Försäkrings AB Göta Lejon

Bilaga 2 till Riktlinjer för utlagd verksamhet

Bilaga 2 - Checklista vid uppföljning av utlagd verksamhet

Nedan anges en checklista för uppföljning av Försäkrings AB Göta Lejons, nedan Bolaget, uppdragstagare beträffande kritiska eller viktiga operativa funktioner eller verksamheter.

Checklistan utgår från för Bolaget gällande regelverk. Detta hindrar dock inte att fler frågor ställs. Uppföljning och kontroller måste alltid anpassas efter vilken verksamhet som är utlagd.

**Avsnitt 1** - Gäller alla kritiska eller viktiga operativa funktioner eller verksamheter och uppföljning följer av försäkringsrörelselagen (FRL) och kommissionens delegerade förordning 2015/35 art. 274 (Solvens II-förordningen).

**Avsnitt 2** – Gäller för molntjänstleverantörer och uppföljning utgår från rekommendationer i Eiopas riktlinjer för molntjänster. Även avsnitt 1 ska följas upp.

**Avsnitt 3** – Gäller IKT-tjänster och uppföljning utgår från rekommendationer i Eiopas riktlinjer för IKT-tjänster. Även avsnitt 1 ska följas upp, och i tillämpliga fall, avsnitt 2 om det är en molntjänst som är utlagd.

# För att uppfylla krav i FRL och Solvens II-förordningen avser Bolaget att följa upp följande:

1. Att uppdragstagaren har den kunskap och de resurser samt erforderlig kompetens som krävs för att utföra uppdraget på ett tillfredställande sätt.

* *Har nyckelpersoner som arbetar i uppdraget tillräcklig kunskap och kompetens?*
* *Har uppdragstagaren beredskap i det fall en nyckelperson hos tjänsteleverantören säger upp sig, blir sjuk eller av annat skäl är frånvarande under en längre period?*
* *Om det tillkommit nyanställda hos uppdragstagaren som ska arbeta i uppdraget kan det övervägas att ta in CV och vandelsprövning vid behov.*

1. Att uppdragstagaren har de ekonomiska resurser som krävs för att korrekt och tillförlitligt utföra de tillkommande uppgifterna.

* *Vid behov kan årsredovisning eller annat underlag begäras in.*
* *Ligger tjänsteleverantören i en rättslig tvist? Kan detta föranleda några risker för Bolaget (ekonomiska, ryktesrisker, annat)?*

1. Att Bolaget och uppdragstagaren har rutiner för att hantera risker med den utlagda verksamheten.

* *Riskerna varierar beroende på vilken verksamhet som är utlagd. Några områden som kan vara av relevans att följa upp under denna punkt är följande:*
* *Har uppdragstagaren ändamålsenliga sekretessrutiner?*
* *Vilka rutiner finns för att säkerställa informationssäkerhet? Hur ofta gör uppdragstagaren backup?*

1. Att uppdragstagaren har långsiktig möjlighet att utföra uppdraget.

* *Här kan ekonomi och personal vara faktorer att beakta.*

1. Att det inte föreligger några intressekonflikter.

* *Skulle det ha identifierats några intressekonflikter är det viktigt att följa upp hur detta hanterats.*

1. Att uppdragstagaren samarbetar med Finansinspektionen, Bolaget och Bolagets externa revisor och att dessa på begäran får tillgång till all information om de funktioner och verksamheter som omfattas av uppdragsavtalet samt att alla har rätt att genomföra inspektioner på plats i uppdragstagarens lokaler.

* *Detta finns stadgat i uppdragsavtalen. Detta kan Bolaget i vissa fall avgöra själva utan att ställa frågan specifikt. Dvs det finns möjligheter att internt stämma av att tjänsteleverantören har levererat efterfrågad information och dokumentation.*

1. Att det finns förutsättningar för Bolaget att styra och följa upp hur uppdraget utförs samt revidera den utlagda verksamheten. D.v.s. att Bolaget löpande och på begäran erhåller information om den utlagda verksamheten samt att uppdragstagaren informerat om alla händelser som kan påverka uppdragsavtalet.

* *Är uppdragstagaren tillgänglig?*
* *Svarar uppdragstagaren i rimlig tid?*
* *Har uppdragstagaren informerat om eventuella incidenter eller annat som berör Bolaget?*

1. Att uppdragstagaren har interna rutiner för att göra uppgifter tillgängliga samt skydda konfidentiella uppgifter avseende Bolaget och Bolagets kunder, anställda och avtalsslutande parter.

* *Här kan man fråga efter specifika sekretessrutiner och om uppgifter enkelt och snabbt kan göras tillgängliga om Bolaget eller Finansinspektionen skulle begära uppgifter.*

1. Att uppdragstagaren upprättat och vidmakthåller en beredskapsplan för oförutsedda händelser som krissituationer eller störningar i verksamheten, inklusive en kris- och katastrofplanering och att denna beredskapsplan löpande testas.

* *Syftar till att säkerställa att eventuella avbrott hos uppdragstagaren inte leder till att Bolaget inte kan bibehålla kontinuitet i verksamheten.*
* *Finns beredskap i form av lokaler/arbeta hemma om uppdragstagarens lokaler brinner upp?*
* *Finns beredskap hos uppdragstagaren om personer som arbetar i uppdraget säger upp sig?*

1. Att uppdragstagaren har rutiner för säkerhetskopiering och, vid behov, testar system för säkerhetskopiering.

* *Backuprutiner? Hur ofta? Sker backup på backup?*
* *Testas system för säkerhetskopiering*?

1. Att Bolaget har en utträdesstrategi i händelse av uppsägning. Överlämning ska kunna ske till en ny uppdragstagare utan att detta påverkar Bolaget eller Bolagets tjänster till kunder.

* *Finns några uppenbara problem som kan uppstå om part säger upp uppdragsavtalet? Kommer uppdragstagaren medverka vid överlämning? Lan dokumentation skickas över utan hinder?*

1. För det fall uppdragstagaren har lagt ut verksamhet som omfattas av uppdragsavtalet på underleverantör: - Har vidaredelegeringen godkänts av Bolaget? - Finns ett ändamålsenligt avtal mellan uppdragstagaren och underleverantören? - Hur fungerar det samarbetet? - Finns i tillämpliga fall personuppgiftsavtal? - Är underleverantören i avtal bunden att rapportera incidenter till uppdragstagaren? - Är underleverantören bunden i avtal att meddela uppdragstagaren om underleverantören avser att i sin tur anlita en underleverantör?
2. I vilken mån uppdragstagaren planerar att framgent lägga ut funktioner och/eller verksamheter som omfattas av uppdragsavtalet på underentreprenad.
3. Om det har skett någon incident hos uppdragstagaren? Om ja:

* *Har den rapporterats till Bolaget?*
* *Hur har incidenten hanterats och vilka åtgärder har vidtagits för att säkerställa att liknande incident inte inträffar igen?*
* *Känner uppdragstagaren till om någon underleverantör haft en incident?*

1. Har uppdragstagaren de rättsliga tillstånd som krävs för att utföra begärda funktioner eller verksamheter?

# För uppföljning av molntjänstleverantörer avser Bolaget att följa upp följande:

1. Den eller de platser (dvs. regioner eller länder) där relevanta uppgifter lagras och behandlas (datacentrens lokalisering).

* *Exakt plats behöver inte anges. Säkerställ dock att servrar inte befinner sig utanför EU.*

1. I vilken mån uppdragstagaren planerar att framgent ändra platsen eller platserna för datacentralens lokalisering.
2. Att molntjänstleverantören uppnår överenskomna servicenivåerna. Följ upp om exakta kvantitativa och kvalitativa resultatmål är satta för att i god tid kunna vidta lämpliga korrigerande åtgärder om de överenskomna servicenivåerna inte uppfylls.
3. Om relevant och lämpligt, efterfråga rapporter från molntjänstleverantörens internrevisionsfunktion och/eller relevanta certifieringar.

* *Här kan man begära kopia på exempelvis revisionsrapporter avseende informationssäkerhet.*

1. Huruvida molntjänstleverantören bör teckna en obligatorisk försäkring mot vissa risker och, i tillämpliga fall, vilken nivå på försäkringsskydd som efterfrågas.

* *Om försäkring finns, vad täcker denna och är nivån tillräcklig?*
* *Om försäkring saknas, vad är anledningen till detta?*

1. Kravet på att molntjänstleverantören ska ge Bolaget, Finansinspektionen och andra personer som utses av Bolaget eller tillsynsmyndigheterna följande:

- Utöver tillträde till lokaler, även tillträde till relevanta enheter, system, nätverk, information och uppgifter som används för att tillhandahålla den funktion som omfattas av uppdragsavtal, däribland anknuten finansiell information, personal och molntjänstleverantörens utomstående revisorer (”åtkomsträttigheter”).

* *Finns några problem med att en begäran ställs om tillträde till lokaler? Ibland kan det exempelvis vara hemligt var företag placerat sina servrar.*

# För uppföljning av IKT-tjänster avser Bolaget att följa upp följande:

1. Lämpliga och proportionerliga mål och åtgärder för informationssäkerhet, däribland krav såsom minimikrav för informationssäkerhet, specifikationer av företags datalivscykel, revisions- och åtkomsträttigheter och krav beträffande placering av datacentraler samt datakrypteringskrav, nätverkssäkerhet och processer för säkerhetsövervakning.

* *Tillämpar uppdragstagaren segmentering?*
* *Tillämpar uppdragstagaren multifaktor autentisering internt?*
* *Backuprutiner?*
* *Sekretessrutiner?*
* *Tillgång till revisionsrapporter?*
* *Rutiner för säkerhetsövervakning?*

1. Servicenivåavtal för att säkerställa IKT-tjänsternas och IKT-systemens kontinuitet och prestandamål under normala omständigheter liksom under omständigheter som anges i beredskapsplaner i händelse av avbrott.

* *Diskussion kring satta servicenivåer. Vad kan Bolaget förvänta sig vid avbrott hos uppdragstagaren? Vad har de för beredskap?*

1. Hanteringsrutiner för operativa incidenter och säkerhetsincidenter, bl.a. eskalering och rapportering.

* *Vem hos uppdragstagaren ansvarar för att kontakta Bolaget vid en eventuell incident?*
* *Om uppdragstagaren har underleverantörer, har man i avtal säkerställt att underleverantörer måste informera uppdragstagaren?*
* *Om det skulle ske en incident hos en underleverantör, informerar uppdragstagaren Bolaget om detta?*