot med större försiktighet än inom privat sektor i övrigt. Sådana mottagare är särskilt känsliga i integritetshänseende.

Exempel: En särskild roll intar mottagare som har avgörande inflytande på beslut, t.ex. i fråga om beviljande av lån och skadereglering. Inga förmåner ska ges till dessa mottagare vid sådana beslut.

Även i övrigt ska det råda större försiktighet vad gäller förmåner till mottagare som har avgörande inflytande på beslut för givaren eller givarens företag, t.ex. i fråga om inköp.

— Förmånen

Risken för att en förmån ska bedömas som otillåten ökar med förmånens ekonomiska eller personliga värde liksom med antalet förmåner till samma mottagare. I allmänhet ska därför försiktighet iakttas när det gäller förmåner av högre värde, förmåner som förekommer frekvent och förmåner med personligt värde, t.ex. varor eller tjänster som kan utnyttjas privat.

Exempel: I rättspraxis har det ansetts utgöra mutbrott att erbjuda inköpsansvariga vid företag möjlighet att välja en present av privat natur till ett värde av några hundralappar, om den inköpsansvarige beställer produkter från det erbjudande företaget.

– Tillfälle

Vid pågående affärsförhandlingar med mottagarens arbets- eller uppdragsgivare eller under pågående uppdrag ska särskild försiktighet iakttas. En förmån som annars skulle vara tillåten kan vid sådant tillfälle bedömas som otillåten.

Exempel: Det är inte tillåtet att under pågående avtalsförhandling bjuda motparten på julbord eller annat liknande evenemang.

– Affärsmässighet

Förmåner ska ha en affärsmässig relevans. Evenemang ska ha koppling till den inbjudande organisationens verksamhet och får inte vara extravaganta. Inbjudan av medföljande, t.ex. anhörig eller vän, gör att den affärsmässiga kopplingen riskeras.

Exempel: Det är som utgångspunkt tillåtet att förena ett i övrigt affärsmässigt evenemang med en nöjesbetonad del, förutsatt att den affärsmässiga delen är det centrala.

3. Redovisning av förmåner som riskerar att strida mot koden

Om arbets- eller uppdragstagaren bedömer att en erbjuden förmån kan vara otillåten, ska denne antingen avvisa den direkt eller - innan den tas emot - hänskjuta bedömningen till närmaste chef eller annan som företaget har hänvisat till.

I oförutsedda eller plötsligt uppkomna situationer, där ett omedelbart avböjande av förmånen inte kan komma i fråga då det skulle kunna skada arbets- eller uppdragsgivarens relation till den som erbjuder förmånen eller medföra en säkerhetsrisk för arbets- eller uppdragstagaren, ska mottagaren så snart omständigheterna tillåter redovisa förmånen för arbets- eller uppdragsgivaren.

E. Mellanhänder

1. Vad handlar det om?

Om mellanhänder inte väljs noggrant eller om de agerar otillåtet, kan det medföra väsentlig skada för företagets goodwill och föranleda rättsligt ansvar för företaget och dess företrädare. Enligt både svensk och utländsk mutlagstiftning ställs krav på att företag gör tillräckliga kontroller av de personer och organisationer som ska företräda företaget. Om kontrollerna inte är tillräckligt långtgående, kan ansvar för brott uppkomma, enligt svensk lag för vårdslös finansiering av mutbrott.

Allmänt sett bör företaget skaffa sig en god kännedom om alla personer och organisationer företaget ska samarbeta med.

I korthet handlar det om att skaffa sig kännedom om mellanhänderna för att med tillräcklig säkerhet kunna svara på följande frågor:

- Vem är mellanhanden och vilka bakomliggande intressen företräder mellanhanden?
- Kan jag lita på att mellanhanden inte agerar korrupt?

2. Vilka utgör mellanhänder?

Med mellanhand avses i denna kod någon som ett företag har utsett att företräda företaget för viss angelägenhet och till vilken företaget tillhandahåller pengar eller andra tillgångar. Det avgörande är inte vad mellanhanden kallas utan mellanhandens faktiska funktion. Mellanhänder kan vara t.ex. agenter, konsulter, ombud, dotterbolag, mäklare eller affärsförmedlare.

Riktlinjerna i denna kod bör också användas som ledning vid kontroll för undvikande av korruptionsrisker förknippade med andra tredjeparter som företag arbetar med eller använder sig av, t.ex. leverantörer.

3. System för utvärdering

3.1 Systemets utformning

Företag ska ha system för att utvärdera mellanhänder. Systemet ska vara anpassat till företagets storlek och ägarförhållanden, den verksamhet som bedrivs och risken för korruption.

Det ska inom ett företag finnas en särskilt utsedd person som har ansvar för att ett sådant system finns och att riskbedömningar, kontroller och utvärderingar genomförs i enlighet med denna kod. Företag ska säkerställa att den utsedda personen har tillgång till tillräcklig kunskap för detta ansvar.

Systemet ska säkerställa att företaget

1. riskbedömer (se 3.2),
2. kontrollerar (se 3.3), och
3. utvärderar mellanhänder (se 3.4).

Systemet ska säkerställa att företag inför anlitande av en ny mellanhand genomför den kontroll som krävs efter en riskbedömning. I det system som företag ska ha för utvärdering av mellanhänder ska det ingå rutiner som säkerställer att förnyad utvärdering sker återkommande av befintliga mellanhänder utifrån risknivå samt om det sker en väsentlig förändring avseende mellanhanden i t.ex. ägarstruktur eller om det uppkommer misstankar om oegentligheter kopplade till mellanhanden.

Exempel: Ett företag har sedan länge arbetat med en mellanhand i ett annat land. Enligt medierapportering har myndigheter i landet inlett utredningar om misstänkt korruption inom den bransch som mellanhanden är verksam i. Företaget bör genomföra en förnyad utvärdering av mellanhanden.

Företag ska ha en eskaleringsrutin för hur mellanhänder kontrolleras och utvärderas, beroende på vilken risk som mellanhanden utgör. Hur detta ansvar fördelas avgör företaget, men följande riktlinjer kan användas.

Låg risk: Kontroll och utvärdering sker i den operativa verksamheten.

Mellanrisk: Kontroll och utvärdering sker med stöd av i förekommande fall compliance-ansvarig eller en person i organisationen utanför den operativa verksamheten som har särskilt ansvar för systemet för mellanhänder. Det är viktigt att en sådan person inte har något eget intresse kopplat till anlitande av mellanhanden eller styrs av operativa mål såsom försäljningsmål.

Hög risk: Vid hög risk bör i de flesta fall någon på högre nivå än i mellanriskfallen involveras. I situationer med särskilt hög risk, t.ex. stora kontraktssummor på högkorrupta marknader, kan utvärderingen behöva göras på styrelsenivå.

De åtgärder och kontroller som genomförs ska ske självständigt och dokumenteras. Med självständigt menas att företag ska göra en egen bedömning av sådana uppgifter som inhämtas från någon utomstående.

För många företag finns skyldighet att genomföra kontroller enligt lagstiftning om penningtvätt och motverkande av terrorfinansiering. Sådana kontroller kan användas även i detta syfte.

3.2 Riskbedömning

3.2.1 Olika risker

Avgörande för kontrollens omfattning är vilken risk som mellanhanden utgör ur ett korruptionsperspektiv. För mellanhänder med låg risk krävs ofta ingen eller begränsad kontroll, medan mellanhänder med hög risk kan behöva kontrolleras ingående. Risken avgörs utifrån flera faktorer. De viktigaste att ta hänsyn till är listade nedan. Till dessa kommer företagets kännedom om och erfarenheter av en viss mellanhand.

3.2.2 Landrisker

Det är en riskfaktor om mellanhanden verkar eller är registrerad i ett land med förhöjd landrisk.

Följande utgör riskfaktorer:

- Mellanhanden verkar eller är registrerad i ett korruptionsutsatt land. Är en mellanhand registrerad eller verksam i ett land som enligt Transparency Internationals korruptionsperceptionsindex har en poäng understigande 50, ska anlitande av mellanhanden alltid föregås av en fördjupad kontroll.
- Det finns krav i den lokala jurisdiktionen att t.ex. anlita lokala agenter för genomförande av affärstransaktioner.

Det kan också vara en riskfaktor om mellanhanden verkar eller är registrerad i ett land som har sträng banksekretess eller svårgenomträngliga skatteredovisningssystem.

Verktyg: Ledning för att bedöma landrisker kan hämtas från OECD:s rapporter avseende olika länders implementering av OECD:s konvention om bekämpande av bestickning av utländska offentliga tjänstemän i internationella affärs-förbindelser, Tax Justice Network's Financial Secrecy Index och förteckningar över länder som är föremål för finansiella eller internationella sanktioner. Även Utrikesdepartementets landrapporter om mänskliga rättigheter, demokrati och rättsstatens principer samt kontakt med den lokala svenska ambassaden kan användas vid bedömning av landrisker.

3.2.3 Branschrisker

Det är en riskfaktor om mellanhanden verkar i en särskilt riskutsatt bransch. Branscher som präglas av en stor andel offentlig upphandling, krav på tillstånd för att utföra verksamhet eller många myndighetskontakter för att utföra verksamheten är generellt mer riskutsatta. Vilka branscher som är särskilt riskutsatta kan variera. Har det t.ex. nyligen förekommit medierapportering om korruptionsskandaler inom en viss bransch antyder det att korruptionsrisken i den branschen är förhöjd.

Verktyg: Verktyg som kan användas för att bedöma branschrisker är IMM:s rättsfallssamling och rättsfallsbank, medierapportering och Transparency Internationals Bribes Payer Index Report.

3.2.4 Val av mellanhand

Hur mellanhanden har valts påverkar riskbedömningen. Det är en riskfaktor om mellanhanden är rekommenderad av en kund eller av en beslutsfattare i ett offentligt organ eller om det som kvalificerar mellanhanden är dennes inflytande på eller nära relation till beslutsfattare i ett offentligt organ.

3.2.5 Kontraktssumma, kontraktstyp och kompensationsstruktur

Kontraktssumma, kontraktstyp och kompensationsstruktur kan samtliga utgöra riskfaktorer. Detta gäller både för kontrakt med mellanhanden och kontrakt som med mellanhandens förmedling ska ingås med annan part. Nedan följer exempel på omständigheter som man särskilt behöver vara uppmärksam på.

- Kontrakt av stor betydelse, t.ex. långvariga kontrakt och/eller kontrakt med en hög kontraktssumma.
- Mellanhanden verkar eller är registrerad i ett annat land än det där uppdraget ska genomföras.
- Mellanhanden ska ges långtgående befogenhet att agera för företagets räkning.
- Mellanhanden ska bistå i samband med offentliga upphandlingar eller i kontakter med offentliga tjänstemän.
- Mellanhandens ersättning är prestationsbaserad.
- Mellanhanden ska erhålla pengar i förskott.
- Mellanhanden önskar att betalning ska ske till annan part, kontant eller till ett annat land än det där parten verkar.
- Mellanhanden kräver ovanligt stor ersättning i förhållande till det arbete som ska utföras.
- Försäljning av företagets produkter/tjänster utgör, eller kommer att utgöra, en stor del av mellanhandens verksamhet.

3.2.6 Koppling till offentliga tjänstemän eller statligt ägda företag

Det är en riskfaktor om mellanhanden är eller ägs, helt eller delvis, av en offentlig tjänsteman eller ett statligt ägt företag alternativt har nära kopplingar till en offentlig tjänsteman.

3.2.7 Riskkategorisering

Mot bakgrund av de olika faktorerna för att bedöma risk kan mellanhänder kategoriseras utifrån risknivå: låg, mellan eller hög. Företag kan använda sig t.ex. av poängsättning av de olika riskfaktorerna för att skapa system för riskkategorisering av mellanhänder. Risknivån avgör sedan den nivå av kontroll som krävs avseende mellanhanden.

Riskbedömningen måste alltid ske efter en avvägning i det enskilda fallet utifrån framkomna riskfaktorer och företagets egen kännedom om mellanhanden.

Exempel 1: Ett företag ska ingå ett samarbetsavtal med en mellanhand i Sverige (lågriskland). Värdet av samarbetsavtalet är lågt (låg risk) och mellanhanden är inte verksam i en särskilt riskutsatt bransch (låg risk). Någon fördjupad kontroll behöver inte göras eller kan vara begränsad.

Exempel 2: Ett företag ska anlita en agent och avtalet föreskriver en för agenten hög provision (hög risk) i ett enligt Transparency Internationals index lågkorrupt land (låg risk). Kontraktsvärdet är inte särskilt högt och agenten har stor annan verksamhet (låg risk). Mot bakgrund av att agentavtalets utformning medför en hög risk behöver en fördjupad kontroll göras för att kontrollera att det inte finns några varningsflaggor som indikerar korruptionsrisker avseende agenten. Eftersom övriga riskfaktorer indikerar låg risk kan mellanhanden klassificeras som mellanrisk, vilket påverkar omfattningen av den fördjupade kontroll som behöver göras.

3.3 Kontroll

3.3.1 Kontrollens syfte

Kontrollen ska ge svar på frågorna om det finns ett reellt behov att använda sig av en mellanhand och om det är försvarbart att använda sig av den tilltänkta mellanhanden. Genom kontrollen ska också klargöras varför en viss mellanhand har valts. Kontrollen ska vara proportionell i förhållande till den riskkategori (låg-mellan-hög) som mellanhanden enligt riskbedömningen har kategoriserats i.

Kontrollen ska i första hand ta sikte på mellanhanden, men det kan finnas anledning att kontrollera även fysiska personer kopplade till denne i fall då mellanhanden är en juridisk person. Möjligheten till behandling av sådan information kan i detta avseende begränsas av dataskyddslagstiftning. Det saknas för närvarande uttryckligt stöd i EU:s dataskyddsförordning och den kompletterande lagstiftning Sverige infört att behandla uppgifter om kriminell bakgrundshistorik för fysiska personer inom ramen för en utvärdering av korruptionsrisker.

Kontrollen ska avse följande delar i syfte att upptäcka eventuella varningsflaggor kopplade till mellanhanden. Utöver varningsflaggorna nedan kan det finnas andra omständigheter som behöver beaktas vid utvärderingen av mellanhanden.

Verktyg: För genomförandet av kontrollen kan olika källor användas:

- Information direkt från mellanhanden genom frågeformulär och vid behov intervjuer med utvalda personer hos mellanhanden och platsbesök hos denne.
- Information genom sökningar i offentliga register och via internet.
- Information från referenser, t.ex. andra företag som har använt sig av mellanhanden eller har erfarenhet från aktuellt geografiskt område.
- Expertis ”på plats” som kan genomföra självständiga utredningar.
- Information från den egna organisationen om skälen för val av mellanhand och kännedom om denne.

3.3.2 Identitet

Det är grundläggande att veta med vem samarbetet avser och mellanhandens identitet behöver säkerställas. I kontrollen ingår att ta reda på företagsnamn, organisationsnummer eller motsvarande, när mellanhanden grundades, mellanhandens ledning och styrelse, antal anställda och var mellanhanden är registrerad.

Varningsflaggor avseende identitet är:

- Mellanhanden är registrerad i ett annat land än det där denne är verksam.
- Kontaktpersonen hos mellanhanden är svår att identifiera.
- Mellanhanden har för få anställda i relation till det uppdrag som denne ska utföra.
- Mellanhanden är nyligen grundad.
- Mellanhanden har komplexa ägarstrukturer som ändras från tid till annan.

3.3.3 Verklig huvudman

Vissa aktörer ska utse verklig huvudman. Med verklig huvudman menas den eller de fysiska personer som ytterst är ägare till eller kontrollerar en organisation. Den verkliga huvudmannen kan också utgöras av den eller de fysiska personer som tjänar på att någon annan agerar åt dem. Utan information om verklig huvudman är det inte möjligt att säkerställa identiteten avseende den eller dem som företaget faktiskt samarbetar med. Kontrollen av verklig huvudman syftar också till att utreda eventuella kopplingar till offentliga tjänstemän eller politiskt exponerade personer.

Varningsflaggor avseende verklig huvudman kan vara:

- Verklig huvudman kan inte fastställas i de fall där verklig huvudman ska vara utsedd.
- Det är svårt att hitta verifierbar information om verklig huvudman.
- Mellanhanden är ovillig att lämna ut information om verklig huvudman.
- Offentliga tjänstemän eller politiskt exponerade personer utgör verkliga huvudmän.

Verktyg: Verklig huvudman kan kontrolleras på olika sätt. Samtliga EU-länder måste ha ett register över verkliga huvudmän. I Sverige är det Bolagsverket som registrerar verklig huvudman. Kontroll av verklig huvudman kan ske genom begäran om information direkt från mellanhanden att ge ut registrerings-dokumenten avseende företagen.

3.3.4 Finansiell bakgrund och ersättningsform

Ersättningsform och mellanhandens finansiella beroende av samarbetet kan utgöra riskfaktorer och mellanhandens finansiella bakgrund är därför relevant.

Senast fastställda och reviderade årsredovisning ska kontrolleras för följande varningsflaggor:

- Det tycks inte bedrivas faktisk verksamhet hos mellanhanden.
- Det finns noteringar om avvikelser i årsredovisningen eller annat som framstår som misstänksamt i förhållande till den verksamhet som mellanhanden bedriver.
- Det planerade anlitandet av mellanhanden är betydelsefullt för mellanhandens ekonomi.

Kontrollen ska också avse hur ersättningen till mellanhanden är utformad. Följande är varningsflaggor:

- Begärd ersättning avviker från marknadsstandard eller från vad företaget normalt ger i ersättning.
- Betalning begärs kontant eller som förskottsbetalning.
- Mellanhanden begär att betalning ska ske i ett annat land än det där uppdraget ska genomföras.

Se också avsnitt 3.2.5.

3.3.5 Inställning till korruption

Det har betydelse vilken inställning mellanhanden har till korruption. I kontrollen i denna del ingår också att ta reda på om mellanhanden har ett antikorruptionsprogram och hur det har implementerats.

Nedanstående är varningsflaggor:

- Mellanhanden är motvilligt inställd till kontrollen och/eller lämnar inte ut efterfrågad information.
- Mellanhanden vill inte godta garantiåtaganden om att inte agera korrupt eller godta att följa företagets eventuella uppförandekod för mellanhänder.
- Mellanhanden saknar antikorruptionsprogram eller har implementerat sitt antikorruptionsprogram bristfälligt.
- Mellanhanden saknar tydliga regler om användning av förmåner och/eller kunskapsnivån hos mellanhanden om korruptionsrisker och hur förmåner får användas är låg.

Ska mellanhanden i sin tur använda sig av underleverantörer i samarbetet är det viktigt att säkerställa att mellanhanden utvärderar dessa i korruptionshänseende samt att undersöka vilka avtalsvillkor som uppställs gentemot sådana underleverantörer. Brister i detta avseende utgör en varningsflagga.

3.3.6 Integritet och rykte

En del i kontrollen är att skaffa kunskap om det finns några varningsflaggor kopplade till mellanhandens tidigare agerande och integritet samt rykte.

Nedanstående är varningsflaggor:

- Mellanhanden är involverad i en juridisk process som rör mutbrottslighet eller annan finansiell brottslighet.
- Det finns indikationer på att mellanhanden har varit involverad i korrupta ageranden.
- Det förekommer i övrigt negativ information om mellanhanden i t.ex. medierapportering.

Verktyg: Kontroller kan genomföras genom direkta frågor till mellanhanden, genom sökningar på internet och genom användning av olika databaser och listor. Här kan kontroller göras mot bl.a. Världsbankens lista över uteslutna företag, European Bank List of Ineligible Firms, Europeiska utrikestjänstens konsoliderade lista över bl.a. företag som är föremål för EU:s sanktioner och lokala listor över sanktioner.

3.3.7 Kompetens

Det utgör en varningsflagga om mellanhanden saknar relevant branscherfarenhet eller kompetens att utföra det aktuella uppdraget. Detta kan indikera att det finns andra faktorer än affärsmässiga som gör att mellanhanden kommer i fråga. Brister i kompetens kan också ge upphov till misstankar om korruption. Kontrollen bör därför säkerställa att mellanhanden har relevant kompetens för uppdraget och referenser bör efterfrågas.

3.4 Utvärdering

Har den genomförda kontrollen inte resulterat i att någon varningsflagga eller annan omständighet har identifierats kan processen med att ingå avtal med mellanhanden fortsätta.

Identifieras varningsflaggor behöver en utvärdering göras av hur dessa ska hanteras och om de innebär att processen att ingå avtal med mellanhanden ska avbrytas eller om ytterligare åtgärder behöver vidtas för att minska risker kopplade till identifierade varningsflaggor.

Exempel 1: Ett företags utvärdering av en mellanhand reser en varningsflagga inom området ”inställning till korruption”, då mellanhanden saknar en policy mot mutor. För att hantera denna varningsflagga kräver företaget att mellanhanden ska följa den antikorruptionspolicy för mellanhänder som företaget har, företaget inkluderar ett garantiåtagande i avtalet att mellanhanden inte ska agera korrupt och företaget genomför en utbildning inom antikorruption med de nyckelaktörer hos mellanhanden som ska genomföra uppdraget. Varningsflaggan har på detta sätt kunnat hanteras.

Exempel 2: Ett företag har trots omfattande kontroller inte kunnat uppnå fullständig klarhet i vem som är verklig huvudman för en tilltänkt mellanhand. Väljer företaget att trots detta gå vidare med samarbetet finns förhöjd risk för straffrättsligt ansvar om mellanhanden senare agerar korrupt.

Företag ska använda sig av en mellanhand endast om företaget är rimligt säkert på att mellanhanden inte kommer att vare sig ge eller ta emot mutor.

F. Förvaltning av koden

Denna kod förvaltas av Institutet Mot Mutor.

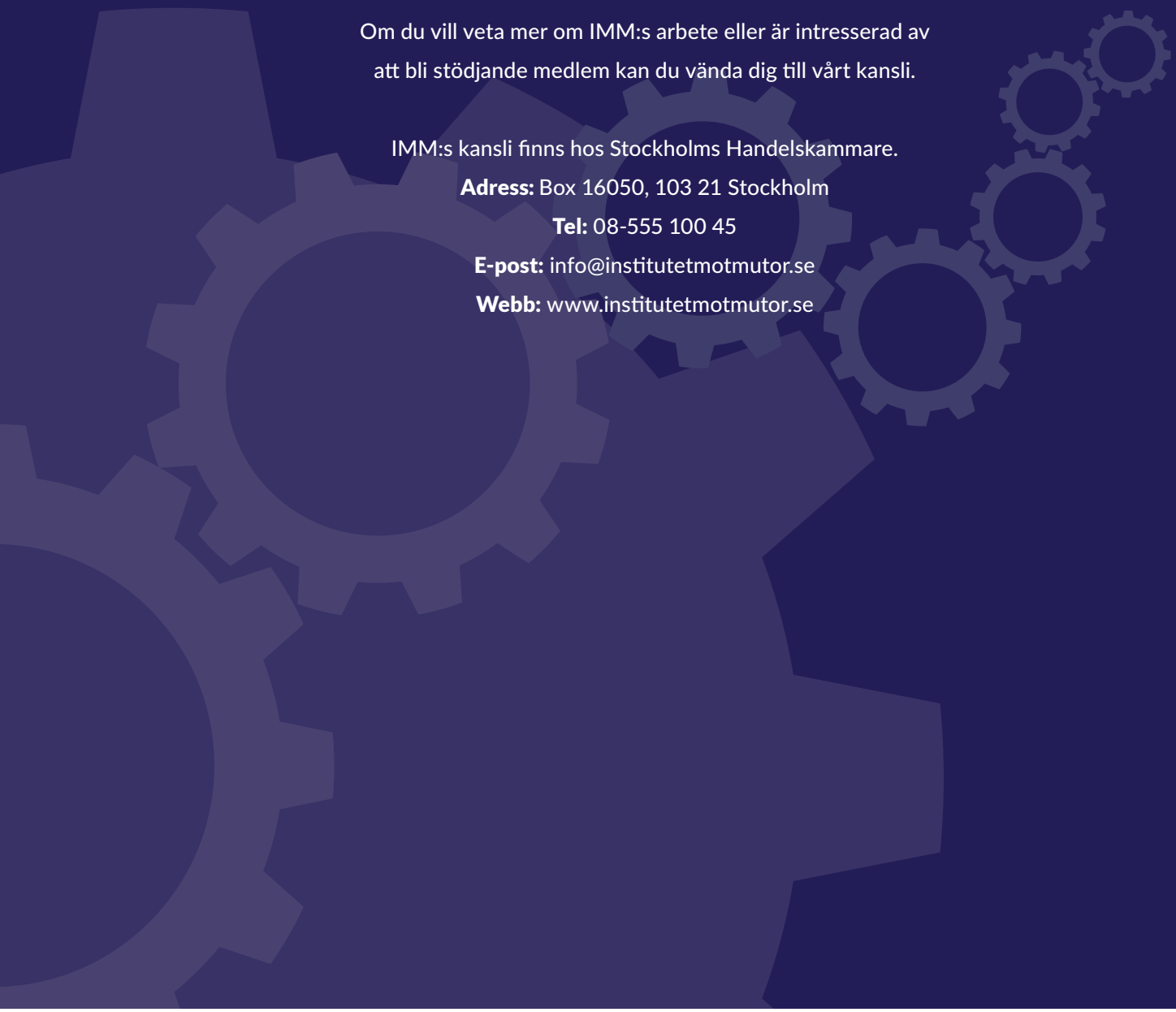
Koden fastställdes första gången av styrelsen för Institutet Mot Mutor den 31 augusti 2012 med verkan från den 1 september 2012. En reviderad kod publicerades den 9 december 2014. Den nu reviderade koden fastställdes av styrelsen den 10 juni 2020 och gäller från den 14 augusti 2020.

Frågor och beställning av material

För mer information om IMM:s skrifter och material,
besök www.institutetmotmutor.se.

Om du vill veta mer om IMM:s arbete eller är intresserad av
att bli stödjande medlem kan du vända dig till vårt kansli.

IMM:s kansli finns hos Stockholms Handelskammare.
Adress: Box 16050, 103 21 Stockholm
Tel: 08-555 100 45
E-post: info@institutetmotmutor.se
Webb: www.institutetmotmutor.se



IMM
INSTITUTET MOT MUTOR

RIKTLINJER FÖR TJÄNSTERESOR FÖR S:T ERIK FÖRSÄKRINGS AB

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa riktlinjer har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Riktlinjerna ska prövas årligen av styrelsen och revideras vid behov.

2 Syfte

Syftet med riktlinjerna är att säkerställa att de resor som sker av bolagets anställda sker trafiksäkert, miljöanpassat och kostnadseffektivt.

2.1 Kostnadseffektivt

Resor skall företas så kostnadseffektivt som möjligt med hänsyn till medarbetarnas individuella förutsättningar och behov, arbetseffektivitetens optimerande samt kostnader för transport, logi, arbetstid och restid. Den resande skall särskilt kontrollera om bolaget omfattas av upphandlade transporter eller bokningsföretag.

2.2 Miljöanpassat

Resor skall planeras och genomföras så att påverkan på den yttre miljön minimeras. Detta innebär att man i första hand skall överväga om det finns alternativ till fysisk resa, ex telefonmöten, videokonferens eller webbmöten. Först därefter skall resa planeras.

Vid resa skall färdmedel väljas i följande ordning:

1. Gå eller cykla
2. Kollektiva färdmedel
3. Bil (i första hand miljöbilar)
4. Flyg

2.3 Trafiksäkert

Resor skall ske på ett så trafiksäkert sätt som möjligt med hänsyn tagen till både resenären och medtrafikanter. Detta innebär bl. a att medarbetaren vi användande av cykel skall bära godkänd cykelhjälm och att bilar som används bör uppnå en säkerhet motsvarande fem stjärnor i EuroNCAP. Vidare får inte alla bolagets anställda färdas samtidigt i samma bil eller flyg.

3 Beslut om tjänste- eller studieresa samt deltagande i kurs eller konferens

Beslut om tjänste- eller studieresa, deltagande i kurs eller konferens fattas av VD. Styrelsens ordförande, eller vid dennes förhinder vice ordförande, skall dock godkänna VD:s tjänste- eller studieresa.

Sker tjänste- eller studieresa på styrelsens uppdrag skall beslut fattas i styrelsen. Vid brådskande fall kan beslut om resa på styrelsens uppdrag fattas av styrelsens ordförande, eller vid dennes förhinder, vice ordförande.

4 Återrapportering

Efter deltagande i kurs eller utbildning skall muntlig återrapportering ske till VD. Efter tjänste- eller studieresa skall skriftlig reserapport delges VD samt arkiveras. Efter tjänste- eller studieresa på styrelsens uppdrag skall skriftlig reserapport anmälas i styrelsen.

5 Ansvar

Var och en har ansvar för att det egna resandet följer dessa riktlinjer, avtal och andra regler, ex upphandlade taxiföretag/bokningföretag.

VD ansvarar för att:

- Informera medarbetarna om dessa riktlinjer
- Besluta om medarbetares tjänste- eller studieresa, deltagande i kurs eller konferens.

Styrelsens ordförande ansvarar för att:

- Godkänna VD:s studie/tjänste- eller konferensresa.

RIKTLINJER FÖR VÄRDERING AV TILLGÅNGAR OCH SKULDER SAMT BOLAGETS KAPITALBASER OCH FINANSIERINGSPLAN PÅ MEDELLÅNG SIKT

FASTSTÄLLD AV STYRELSEN 2022-05-23

1 Allmänt

Dessa instruktioner har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler”.

Syftet med instruktionerna är att korrekt värdera de tillgångar och skulder som används för solvensbalansberäkningar samt att klassificera och definiera bolagets kapitalbas.

Riktlinjerna revideras löpande och skall fastställas årligen eller vid materiella förändringar av styrelsen.

2 Ansvar

2.1 Styrelsen

Styrelsen ansvarar för att uppdatera dessa riktlinjer och att godkänna den värdering av tillgångar och skulder som sker.

2.2 VD

VD ansvarar för att ekonomiansvarig utför den värdering av tillgångar, skulder och kapitalbaser som måste ske och att kvalitetssäkring av detta skett med aktuarien och andra berörda funktioner.

Vidare ansvarar VD för att i sin ekonomiska rapportering till styrelsen vid styrelsemötena beskriva värderingen som använts.

2.3 Ekonomiansvarig

Ekonomiansvarig ansvarar för att den information som krävs för värdering och härledning finns tillgänglig, för värdering av bolagets tillgångar och skulder samt sammanställning och klassificering av kapitalbasposter.

2.4 Aktuarie

Aktuarien ansvarar för beräkning av de försäkringstekniska avsättningarna samt att vara andra funktioner behjälplig med råd och synpunkter angående värdering, samt att uttala sig om kvalitén på de data som används.

3 Värdering av tillgångar och skulder

3.1 Allmänt

Tillgångar och skulder ska värderas till verkligt värde, d.v.s. till det belopp som en tillgång eller skuld skulle kunna överlåtas i en transaktion mellan sinsemellan oberoende parter som har ett intresse av att transaktionen genomförs.

Vid värdering av skulder får inte hänsyn tas till S:t Erik Försäkrings egen kreditvärdighet.

Efter en inledande värdering ska denna kontrolleras och vid behov justeras vid beräkning av solvenskapitalkrav och försäkringstekniska avsättningar för rapportering och ORSA samt vid följande händelser:

A. Ny marknadsutveckling förändrar marknadsförhållandena.

B. Ny information blir tillgänglig.

C. Tidigare använd information inte längre finns tillgänglig.

D. Värderingstekniker förbättras.

Oberoende kontroll av värdering ska ske enligt 3.9 nedan.

3.2 Generella värderingsmetoder

Tillgångar och skulder värderas enligt följande:

A. Värdering ska ske i enlighet med de internationella redovisningsstandarder som antagits av kommissionen i förordning (EG) 1606/2002 – IFRS under förutsättning att de är förenliga med de principer som anges i artikel 75 i direktiv 2009/138/EG.

B. Individuella tillgångar ska värderas separat.

C. Tillgångar och skulder ska värderas under antagandet att bolaget fortsätter bedriva sin affär i nuvarande form.

3.3 Värderingshierarki

Verkligt värde beräknas i följande ordning:

A. Aktiva marknader enligt definition i IFRS.

B. Alternativa värderingsmetoder

3.3.1 Aktiva marknader

A. Noterade priser på en aktiv marknad.

B. Noterade priser på aktiv marknad för likartade tillgångar och skulder med nedan justeringar specifika för tillgången/skulden:

i. Tillgångens/skuldens plats
ii. Hur indata relaterar till poster jämförbara med tillgången/skulden
iii. Volymen och intensitetsnivån på de marknader där indata observeras.

3.3.2 Alternativa värderingsmetoder

Alternativa värderingsmetoder används då aktiva marknader inte finns.

Vid användning av alternativa värderingsmetoder ska bolagets minimera användningen av egna indata och maximera användningen av relevanta marknadspriser enligt nedan.

A. Noterade priser för identiska eller liknande tillgångar/skulder på icke aktiva marknader.

B. Andra indata än noterad priser, ex räntor, avkastningskurvor, implicit volatilitet och kreditspread.

C. Indata som inte är observerbara men stöds av observerbara marknadsdata.

D. Justeringar ska göras enligt 3.3.1 B.

E. Icke observerbara data ska återspegla de antaganden som marknadsaktörer skulle göra vid prissättning för tillgången/skulden, inbegripet antaganden om risk som följer av vald värderingsmetod och indata.

Bolagets valda värderingstekniker ska stämma med någon av följande metoder:

i. Marknadsmetod där relevant information genereras av marknadstransaktioner med identiska eller liknande tillgångar/skulder eller grupp därav.

ii. Avkastningsmetod där framtida belopp (ex. kassaflöden, intäkter eller kostnader) nuvärdesberäknas till ett belopp som återspeglar marknadens förväntningar.

iii. Kostnadsmetod/löpande återanskaffningsvärde som krävs för en tillgångs tjänstekapacitet. Priset avser vad en köpare skulle behöva betala för förvärv eller konstruktion av ersättningstillgång med jämförbar kvalité, justerat för inkurans.

3.4 Icke tillåtna värderingsmetoder

Bolaget får inte värdera en finansiell tillgång eller finansiell skuld till anskaffningsvärde eller ett upplupet anskaffningsvärde.

Bolaget får inte tillämpa värderingsmodeller som värderar till det som är lägst av det redovisade värdet och det verkliga värdet efter avdrag för försäljningskostnader.

Bolaget får inte värdera egendom, förvaltningsfastigheter eller materiella anläggningstillgångar med modeller där tillgångsvärdet fastställs som anskaffningsvärdet efter avdrag för avskrivningar och nedskrivningar.

3.5 Försäkringstekniska beräkningar

Värdering och beräkning av försäkringstekniska avsättningar framgår av ”Processbeskrivning – Beräkning av försäkringstekniska avsättningar-”.

3.6 Datakvalité

Vid värdering ska bolaget kontrollera att de data som används är fullständiga och lämpliga. Jämförelse ska göras mot indata vid tidigare värdering. Aktuarien ska uttala sig om kvalité på data och vid behov föreslå förbättringar. Vid kontroll/förnyad värdering ska utredning av datakvalité övervägas om data/datakällor ändrats.

A. Fullständighet innebär att data:

i. innehåller den mängd information som behövs för att kunna ligga till grund för värdering enligt vald metod, ex historik, transparens, risk som finns i metoden.

ii. Är konsistent över tid, dvs inte varierar i utförande

iii. Är fri från materiella felaktigheter (dvs inte innehåller ett fel som skulle påverka användarens beslutsprocess)

iv. Är registrerade i god tid och på konsekvent sätt

B. Lämplighet innebär att data:

i. Data ska stämma med syftet för vilket de används oavsett om de kommer från interna eller externa källor

ii. Insamlas, behandlas och tillämpas på ett transparent och konsekvent sätt över tid avseende källor, metod och personer

iii. Ska komma från källor som kan verifieras

C. Datakvalité ska bedömas med beaktande av följande information:

i. Källa (ex datasystem, person, statistik, Standard &Poors)

ii. Beskrivning av källa avseende historik och verifierbarhet

iii. Syftet med vald källa kopplat till vald värderingsmetod

iv. Bedömning av risk för ev materiella fel

v. Insamling – på vilket sätt och av vem

vi. Ev justeringar för att passa syftet

vii. Jämförelse med tidigare använd källa

viii. Aktuariens bedömning av datakvalité och ev synpunkter på förbättringar

3.7 **Rapportering**

Rapportering till styrelsen av värdering sker årligen samt vid byte av eller förändring av värderingsmetod.

3.8 **Dokumentation**

Värderingen ska dokumenteras elektroniskt samt i dokumentform hos ekonomifunktionen enligt följande:

<u>Ny eller justerad värdering</u>

A. Tid för värdering

B. Orsak till värdering /kontroll

C. Tillgång/skuld som värderas

D. Beskrivning av aktiv marknad eller metod alternativ värdering samt eventuella justeringar

E. Bedömning av data som använts i enlighet med 3.6.

F. Utlåtande från aktuarien över metod och datakvalité

G. Utförd kontroll av VD

H. Huruvida värderingen ska tillställas styrelsen eller ej (motivering)

Kontroll av värdering

Vid kontroll av värdering som inte föranleder justering noteras endast A , B och anledning till att justering inte sker , i den rapport eller beräkning som utförts.

3.9 **Kontroll och uppföljning**

Bolaget ska minst årligen samt vid behov (se 3.1) se över sina värderingsmetoder och strategier.

En oberoende översyn av bolagets värdering (annan än av bolaget anställd personal) ska utföras:

A. Regelbundet, dvs minst årligen.

B. Efter genomförandet av ny värderingsmetod

C. Vid större ändringar av existerande värderingsmetoder.

3.10 **Skillnad i värdering vid solvensbalansräkning och IFRS**

Följande skillnader finns mellan lagbegränsad IFRS-balansräkning (legal redovisning) och solvensbalansräkning och redovisas i syfte att kunna rapportera skillnaderna enligt gällande regelverk. Ansvaret för att omvärdering till solvensbalansräkningen utförs ligger hos ekonomifunktionen.

3.10.1 Goodwill

Goodwill ska värderas till 0.

3.10.2 Immateriella tillgångar

Immateriella tillgångar ska värderas till 0 såvida den inte kan säljas separat och försäkringsbolaget kan demonstrera att det finns ett värde för en identisk eller likadan tillgång i en aktiv marknad. Värdet ska i sådana fall beräknas enligt 3.3.

3.10.3 Försäkringstekniska avsättningar **och återförsäkrares andel av dessa**

I den legala redovisningen (lagbegränsad IFRS) består de försäkringstekniska avsättningarna av odiskonterade avsättningar avseende skadereserver, dels redan inträffade fastställda skadereserver samt en statistisk skadereserv (IBNR). De försäkringstekniska avsättningarna består även av en premiereserv som motsvarar den ännu ej intjänade/kostnadsförda premien i enlighet med en linjär avskrivning (pro rata temporis).

I Solvens II ska försäkringsföretag göra försäkringstekniska avsättningar för sina åtaganden med anledning av ingångna försäkringsavtal. Detta innebär att de försäkringstekniska avsättningarna i den legala redovisiningen har ersatts av en bästa skattning av samtliga kassaflöden som rör den försäkringstekniska verksamheten. Detta innebär även att fordringar och skulder som avser försäkringstekniska poster skall inkluderas i denna bästa skattning i solvensbalansräkningen. Värdet av de försäkringstekniska avsättningarna i solvensbalansräkningen ska motsvara det aktuella belopp som bolaget skulle vara tvungna att betala om de omedelbart skulle föra över sina försäkrings- och återförsäkringsförpliktelser till ett annat försäkrings- eller återförsäkringsföretag, som är oberoende och som har intresse av att transaktionen genomförs. Detta inkluderar därför en riskmarginal som ska motsvara belopp som motparten kan förväntas kräva för att ta över och uppfylla försäkrings- och återförsäkringsförpliktelserna. Värderingen görs enligt bolagets ”Processbeskrivning – Beräkning av försäkringstekniska avsättningar-”.

3.10.4 Fordringar och skulder avseende direkt försäkring och återförsäkring

Försäkringstekniska fordringar och skulder som har förfallit till betalning skall inte tas upp i kassaflödet för försäkringstekniska avsättningar. Inför varje solvens 2-värdering bedöms riktigheten i det bokförda värdet avseende verkligt värde och eventuell förlustprövning görs i enlighet med IFRS 4.

3.10.5 Placeringstillgångar

Bolagets finansiella tillgångar under placeringstillgångar har klassificerats som låne- och kundfordringar i enlighet med IAS 39 och som värderats till upplupet anskaffningsvärde. Då det inte finns någon aktiv marknad för det lån och det koncernkonto som bolaget har till sitt moderbolag så använder sig bolaget av en kostnadsmetod/löpande återanskaffningsvärde för att bedöma verkligt värde (se 3.3.2 iii). Detta innebär att den upplupna räntan skall tas med i värderingen.

3.10.6 Fordringar

Finansiella tillgångar som klassificerats som låne- och kundfordringar i enlighet med IAS 39 och som värderats till upplupet anskaffningsvärde. När dessa tillförts ett värde som inte motsvarar verkligt värde ska dessa omvärderas till verkligt värde i solvensbalansräkningen. Bolagets finansiella tillgångar har generellt sett kort löptid vilket medför att bokfört värde är en god approximation av verkligt värde.

3.10.7 Uppskjuten skatt

Uppskjuten skatt ska som grundprincip värderas enligt IFRS-regelverket (IAS 12) såvida inte den uppskjutna skatten hänför sig till underskottsavdrag eller andra framtida skattemässiga avdrag (med undantag för uppskjutna skattefordringar). Värdering ska i sådana fall ske på basis av skillnaden mellan:

A. Värdena av tillgångar och skulder i solvensbalansräkningen

B. Värdena av tillgångar och skulder i skattebalansräkningen

Ett positivt belopp av uppskjuten skattefordran ska enbart tas upp till ett positivt värde om det är sannolikt att avdragen kan avräknas mot överskott vid framtida beskattning med hänsyn tagen till rättsliga krav om tidsfrister för utnyttjande av dessa (enligt gällande regelverk har bolaget enbart sex beskattningsår på sig att utnyttja en skattefordran).

3.10.8 Materiella anläggningstillgångar

Materiella anläggningstillgångar som inte värderas till verkligt värde i IFRS ska omvärderas till marknadsvärde. I bolaget uppskattas detta inte beröra någon post i dagsläget.

3.10.9 Förutbetalda anskaffningskostnader

Förutbetalda anskaffningskostnader värderas till 0 i solvensbalansräkningen.

3.10.10 Obeskattade reserver (Säkerhetsreserven)

I solvensregelverket är säkerhetsreserven en del av eget kapital och tas inte upp i balansräkningen bland tillgångar och skulder. Om bolaget gör bedömningen att en uppskjuten skatteskuld föreligger för säkerhetsreserven på grund av framtida upplösning som inte möter ett underskott ska en sådan redovisas i Solvens 2-balansräkningen. En sådan skuldföring innebär därmed att avstämningsreservsposten i eget kapital minskar med motsvarande belopp och därmed även värderingen av säkerhetsreserven.

3.10.11 Skulder

Finansiella skulder som värderats till upplupet anskaffningsvärde i enlighet med IAS 39. Då dessa tillförts ett värde som inte motsvarar verkligt värde ska dessa omvärderas till verkligt värde i solvensbalansräkningen. Bolagets finansiella skulder har generellt en kort löptid vilket medför att bokfört värde är en god approximation av verkligt värde.

4 Kapitalbasposter

Bolaget ska fastställa, klassificera och bedöma medräkningsbarhet av det kapital som används för att täcka solvenskapitalkravet och minimikapitalkravet i enlighet med SII-direktivet kapitel VI, avsnitt 3 och underliggande förordning och riktlinjer.

4.1 Kapitalbasmedel

Kapitalbasmedel omfattar summan av primärkapital och tilläggskapital.

Primärkapitalet består av den positiva skillnaden mellan tillgångar och skulder, värderad enligt kapitel VI i SII-direktivet, samt efterställda skulder.

Tilläggskapital består av poster utöver de i primärkapitalet och som kan krävas in för att täcka förluster. Tilläggskapitalet upptas således inte i solvensbalansräkningen och förhandsgranskas av Finansinspektionen innan de kan användas i kapitalbasen.

4.2 Klassificering av kapitalbasposter S:t Erik Försäkrings AB

Följande klassificeringar har gjorts efter SII-direktivet (2009/168/EG), SII-förordningen (2015/35) och Riktlinjer för klassificering av kapitalbasen (14/168) samt nationell lagstiftning i försäkringsrörelselagen och författningar från Finansinspektionen.

Övergripande för klassificeringen gäller följande ur artikel 93 (SII-direktivet):

Posterna i kapitalbasen ska delas upp på tre nivåer. Klassificeringen av dessa poster ska vara beroende av om de är primärkapital eller tilläggskapital och i vilken omfattning de uppfyller följande egenskaper:

A. *Posten är tillgänglig, eller kan infordras på begäran, för att i sin helhet förlustabsorbera, såväl i den löpande verksamheten som vid likvidation (permanent tillgänglighet).*
B. *Vid likvidation är postens hela belopp tillgängligt för att täcka förluster och posten får inte återbetalas till innehavaren förrän alla andra förpliktelser, däribland försäkrings- och återförsäkringsförpliktelser gentemot försäkringstagare och ersättningsberättigade enligt försäkrings- och återförsäkringsavtal, har uppfyllts (efterställdhet).*

Enligt 7 kap. försäkringsrörelselagen (2010:2043) ska bolaget ta hänsyn till både nuvarande och framtida förhållanden när det bedömer en posts förlusttäckningsförmåga och efterställdhet.

4.2.1 Aktiekapital

Bolagets aktiekapital har inga begränsningar och är i enlighet med SII-förordningen klassas som primärkapital nivå 1 (artikel 69 a-i). Posten finns med i förteckningen (artikel 69) och uppfyller särdragen som specificeras i artikel 71 och främst så är det är ett inbetalt stamaktiekapital och den prioriteras efter alla andra fordringar i händelse av likvidationsförfaranden för företaget. Bolaget har full flexibilitet i fråga om utskiftning (det finns inga begränsningar i hur utskifte skall ske).

Ägaren är Stockholm Stadshus AB och aktiekapitalet består av 100 000 A-aktier till ett värde av 100 000 000 kr.

4.2.2 Avstämningsreserv

Avstämningsreserven motsvarar den sammanlagda skillnaden mellan tillgångar och skulder minskat med aktiekapital enligt ovan. I enlighet med punkt 1.5 i Riktlinjer för klassificering av kapitalbasen (14/168) skall balanserade vinstmedel vara en del av avstämningsreserven. Utöver detta skall även förutsebara utdelningar, utskiftningar och avgifter reduceras från posten. Avseende förutsebara kostnader bör bolaget främst ta hänsyn till förutsebara och inte redan redovisade skattebelopp.

Fastställandet av huruvida och i vilken omfattning avstämningsreserven uppvisar de särdrag som anges i artikel 71 ska inte innebära en bedömning av särdragen hos de tillgångar och skulder som ingår i beräkningen av hur mycket tillgångarna överstiger skulderna eller de underliggande posterna i företagens finansiella redovisning (SII-förordningen artikel 70.3).

I enlighet med bolagets bolagsordning står bolagets vinst till årsstämmans förfogande där ägaren har rätt att besluta om disponering. Eventuella förutsebara utdelningar skall reduceras i avstämningsreserven, och bolaget bör betrakta utdelningen som förutsebar senast när den är deklarerad eller godkänd av styrelsen, oavsett krav på att det ska godkännas vid årsstämman.

I enlighet med instruktioner från Finansinspektionen skall bolagets säkerhetsreserv vara en del av bolagets avstämningsreserv. Bolaget ska i samband med sin Solvens 2-rapportering göra en bedömning om uppskjuten skatt kan anses föreligga för säkerhetsreserven. Denna bedömning ska göras utifrån de faktiska omständigheter som gäller för det enskilda företaget. Hänsyn ska tas till faktorer såsom eventuella förlustsituationer i det tekniska resultatet för företaget, sannolikheten att företaget kan behöva göra en tvångsmässig upplösning av säkerhetsreserven samt andra omständigheter som skulle kunna påverka en eventuell beskattning av en upplösning. Det är här viktigt att göra en bedömning av hela bolagets skattemässiga situation.

Om bolaget gör bedömningen att en uppskjuten skatteskuld föreligger för säkerhetsreserven ska en sådan redovisas i Solvens 2-balansräkningen, i annat fall redovisas inte någon uppskjuten skatteskuld hänförlig till säkerhetsreserven. En sådan skuldföring innebär även att avstämningsreserven minskar med motsvarande belopp.

Avstämningsreserven klassas som primärkapital nivå 1 i enlighet med SII-förordningen (artikel 69 a-vi). Värderingen av bolagets tillgångar och skulder, inklusive bolagets försäkringstekniska avsättningar, görs i enlighet med bolagets riktlinjer för ”värdering av tillgångar och skulder samt bolagets kapitalbaser och finansieringsplan på medellång sikt”. Där framgår även skillnaden i värdering mellan den legala redovisningen och Solvens II-regelverket (kapitel VI i SII-direktivet).

4.3 Medräkningsbarhet

Beroende på kapitalets kvalité gäller enligt nuvarande regelverk gränsvärden för medräkningsbara kapitalbasmedel.

Medräkningsbara kapitalbasmedel ska täcka solvenskapitalkravet (SCR) och medräkningsbart primärkapital ska täcka minimikapitalkravet (MCR).

4.3.1 Gränsvärden för SCR

Följande kvantitativa gränsvärden gäller för medräkningsbara kapitalmedel avseende SCR:

- Nivå 1-poster ska utgöra minst 50 % SCR
- Nivå 3-poster ska utgöra mindre än 15 % av SCR
- Summan av nivå 2- och 3-poster får inte överstiga 50 % av SCR

Inom dessa ramar gäller att följande primärkapitalposter måste understiga 20 % av totalt belopp avseende nivå 1-poster:

- Efterställda skulder
- Poster inom nivå 1 som resulterar av övergångsbestämmelserna.

4.3.2 Gränsvärden MCR

Följande kvantitativa gränsvärden gäller för medräkningsbara kapitalmedel avseende MCR:

- Nivå 1-poster ska vara minst 80 % av MCR
- Nivå 2-poster ska vara mindre än 20 % av MCR.

Inom dessa ramar ska summan av följande primärkapitalposter utgöra mindre än 20 % av beloppet för nivå 1 poster:

- Efterställda skulder
- Nivå 1-poster angivna ramarna

4.4 **Fastställande av kapitalbasmedel.**

Ekonomifunktionen ansvarar för att klassa kapitalbasmedel samt att kontrollera deras medräkningsbarhet enligt gällande rätt och därmed:

A. Klassificera kapitalbasposter före och vid utgivningstidpunkten samt:
    i. Inför beräkning av SCR/MCR
    ii. Vid legala förändringar
    iii. Vid förslag på aktieutdelning.

B. Kontrollera att kapitalbasposter inte belastats till följd av avtal eller anknutna transaktioner på ett sätt som påverkar dess medräkningsbarhet.

C. Säkerställa att avtalsvillkoren för kapitalbasposter uppfyller kriterierna för att kunna genomföra en klassificering och kontrollera postens medräkningsbarhet.

D. Tillse att eventuella förslag på aktieutdelningar beaktas vid bedömningen av kapitalsituationen.

E. I god tid meddela VD och styrelse om behov av tilläggskapital så att ägaren kan tillskjuta medel enligt finansieringsplanen på medellång sikt nedan.

4.5 **Kontroll**

VD kontrollerar att fastställande och bedömning av kapitalbasposter sker i samband med beräkning av SCR/MCR, förslag till aktieutdelning m.m.

4.6 **Rapportering**

Ekonomifunktionen rapporterar samtliga bedömningar till VD, riskhanteringsfunktionen samt i sin ekonomiska redovisning till styrelsen.

5 Finansieringsplan på medellång sikt

Bolagets finansieringsplan på medellång sikt utgöras av den flerårsbudget som fastställs av styrelsen med beaktande av resultatet av kapitalbehovet i ORSA samt ekonomifunktionens bedömning av kapitalbasposternas medräkningsbarhet över sikt och eventuella aktieutdelningar.

Således påverkas finansieringsplanen av en kapitalbasposts förväntade medräkningsbarhet i framtiden. Om variationer förväntas ske i en kapitalbaspost med anledning av dessa inneboend kvalité (ex lagkrav, avtalsvillkor, utskiftningar) kan detta påverka finansierings-planen.

5.1 **Tilläggskapital**

Behov av tillskottskapital sker vid behov genom att ägaren (tillika försäkringstagaren) på begäran tillskjuter det kapital som behövs. Kontakt tas i god tid med Stockholm kommuns finansavdelning samt Stockholms Stadshus AB. Bedömning av tilläggskapitalets medräkningsbarhet skall göras i samband med att kapitaltillskottet sker. Då tillskjutet kapital kommer att innebära ett aktieägartillskott när det betalats in så kommer bolaget att klassa det som aktiekapital och därmed primärkapital nivå 1. Därmed kan bolaget använda det till 100 % för att täcka SCR när det infordrats. Till dess måste bolaget ansöka hos Finansinspektionen om ett godkännande på att garantin hos ägaren kan klassas som nivå 2 i tilläggskapital om bolaget vill använda det som kapitalbaspost.

Återbäringsprinciper

Dessa principer för återbäring har upprättats i enlighet med de rättsregler som anges i dokumentet ”Register över rättsregler” och har antagen av styrelsen för S:t Erik Försäkring den 23 maj 2022.

S:t Erik Försäkring har möjlighet att ge återbäring till sina försäkringstagare i enlighet med av styrelsen antagna försäkringstekniska riktlinjer och under de förutsättningar som redovisas nedan.

En försäkringsrörelse visar normalt stora fluktuationer beroende på olika skadefall under åren. Styrelsen för S:t Erik Försäkring har mot denna bakgrund beslutat att hålla bolaget så välkonsoliderat som möjligt. Det innebär att de försäkringstekniska avsättningarna ska ske enligt de principer som anges i bolagets försäkringstekniska riktlinjer. Härutöver ska de obeskattade reserverna årligen vara till fullo utnyttjade. Om S:t Erik Försäkring efter dessa nämnda avsättningar har ett överskott i försäkringsrörelsen kan styrelsen inför årsbokslutet besluta om att återbäring kan utges till försäkringstagarna.

Storleken på den totala återbäringen för samtliga försäkringstagare beslutas av styrelsen för S:t Erik Försäkring. Återbäringen fördelas på respektive försäkringstagare i förhållande till skadeprocenten. Försäkringstagarens maximala ersättning begränsas dock till att ersättning inte får överstiga S:t Erik Försäkrings intäkter minus kostnad för respektive kund. Den maximala ersättningen beräknas utifrån inträffade skador minus premie för egen räkning per kund och försäkringsår.

Skadeprocenten beräknas genom att dividera beloppet för inträffade skador under försäkringsperioden med av S:t Erik Försäkring intjänad premie för egen räkning för motsvarande period.

Återbäringen betalas ut tidigast efter ordinarie bolagsstämma och senast den 1 oktober året efter försäkringsperioden.

Återbäringen kan lämnas enligt följande skala:

Skadeprocent	Återbärings-procent
0	20 %
1-10	15 %
11-20	12,5 %
21-30	10 %
31-40	7,5 %
41-50	5 %
51-	0 %