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 försämras väsentligt.
- Den operativa risken i bolaget får inte ökar 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 faktiskt tillträde till dess lokaler
- Att bolaget fortsatt kan tillgodose samtliga sina skyldigheter mot sina intressenter inklusive Finansinspektionen och samtliga kunder.
- Försäkringstagarnas möjlighet till tillfredsställande 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 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
- 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. Använvändaren 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 molntjänsteleverantör 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 riskhanteringens årsplan).

steg 7 **Upprätta anmälan till Finansinspektionen avseende Molntjänsteleverantör (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**

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		
Beställaransvarig		

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 vägledningar 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, avtalsslutande 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 anlitade 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		