# Riktlinje för utlagd verksamhet

## 1 Om dokumentet

### 1.1 Bakgrund och syfte

Försäkrings AB Göta Lejon kan från tid till annan uppdra åt annan juridisk person att utföra bolagets försäkringsrörelse eller funktioner eller verksamheter som har ett naturligt samband med försäkringsrörelsen (outsourcing). Bolaget ansvarar dock alltjämt för den utlagda verksamheten och ska övervaka att leverantören uppfyller sina åtaganden

Dessa riktlinjer 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.

Enligt 10 kap. 19§ FRL (2010:2043) samt artikel 274.1 Solvens II- förordningen 2015/35 ska ett försäkringsbolag upprätta och följa styrdokument för bland annat verksamhet som omfattas av uppdragsavtal. Dessa riktlinjer syftar till att ange hur bolagets utlagda verksamhet ska genomföras och hanteras. VD kan med utgångspunkt från riktlinjerna utarbeta mera detaljerade instruktioner, anvisningar och rutiner om bolagets utlagda verksamhet.

### 1.2 Omfattning och avgränsningar

Riktlinjerna gäller för all verksamhet i bolaget som har eller ska läggas ut till annan leverantör och träder i kraft dagen för styrelsens fastställande. Styrelsen ska godkänna verksamhet som ska utföras på uppdragsavtal. Beslutet skall föregås av en riskanalys, vilket ska dokumenteras.

VD ansvarar för att berörda medarbetare i bolaget informeras om dessa riktlinjer. Det åligger därefter varje berörd medarbetare att se till att riktlinjerna tillämpas inom det egna ansvarsområdet.

### 1.3 Dokumentets beslutsordning

Riktlinjen ska fastställas och godkännas minst en gång per år även om inga ändringar beslutas. Ansvarig för uppdatering av riktlinjen är VD.

### 1.4 Efterlevnad

Alla medarbetare ansvarar för att denna riktlinje följs. Chefer i organisationen säkerställer att riktlinjen efterlevs och att kunskap om innehållet finns inom bolaget. Ansvarig för att granska verksamhetens efterlevnad är regelefterlevnadsfunktionen.

## 2 Ansvarsfördelning och beställarkompetens

### 2.1 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. 1.7.

VD ansvarar för följande.

* Att styrelsen erhåller en riskanalys enligt nedan samt att erforderliga avtal upprättas med extern part i enlighet med LOU, den delegerade förordningen 2015/35 samt, i tillämpliga fall, i enlighet med EIOPA:s riktlinjer för IKT respektive uppdragsavtal med molntjänstleverantörer.
* Att följa upp den verksamhet som utförs på uppdragsavtal samt att minst årligen rapportera utfallet av uppföljningen av utlagd verksamhet till styrelsen. VD:s ansvar för uppföljning kan delegeras.
* Att godkänna upphandlingsunderlag och tillställa detta till styrelsen för godkännande avseende kritiska och viktiga funktioner som ska outsourcas. Detta gäller vid varje upphandling och ej endast vid upphandling av ny leverantör.
* Att avtal tecknas för den utlagda verksamheten i enlighet med LOU och avsnitt 4.8 nedan.
* Att de som utför verksamheten på uppdragsavtal får del av och följer de riktlinjer och policys som antagits av styrelsen.
* Att Finansinspektionen informeras om uppdragsavtal enligt avsnitt 6 nedan.
* Att en överlämningsplan och/eller beredskapsplan aktualiseras om verksamhet eller funktion ska återtas till bolaget alt. läggas ut på annan leverantör.

Av VD delegerad ansvarig person för den outsourcade verksamheten ska, 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.

### 2.2 Beställarkompetens

Bolaget utvärderar beställarkompetens för anmälda personer till Finansinspektionen enligt Riktlinjen för Lämplighetsprövning såsom ansvarig för nyckelfunktion.

## 3 Kritiska och 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, se riktlinje 7.

Styrelsen har identifierat följande funktioner och aktiviteter som kritiska och viktiga:

* aktuariella tjänster,
* IT
* internrevision
* regelefterlevnad
* skadereglering
* försäkringshantering/försäkringssystem
* riskhantering

## 4 Behovs- och riskanalys

### 4.1 Behovsanalys

Innan bolaget lägger ut verksamhet eller funktion på en tjänsteleverantör ska bolaget se över behoven av detta. Sådana behov kan vara exempelvis

* lagkrav för bolagets verksamhet,
* kritisk/nödvändig för att bolaget ska kunna leverera sina tjänster, eller att
* inga interna resurser eller kompetens finns att tillgå.

### 4.2 Riskanalys

Riskanalys avseende potentiella tjänsteleverantörer ska genomföras av bolaget och ska, avseende kritiska eller viktiga funktioner, vara ett underlag för styrelsens beslut om att lägga ut verksamhet till annan. Vid förnyad outsourcing ska ny riskanalys genomföras om riskerna har ändrats.

Riskanalysen ska beskriva om en funktion eller aktivitet som omfattas av ett uppdragsavtal är en kritisk eller viktig funktion eller aktivitet baserat på om funktionen eller aktiviteten är nödvändig för företagets verksamhet, eftersom det utan funktionen eller aktiviteten inte skulle kunna tillhandahålla tjänster åt sina försäkringstagare.

Riskanalysen skall därutöver minst innehålla en beskrivning av hur minimikraven enligt nedan säkerställs och en värdering av risken att dessa inte nås för var och en av punkterna samt utvärdera molntjänster avseende informationssäkerhet och kontinuitetshantering för att undvika systemstörningar. (se checklista/utvärdering, separat bilaga)

### 4.3 Riskanalysprocess

**1. Behovsanalys & beslutsunderlag**

**2.** **Upprättande av avtal**

**3.** **Uppföljning & utvärdering**

**4.** **Utveckling eller avveckling**

1. VD alternativt beställaransvarig förmedlar resursbehov och beslutsunderlag för behandling av styrelsen. VD alt. beställaransvarig eller av VD delegerad ska tillse att en behovs- och riskanalys enligt Bilaga 1 - *Checklista inför tecknande av uppdragsavtal* inkluderas i beslutsunderlaget.
2. Vid upprättande av avtal kontrollerar VD, (alt genom delegering till kontrollfunktion eller tredje part), att avtalets formalia minst möter lagkraven.
3. Beställaransvarig, eller av VD delegerad person, för respektive uppdragstagare utför årlig uppföljning samt utvärdering av uppdraget samt av uppdragstagaren enligt separat dokument, se *Checklista vid uppföljning av utlagd verksamhet*.
4. Vid återtagande av uppdrag alternativt byte av tjänsteleverantör ska överlämningsplan aktualiseras och eller beredskapsplan samt nytt beslutsunderlag enligt punkt 1.

### 4.4 Verksamheter som idag bedrivs på uppdragsavtal

Verksamhet som idag bedrivs på uppdragsavtal är

* aktuariella tjänster
* IT
* internrevision
* regelefterlevnad
* riskhantering
* skadereglering

### 4.5 Krav som ska vara uppfyllda för att verksamhet ska få bedrivas av extern part genom uppdragsavtal

För att uppdrag ska få läggas ut på extern tjänsteleverantör krävs att leverantören uppfyller följande minimikrav:

* uppdragstagaren ska förstå bolagets verksamhet och behov
* inga intressekonflikter

Innan ett uppdragsavtal läggs ut på en tjänsteleverantör ska VD alt. beställaransvarig eller av VD delegerad person upprätta en behovs- och riskanalys innan avtal tecknas. Sådan behovs- och riskanalys ska utföras enligt Bilaga 1 – *Checklista inför tecknande av uppdragsavtal*. För att en verksamhet ska få läggas ut på uppdragsavtal krävs det att leverantören uppfyller kraven enligt ovan.

Kraven på leverantören beskrivs utförligare i artikel 274 Solvens II förordningen 2015/35, vilka alltid ska beaktas vid utläggning av funktioner eller verksamhet.

### 4.6 Molntjänster och IKT-tjänster

För utlagd verksamhet avseende molntjänster ska även EIOPA:s riktlinjer om uppdragsavtal med molntjänstleverantör, riktlinjerna 2, 6, 12 och 15 beaktas.

Bolaget ska identifiera om tjänsteleverantören anses tillämpa molntjänster enligt

a) Software as a Service (SaaS),

b) Infrastructure as a Service (IaaS), eller

c) Plattform as a Service (PaaS).

Vad dessa olika molntjänster innebär samt vilka moment som måste säkerställas och inkluderas i en riskanalys innan molntjänster läggs ut på en molntjänsteleverantör, finns angivna i bilaga 1 - *Checklista inför tecknande av uppdragsavtal*.

För IKT-tjänster ska EIOPA:s IKT riktlinjer, riktlinje 25, beaktas.

# 4.7 Uppdragsavtalets innehåll

I avtal med extern part skall åtminstone följande punkter regleras:

* parternas rättigheter och skyldigheter samt parternas ansvar,
* möjligheten att vidmakthålla gällande sekretesskydd,
* hantering av personuppgifter i enlighet med Dataskyddsförordningen,
* i tillämpliga fall, krav på personuppgiftsbiträdesavtal,
* riktlinjer för styrning, uppföljning och revidering av uppdraget,
* krav på leverantörens kompetens, kvalité och internkontroll,
* krav på beredskapsplan eller motsvarande samt test av beredskapsplan,
* krav på möjlighet för Finansinspektionen att bedriva tillsyn av den utlagda verksamheten på plats i leverantörens lokaler (detta inkluderar också att bolagets interna och externa revisorer får tillgång till uppgifter om den utlagda verksamheten),
* krav på information och rapportering,
* att leverantören skall ha riktlinjer avseende jäv och intressekonflikter och skall beskriva hur dessa kontrolleras,
* avtalstid och uppsägningstid,
* att leverantören har riktlinjer avseende rapportering av väsentliga händelser och kan beskriva hur dessa dokumenteras och rapporteras,
* ersättning, prisjustering, fakturering och betalningsvillkor,
* skatter och avgifter,
* när och hur uppdrag får läggas ut på underleverantörer,
* om tillämpligt, krav på försäkring,
* force majure,
* rättigheter till material,
* fel, förseningar och brister,
* överlåtelse av avtal, rättigheter och skyldigheter,
* leverantörens medverkan vid upphandling och återgång och behjälplighet med eventuell överföring av uppdraget och uppgifter till en ny leverantör eller bolaget, samt
* tillämplig lag och tvistefora.

Bolaget ska även ta hänsyn till om tjänsteleverantören tillämpar en lämplig etisk standard eller har en uppförandekod (Code of Conduct). Vidare ska avtalet, för det fall tjänsten avser en molntjänst eller en IKT-tjänst, anpassas för att överensstämma med EIOPA:s riktlinjer för sådana tjänster.

Avtalets innehåll ska innan signering stämmas av mot vid var tid gällande checklista (separat Exceldokument) för att säkerställa aktuella regelverkskrav.

## 5 Uppföljning av utlagd verksamhet

Bolagets VD ansvarar för att löpande följa upp den verksamhet som utförs på uppdragsavtal. VD:s ansvar för uppföljning kan delegeras.

Vid uppföljning av utlagd verksamhet ska Bilaga 2 – Checklista vid uppföljning av utlagd verksamhet tillämpas.

Bolagets VD ansvarar för att styrelsen erhåller information om den utlagda verksamheten enligt de utvärderingar som genomförs.

## 6 Anmälan till Finansinspektionen

Om bolaget avser att lägga ut en betydande del av sin tillståndspliktiga verksamhet, eller verksamhet som har ett naturligt samband med denna eller dess stödfunktioner på en extern part, skall bolaget anmäla detta i förväg till Finansinspektionen.

För utläggning av molntjänster ska EIOPAs:s riktlinjer för uppdragsavtal med molntjänstleverantörer, riktlinje 4, beaktas. I dessa anges vad som särskilt ska anges vid anmälan till Finansinspektionen avseende molntjänstleverantör.

**Ändringshistorik**

|  |  |  |
| --- | --- | --- |
| Version | Datum för ändring | Beskrivning av ändring |
| 1 |  | Första version |
| 2 | 2019-09-26 | Tillägg under punkt 1.6 Riskanalys, kritisk eller viktig funktion/aktivitet |
| 3 | 2020-06-16 | Rubrik 1.6 beställarkompetens. 1.7 riskanalys, 2.0 uppdragsavtalets innehåll |
| 4 | 2021-06-08 | Tillägg rubrik 1.7 samt utvärdera molntjänster avseende informationssäkerhet och kontinuitetshantering för att undvika systemstörningar. (se checklista/utvärdering, separat bilaga) |
| 5 | 2021-09-27 | Tillägg under punkten 2.0 i enlighet med Artikel 274 i 2015/35 Solvens II-förordningen |
| 6 | 2022-03-30 | Övergripande översyn och revidering i enlighet med artikel 274 Solvens II-förordningen och EIOPA:s riktlinjer för IKT och uppdragsavtal med molntjänstleverantörer. |