



Göteborgs
Stad

Försäkrings AB Göta Lejons riktlinje för uppdragsavtal och utlagd verksamhet

Reglerande styrande dokument

Policy
► Riktlinje
Regel
Anvisning
Rutin
Instruktion

Göteborgs Stads styrsystem



Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.

Styrande dokument			
Kommunala föreskrifter		Planerande och reglerande styrande dokument	
Normgivning mot enskild	Riktade styrande dokument	Planerande styrande dokument	Reglerande styrande dokument

Beslutad av: Styrelse	Gäller för: Försäkrings AB Göta Lejon	Diarienummer: 0082/24	Datum och paragraf för beslutet: 2023-10-12 § 111
Dokumentsort: Riktlinje	Giltighetstid: Tillsvidare	Senast reviderad: 2024-05-28	Dokumentansvarig: Bolagscontroller

Bilagor:

-

Innehåll

Inledning	4
Syftet med denna riktlinje	4
Vem omfattas av riktlinjen.....	4
Lagbestämmelser	4
Koppling till andra styrande dokument.....	4
Stödjande dokument.....	4
Riktlinje	5
Ansvar.....	5
Anmälan till Finansinspektionen	5
Process för utlagd verksamhet	6
1. Behovs-, riskanalys och beslutsunderlag.....	6
2. Upprättande och kontroll av avtal	7
3. Årlig uppföljning och utvärdering.....	8
4. Utveckling eller avveckling.....	8
5. Utträde	8
Göta Lejons utlagda verksamhet.....	9
Fastställande och efterlevnad.....	9
Bilaga.....	9

Inledning

Syftet med denna riktlinje

Syftet med denna riktlinje är att reglera vilken typ av verksamhet i bolaget som får läggas ut på uppdragsavtal samt processen för utlagd verksamhet.

Vem omfattas av riktlinjen

Denna riktlinje gäller tillsvidare för hela bolaget och personer som utför uppdrag för bolaget genom uppdragsavtal.

Lagbestämmelser

Denna riktlinje har upprättats i enlighet med Försäkringsrörelselagen (FRL) 10 kap § 19 samt artikel 274.1 Solvens II-förordningen 2015/35 samt EIOPA riktlinje 60, 63.

Koppling till andra styrande dokument

Försäkrings AB Göta Lejons riktlinje för lämplighetsprövning

Försäkrings AB Göta Lejons riktlinje för hantering och rapportering av väsentliga händelser

Stödjande dokument

Checklista för tecknade av uppdragsavtal

Försäkrings AB Göta Lejons instruktion för genomförande och bedömning av uppföljning av utlagd verksamhet

Riktlinje

Försäkrings AB Göta Lejon kan uppdra åt annan juridisk person att utföra bolagets försäkringsrörelse eller funktioner eller verksamheter som har ett naturligt samband med försäkringsrörelsen. Detta förfarande kallas uppdragsavtal. Göta Lejon använder begreppet utlagd verksamhet för de funktioner bolaget valt att utföra på uppdragsavtal.

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 tillfredsställelse och fortlöpande service inte kan upprätthållas.

Ansvar

Bolaget ansvarar för den utlagda verksamheten och ska övervaka att leverantören uppfyller sina åtaganden utifrån nedanstående interna arbetsfördelning.

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
- godkänna att kritisk eller viktig funktion får utföras genom uppdragsavtal

Vd ansvarar för att:

- beslutsunderlag innehållande behovs- och riskanalys tas fram avseende ny verksamhet bolaget önskar utföra på uppdragsavtal
- godkänna upphandlingsunderlag
- vid nya uppdragsavtal presentera detta till styrelsen för godkännande
- erforderliga avtal upprättas
- de som utför verksamheten på uppdragsavtal får del av och följer de riktlinjer och policys som antagits av styrelsen.
- informera Finansinspektionen om uppdragsavtal.
- uppföljning sker av den verksamhet som utförs på uppdragsavtal samt att utfallet rapporteras till styrelsen minst årligen. Ansvaret för uppföljning kan delegeras.

Ansvarig person för den utlagda verksamheten ska, med hänsyn till verksamhetens art och omfattning, löpande följa upp uppdragstagarens arbete. Minst årligen ska en dokumenterad utvärdering av verksamheten genomföras och som rapporteras till vd.

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

Process för utlagd verksamhet

Processen för utlagd verksamhet kan sammanfattas i fem steg:

1. Behovs-, riskanalys och beslutsunderlag
2. Upprättande och kontroll av avtal
3. Årlig uppföljning och utvärdering
4. Utveckling eller avveckling
5. Utträde

1. Behovsanalys, riskanalys och beslutsunderlag

Innan beslut fattas om utläggning av verksamhet ska en behovs- och riskanalys genomföras. Dessa ska utgöra beslutsunderlag till styrelsens beslut om att lägga ut verksamhet till annan.

Behovsanalysen syftar till att undersöka bakgrund och möjligheter till varför bolaget önskar lägga ut verksamhet eller funktion på en tjänsteleverantör. I analysen ska följande aspekter beaktas:

- lagkrav för bolagets verksamhet
- om funktion eller aktiviteten anses vara kritisk eller viktig
- i vilken utsträckning interna resurser eller kompetens finns att tillgå

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.

Riskanalysen ska genomföras avseende potentiella tjänsteleverantörer. Vid genomförande av riskanalysen ska Checklista inför tecknande av uppdragsavtal användas. Kraven på leverantören beskrivs utförligare i artikel 274 Solvens II förordningen 2015/35, vilka alltid ska beaktas vid utläggning av funktioner eller verksamhet.

Riskanalysen ska beskriva om en funktion eller aktivitet som omfattas av ett uppdragsavtal är en kritisk eller viktig funktion eller aktivitet. Detta ska baseras på om funktionen eller aktiviteten är nödvändig för företagets verksamhet, dvs att funktionen eller aktiviteten är nödvändig för att kunna tillhandahålla tjänster åt sina försäkringstagare.

Riskanalysen ska innehålla en beskrivning av hur följande minimikrav säkerställs:

- uppdragstagaren förstår bolagets verksamhet och behov
- det föreligger inga intressekonflikter i uppdragstagarens utförande av uppdraget

I riskanalysen ska en värdering göras av risken att minimikraven inte nås. Dessutom ska

en utvärdering av molntjänster avseende informationssäkerhet och kontinuitetshantering för att undvika systemstörningar göras, se Checklista inför tecknande av uppdragsavtal användas. Vidare ska även långsiktiga hållbarhetsmål och principer ska beaktas vid riskanalysen, så att bolaget säkerställer att en ansvarsfull och hållbar affärspraxis upprätthålls.

Verksamhet får endast läggas ut på uppdragsavtal om minimikraven anses uppfyllas.

Vid förnyad upphandling av utlagd verksamhet ska checklista inför tecknande av uppdragsavtal gås igenom och förnyad riskanalys genomföras om omständigheter visar på att riskerna har förändrats.

Vd förmedlar resursbehov och beslutsunderlag för behandling av styrelsen.

2. Upprättande och kontroll av avtal

Inför upphandling av utlagd verksamhet ska upphandlingsunderlag godkännas av vd.

Vid upprättande av avtal kontrollerar vd att avtalets formalia minst möter lagkraven.

Särskilda krav avseende 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 tjänstleverantören 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 molntjänstleverantör, finns angivna i *Checklista inför tecknande av uppdragsavtal*.

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

Uppdragsavtalets innehåll

Avtal ska upprättas i enlighet med:

- LOU
- artikel 274.1 Solvens II-förordningen 2015/35,
- EIOPA:s riktlinjer för IKT (i tillämpliga fall)
- EIOPAS riktlinjer för uppdragsavtal med molntjänstleverantörer (i tillämpliga fall)

I avtalet ska det finnas en utträdesstrategi i form av överlämningsplan och/eller kontinuitetsplan som kan aktualiseras om verksamhet eller funktion ska återtas till bolaget eller läggas ut på annan leverantör.

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

Avtalets innehåll ska innan signering stämmas av mot checklista i bilaga för att säkerställa aktuella regelverkskrav.

3. Årlig uppföljning och utvärdering

Den utlagda verksamheten ska följas upp löpande under året. Eventuella brister i verksamheten ska diskuteras med leverantören. Större brister rapporteras till vd. En gång per år ska samtliga uppdragstagare följas upp och utvärderas enligt separat instruktion, Försäkrings AB Göta Lejons instruktion för genomförande och bedömning av uppföljning av utlagd verksamhet. Resultatet av uppföljningen ska rapporteras till vd. Eventuella avvikelser ska hanteras i bolagets arbete med intern styrning och kontroll.

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

4. Utveckling eller avveckling

Vid återtagande av uppdrag alternativt byte av tjänsteleverantör ska bolagets kontinuitetsplan aktualiseras samt överlämningsplan tas i bruk. Nytt beslutsunderlag och riskanalys enligt punkt 1 ovan ska genomföras.

5. Utträde

Händelser som aktualiserar bolagets utträdesstrategi är om uppdragstagaren ej kan uppfylla angivna avtalskrav eller om de operativa riskerna ökar i oacceptabel omfattning. Detta kan till exempel vara.

- Brister eller avvikelser mot det skriftliga avtal där parternas samtliga rättigheter och skyldigheter regleras.
- Brist på resurser utifrån uppdragsgivarens behov.
- Bristande i tillräcklig kompetens för att långsiktigt utföra uppdraget med god kvalitet och med väl fungerande internkontroll.
- Brister rörande uppdragstagarens sekretesskydd.
- Uppkomna intressekonflikter eller jäv.

Vid aktualisering av utträdesstrategi ska vd tillsammans med uppdragsgivare upprätta en överlämningsplan minst innehållande:

- Tidsplan för överlämning
- Resursbehov
- Ansvarig för överlämning hos uppdragsgivare, uppdragstagare och ny uppdragstagare eller ansvarig för övergångsverksamheten

Vid genomförd utträdesstrategi ska bolagets kontinuitetsplan ses över och vid behov uppdateras utifrån resultatet av ovan. Vidare bör en uppföljning och utvärdering, enligt

punkt 3, av uppdraget och uppdragstagare genomförs inom 6 månader från uppstart i syfte att säkerställa att övergången har lyckats.

Göta Lejons utlagda verksamhet

Göta Lejon har följande verksamhet som bedrivs på uppdragsavtal:

- Aktuariella tjänster
- Internrevision
- Regelefterlevnad
- Riskhantering
- Skadereglering
- IT
- Försäkringshantering/försäkringssystem (Insman)

Ovanstående tjänster har styrelsen identifierat som kritiska och viktiga. Tjänsterna anses kritiska då de är nödvändiga för att bolaget ska kunna tillhandahålla tjänster i bolagets kärnverksamhet åt försäkringstagarna.

Fastställande och efterlevnad

Denna riktlinje fastställs av styrelsen och träder i kraft dagen för beslut. Riktlinjen ska årligen fastställas av styrelsen även om inga ändringar beslutas. Vd ansvarar för att riktlinjen uppdateras.

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

Bilaga

Checklista för uppdragsavtal



Bilaga 1 - Checklista inför tecknande av uppdragsavtal

1 Risker att bedöma innan tecknande av uppdragsavtal:

1.1 Riskanalys

En riskanalys ska utföras **innan** verksamhet läggs ut och ska avrapporteras till styrelsen. För att en verksamhet ska få läggas ut på uppdragsavtal krävs det en analys av följande faktorer:

- Att tillräcklig beställarkompetens finns inom bolaget,
- Kvaliteten i bolagets försäkringsstyrningssystem får inte försämrats väsentligt.
- Den operativa risken i bolaget får inte öka väsentligt.
- Finansinspektionens möjlighet att utöva tillsyn vidmakthålls.
- Att leverantören samarbetar med Finansinspektionen gällande de funktioner eller verksamhet som omfattas av uppdragsavtalet samt på begäran ger Finansinspektionen, bolaget eller av bolaget utsedd part faktisk tillträde till dess lokaler
- Att bolaget fortsatt kan tillgodose samtliga sina skyldigheter mot sina intressenter inklusive Finansinspektionen och samtliga kunder.
- Försäkringstagarnas möjlighet till tillfredsställelse och fortlöpande service ska kunna upprätthållas.
- Leverantören ska ha effektiva processer för att identifiera, bedöma, lindra, hantera, övervaka och rapportera risker som kan påverka verksamheten i bolaget.
- Det kan säkerställas att gällande sekretesskydd kan vidmakthållas och regler avseende personuppgifter kan följas,
- Att bolaget kan styra, följa upp och revidera uppdraget i tillräcklig omfattning.
- Att leverantören har tillräcklig kunskap och kompetens för att långsiktigt utföra uppdraget med god kvalitet och med väl fungerande internkontroll.
- Leverantören ska ha tillräckliga resurser för att ta sig an de arbetsuppgifter som bolaget planerar att överföra och att leverantören korrekt och tillförlitligt kan fullgöra sina skyldigheter gentemot bolaget.
- Leverantören ska ha beredskapsplaner för hur man ska avsluta uppdraget och överföra tillbaka verksamheten till bolaget eller annan leverantör utan betydande störningar av bolagets verksamhet.
- Leverantören ska ha tillräckliga beredskapsplaner för att hantera nödsituationer eller affärsstörningar.
- Frågor kring jäv och intressekonflikter har identifierats och utretts.

- Att reglerna om offentlig upphandling och annan gällande rätt följs.
- Att den utlagda verksamheten och parternas rättigheter och skyldigheter kan regleras i ett skriftligt uppdragsavtal som minst täcker samtliga punkter i avsnitt 2.
- Att verksamhetens relevanta riktlinjer kan följas, särskilt avseende, utlagd verksamhet, intressekonflikter, informationssäkerhet och personuppgifter.
- Att bolaget fortsatt kan upprätthålla en ansvarsfull och hållbar affärspraxis

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 majeure
- 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
- tillämplig lag och tvistefora.

2 Definition av molntjänster enl. Eiopas definition av molntjänster, EIOPA-BoS-20-002:

Tjänsteleverantör En enhet från tredje part som utför en process, tjänst eller verksamhet, eller delar därav, inom ramen för en överenskommelse om uppdragsavtal.

Molntjänstleverantör En tjänsteleverantör enligt definitionen ovan som ansvarar för att tillhandahålla molntjänster inom ramen för ett uppdragsavtal.

Molntjänster Tjänster som tillhandahålls med hjälp av molnbaserade datortjänster, dvs. en modell som möjliggör en allmän, lämplig nätverksåtkomst på begäran till en gemensam samling konfigurerbara datorresurser (t.ex. nätverk, servrar, lagring, applikationer och tjänster) som snabbt kan tillhandahållas och överlåtas med minimala driftsinsatser eller interaktion med tjänsteleverantören.

Molntjänst är inte bara lagring av data utan innefattar även system/programvaror/applikationer med internet åtkomst där Bolaget/användaren har åtkomst via inloggning och lösenord för att förändra, lägga till, radera eller ha åtkomst av data. Typiska molntjänster är s.k. SaaS och IaaS enligt nedan exempel,

Software as a Service (SaaS): - En typ av molntjänst som tillhandahåller programvara över internet. Google, Twitter, Facebook är typiska exempel, men även försäkrings- och skadehanteringssystem. Användarna kan få åtkomst till applikationen från vilken uppkopplad enhet som helst.

Användningen av den påminner mer om att hyra programvara än att köpa den. Software as a Service-användare prenumererar på programvaran istället för att köpa den, ofta månadsvis. Applikationerna köps och används online och filer sparas oftast i molnet istället för på enstaka datorer.

Infrastructure as a Service (IaaS): IaaS är en infrastruktur för omedelbar databehandling som etableras och hanteras över internet. IaaS gör det möjligt för bolag att snabbt skala upp och ned på begäran och endast betala för det man använder. Man slipper kostnaderna och besväret med att köpa och hantera egna fysiska servrar och annan infrastruktur för datacenter. En typisk aktör för detta är Azure, där de hanterar infrastrukturen medan du köper, installerar, konfigurerar och hanterar din egen programvara – operativsystem, mellanprogram och program.

Platform as a Service (PaaS): En typ av molntjänst som tillhandahåller en dataplattform och en uppsättning programvarusystem som en tjänst. Användaren blir tilldelad programvara med hjälp av verktyg och lagring med flera tjänster ... bibliotek från leverantören så kan användaren skapa saker. Användaren styr driftsättning och konfigurering. Leverantören tillhandahåller nätverk, servrar, lagring med flera tjänster.

3 Att säkerställa innan molntjänst upphandlas

Inför att bolaget ska teckna avtal med en molntjänstleverantör ska följande beaktas.

- steg 1** Vid behov använd frågeformulär, separat word dokument, som tillsänds leverantör för att säkerställa typ av molntjänst.
- steg 2** Utför riskanalys inför utläggning av verksamhet till molntjänstleverantör tillsammans med intern CISO eller IT avdelning. Även punkter enligt riskanalys i avsnitt 1 ovan ska beaktas om viktig eller kritisk verksamhet eller funktion ska läggas ut på en molntjänstleverantör.
- Mall enligt EIOPA riktlinje 12, specificeras nedan.
- För bedömning av datasäkerhet (tillräckliga tekniska och organisatoriska säkerhetsarrangemang) inkluderat
- i. kontinuerlig efterlevnad av de lagstadgade kraven
 - ii. kort- och långsiktiga motståndskraft och bärkraft vad gäller ekonomi och solvens
 - iii. affärskontinuitet och operativa motståndskraft
 - iv. operativa risk, inbegripet vad gäller uppförande kod (CoC), IKT och juridiska risker
 - v. ryktesrisker.
- steg 3** Bedöm ev intressekonflikter mellan bolaget, ledningen, styrelse, IT avd och molntjänstleverantör för bedömning av datasäkerhet (tillräckliga tekniska och organisatoriska säkerhetsarrangemang) inkluderat, i. kontinuerliga efterlevnad av de lagstadgade kraven.
- steg 4** Bedöm om förbesiktning/IT-revision ska utföras - Se riktlinje 9 i EIOPA-BoS-20-002.
- steg 5** Granska avtalet enligt nedan, OBS beakta speciellt krav om
- i. kontrollera att revisionsrättigheter (access and audit rights) anges i avtalet,
 - ii. kontrollera att kedjeoutsourcing av kritiska och viktiga funktioner eller aktiviteter hanteras i avtalet, och
 - iii. kontrollera att uppsägning och exitstrategier hanteras i avtalet.
- steg 6** tillse eller upprätta ansvar och process för bevakning och översyn av molntjänst (minst årligen) och förnyelse av molntjänstarrangemang, incidentrapporteringsprocess (CISO, IKT ansvarig etc. kan ingå i riskhanterings årsplan).
- steg 7** **Upprätta anmälan till Finansinspektionen avseende Molntjänstleverantör (namn, org.nr, systemnamn och eller tjänst).**
- steg 8** Uppdatera avtalsregister med ovan avtal.

EIOPA molntjänster Riktlinje 12 – uppgifts- och systemsäkerhet		
§	Kontrollbeskrivning	Kommentar av utvärdering/avtal

§	Kontrollbeskrivning	Kommentar av utvärdering/avtal
----------	----------------------------	---------------------------------------

47	Företaget bör säkerställa att molntjänstleverantörerna efterlever europeiska och nationella föreskrifter samt lämpliga IKT-säkerhetsstandarder	
48	Vid uppdragsavtal för kritiska eller viktiga operativa funktioner eller verksamheter med molntjänstleverantörer bör företaget dessutom definiera särskilda informationssäkerhetskrav i uppdragsavtalet och regelbundet övervaka efterlevnaden av dessa krav	
49	Vad beträffar §48 bör företaget, vid uppdragsavtalet för kritiska eller viktiga operativa funktioner eller verksamheter med molntjänstleverantörer, utifrån en riskbaserad strategi och med beaktande av sitt ansvar samt molntjänstleverantörens ansvar:	
a	komma överens om tydliga roller och ansvarsområden för molntjänstleverantören och bolaget avseende de operativa funktionerna eller verksamheter som påverkas av uppdragsavtalet om molntjänster och fördelningen bör vara tydlig.	
b	definiera och besluta om en lämplig skyddsnivå för konfidentiella uppgifter, kontinuiteten för de verksamheter som ska omfattas av uppdragsavtal samt mot bakgrund av det avsedda uppdragsavtalet om molntjänster	
c	överväga särskilda åtgärder om så behövs för transiterande, minnesbelägna och vilande data, till exempel användning av krypteringstekniker i kombination med en lämplig nyckelhantering	
d	överväga molntjänsternas integreringsmekanismer med företagets system, till exempel gränssnitten för tillämpningsprogram och en sund användar- och åtkomsthantering	
e	i avtalet säkerställa att nätverkstrafikens tillgänglighet och förväntade kapacitet efterlever höga kontinuitetskrav, om så är tillämpligt och rimligt	
f	definiera och besluta om lämpliga kontinuitetskrav som säkerställer lämpliga nivåer på varje nivå i den tekniska kedjan, i tillämpliga fall,	
g	ha en sund och väldokumenterad hanteringsprocess för tillbud, inbegripet respektive ansvarsområden, till exempel genom	

	att definiera en samarbetsmodell om faktiska eller misstänkta tillbud inträffar	
h	anta en riskbaserad strategi för platser för lagring och hantering av uppgifter och informationssäkerhetsbeaktanden	
i	övervaka efterlevnaden av kraven på ändamålsenligheten och effektiviteten hos kontrollmekanismen som molntjänstleverantören genomför och som skulle minska riskerna för de tillhandahållna tjänsterna	

BILAGA 2

Utvärdering av avtal – leverantör

Den här checklistan ska bidra med att definiera om alla nödvändiga villkor/krav är inkluderade i uppdragsavtalet.

Checklistan ska fyllas i för ALLA uppdragsavtal.

Namn på leverantör	XX	Uppdragsavtalet (minimumkrav) se rad 28-48 nedan samt; - detaljerad beskrivning - kostnader och omfattning - uppsägning eller förlängning - ansvar och befogenheter - beredskapsplan - sekretessklausul - suboutsourcing
Org. nummer	XX	
Funktion som är utlagd enligt uppdragsavtalet		
Upprättat		
Utlagd internt/externt		
Beställansvarig		

Anmälan Finansinspektionen	JA	NEJ
Den ansvarige för den utlagda verksamheten har innan avtalet trätt i kraft anmält detta till Finansinspektionen		
Samtliga kriterier ska tydligt framgå av det skriftliga avtalet, i enlighet med gällande regelverk;		
Parternas skyldigheter och ansvar		
Uppdragstagarens åtagande att, i tillämpliga delar, följa de lagar, föreskrifter och allmänna råd som reglerar den utlagda verksamheten och de styrdokument som antagits av bolaget avseende denna och att samarbeta med Finansinspektionen avseende den utlagda verksamheten		
Uppdragstagarens skyldighet att informera om alla händelser som kan inverka materiellt på dennes förmåga att effektivt utföra den utlagda verksamheten i enlighet med tillämpliga lagar eller föreskrifter		
Att avtalet endast kan sägas upp av uppdragstagaren med en uppsägningstid som är tillräckligt lång för att bolaget ska ha möjlighet att finna en alternativ lösning.		

En uppsägningstid på tre månader anses vanligtvis som tillräcklig		
Att bolaget har möjlighet att vid behov avsluta uppdraget utan att det inkräktar på kontinuiteten hos och kvaliteten på dess tillhandhållande av tjänster till försäkringstagarna		
Att bolaget har rätt att få information från uppdragstagaren om den utlagda verksamheten och dess resultat		
Att bolaget har rätt att meddela allmänna vägledning och enskilda instruktioner till uppdragstagaren angående vad som måste beaktas vid utförandet av den utlagda verksamheten		
Att uppdragstagaren ska skydda alla konfidentiella uppgifter avseende bolaget och dess försäkringstagare, förmånstagare, anställda, avtalslutande parter och alla andra personer och iaktta samma krav på säkerhet och sekretess som gäller för bolaget självt		
Att bolaget, dess externa revisorer och Finansinspektionen ska ha tillgång till all information om den utlagda verksamheten samt rätt att genomföra inspektioner på plats i uppdragstagarens lokaler		
Uppdragstagaren ska även vara skyldig att besvara frågor som Finansinspektionen inom ramen för sin tillsyn ställer till uppdragstagaren avseende den utlagda verksamheten		
Villkoren för när uppdragstagaren får anlita underleverantör för utförandet av utlagd verksamhet. Uppdragstagarens skyldighet och ansvar enligt avtalet med bolaget ska vara opåverkat av att uppdragstagaren anlitar underleverantör. Bolaget ska godkänna anlitate underleverantör för verksamheter som är av väsentlig betydelse och i övriga fall få information om vilka underleverantörer som anlitas		
Lämplig beskrivning av uppdraget som utförs av uppdragstagaren		
Regelbundna rapporteringskrav som är nödvändiga/lämpliga för den utlagda verksamheten		
Avgifter, betalningsvillkor och uppdragstidens längd		
Uppdragstagarens åtagande att avseende den utlagda verksamheten upprätthålla ändamålsenliga		

beredskapsplaner för hantering av krissituationer eller störningar i verksamheten samt att, där det finns behov, regelbundet testa systemen för säkerhetskopiering		
Vilket land lag ska tillämpas på avtalet		
Det ska framgå vilket land uppdragstagaren utför uppdraget ifrån, särskilt viktigt om uppdragstagaren befinner sig i tredje land		
Vid behov bör det införas krav på ansvarsförsäkring för uppdragstagaren		
Hanteras ansvar om personuppgifter/GDPR i avtalet eller via PUB avtal		
Hanteras grundläggande krav om informationssäkerhet i avtalet		
Beaktas lagring av data (personuppgifter) i avtalet beaktat särskilt molnlagring utanför EES		
Attestpolicy		
Det skriftliga uppdragsavtalet ska vara undertecknat av behöriga personer. Avtalet ska i den mån det är möjligt helst vara undertecknad av funktionsansvarig eller styrelsemedlem enligt firmateckning		