Tjänsteutlåtande
Utfärdat 2026-11-03
Ärendenummer FGL-2026-00005

Handläggare
Petra Willquist Rönnäng
Telefon: 031-368 5514
E-post: petra.willquist.ronnang@gotalejon.goteborg.se

Regelefterlevnadsfunktionens rapport kvartal 3 2026

Förslag till beslut

I styrelsen för Försäkrings AB Göta Lejon:

Styrelsen antecknar regelefterlevnadsfunktionens rapport kvartal 3 2026.

Sammanfattning

Regelefterlevnadsfunktionen avrapporterar den granskning som utförts i enlighet med beslutad granskningsplan. Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag anmärkt på bolagets arbete med att säkerställa att alla IKT-avtal är på plats, men i övrigt inte funnit något som innebär att bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för bolagets tillståndspliktiga verksamhet.

Bedömning ur ekonomisk dimension

Kontrollfunktionens granskar bolagets följsamhet mot krav som gäller för bolagets tillståndspliktiga verksamhet. Ur ekonomiskt perspektiv är det viktigt då det är en del av att säkerställa bolagets långsiktiga ekonomiska hållbarhet.

Bedömning ur ekologisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bilagor som ingår i beslutsunderlaget

Regelefterlevnadsfunktionens kvartalsrapport 3 2026

Beskrivning av ärendet

Information till styrelsen om regelefterlevnadsfunktionens rapport från kvartal 3 2026.

Enligt Försäkringsrörelselagen 10 kap, 4 § ska försäkringsföretag ha fyra centrala funktioner. Dessa utgörs av regelefterlevnadsfunktionen, riskhanteringsfunktionen, aktuariefunktionen och internrevisionsfunktionen. Dessa kontrollfunktioner ska utvärdera systemet för internrevision, regelefterlevnad och riskhantering. Funktionerna ska även utvärdera andra delar av företagsstyrningssystemet och rapportera resultatet och lämna rekommendationer efter utvärdering till företagets styrelse.

Regelefterlevnadsfunktionen avrapporterar den granskning som utförts i enlighet med beslutad granskningsplan. Tredje kvartalet har regelefterlevnadsfunktionen kontrollerat bolagets hantering av kunskap och kompetens hos anställda och styrelse, bolagets hantering av intressekonflikter samt bolagets riktlinjer för ändamålet.

Regelefterlevnadsfunktionen har i samband med tidigare granskningar lämnat en rekommendation avseende att visst arbete kvarstår med att ta fram tilläggsavtal med IKT-leverantörer samt att vissa leverantörer uppvisat svårighet med att efterleva redan uppdaterade IKT-avtal. Denna rekommendation kvarstår och avses följas upp under fjärde kvartalet.

Utförda kontroller har i övrigt inte föranlett någon anmärkning för bolaget. Funktionen för regelefterlevnad har vid fullgörandet av sitt uppdrag inte funnit något som innebär att bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för bolagets tillståndspliktiga verksamhet.

Bolagets bedömning

Det är bolagets bedömning att rapporten är relevant för bolagets arbete.

Petra Willquist Rönnäng	Anders Jonasson
Bolagscontroller	VD

Till
Styrelsen i Försäkrings AB Göta Lejon

Kvartalsrapport för perioden 1 juli 2026 – 30 september 2026 avseende regelefterlevnad

1. Inledning

Genom denna rapport återkopplar funktionen för regelefterlevnad resultatet av senast genomförda kontroll av Försäkrings AB Göta Lejons, nedan Bolaget, regelefterlevnad samt redogör för de övriga åtgärder som funktionen för regelefterlevnad har vidtagit under det tredje kvartalet 2026.

För en överblick över utfallet av kvartalets utförda kontroller, se bilaga 1.

2. Händelser av relevans under perioden

2.1. Regelbevakning

Följande nyhetsbrev har tillställts Bolaget under årets tredje kvartal. Dessa finns återgivna i sin helhet i bilaga 2.

- Nya nationella råd och rekommendationer om cybersäkerhetshot från avancerad AI
- Förslag om elektroniska meddelanden vid försäkringsavtal (Ds 2026:7)
- IMY klargör ansvarsroller enl GDPR vid finjustering av AI
- FI ger AIFM Capital en anmärkning och en sanktionsavgift 260916

2.2. Kontroll av Bolagets regelefterlevnad

Metod

Periodens kontroll har till övervägande del bestått i att följa upp Bolagets hantering av kunskap och kompetens hos såväl anställda som styrelsen. Kontrollen har utgått från de krav som uppställs i försäkringsrörelselagen (FRL) samt i lagen om försäkringsdistribution (LFD).

Därtill har funktionen för regelefterlevnad granskat Bolagets hantering av intressekonflikter samt Bolagets riktlinjer för ändamålet.

Funktionen för regelefterlevnad har vidare följt upp den tidigare anmärkningen beträffande Bolagets anpassningar till DORA-förordningen.

Relevanta regler och riktlinjer

- Periodens kontroller baseras på följande regelverk och styrdokument i Bolagets verksamhet:Försäkringsrörelselag (2010:2043)
- FFFS 2015:8 om Försäkringsrörelse
- Kommissionens delegerade förordning 2015/35 om upptagande och utövande av försäkringsverksamhet
- Riktlinjer för intressekonflikter
- Intressekonfliktsregister
- Riktlinjer för kunskap och kompetens (fit & proper)
- Riktlinjer för försäkringsdistribution

Intressekonflikter

Uppföljning av identifiering och hantering av intressekonflikter har gjorts. Kontrollen har syftat till att följa upp om Bolaget har identifierat några nya intressekonflikter som behövt hanteras.

Bolaget har redogjort för Bolagets interna rutiner för att identifiera och hantera intressekonflikter. Funktionen för regelefterlevnad har vidare tagit del av Bolagets interna riktlinjer för hantering av intressekonflikter som omfattar samtliga anställda och Bolagets ledning. Utöver att det finns en anmälningsskyldighet avseende intressekonflikter i verksamheten så är det även en stående punkt vid varje styrelsesammanträde i Bolaget. Funktionen har därtill utfört en särskild kontroll där anställda och styrelsen har fått besvara frågor angående intressekonflikter, samt intygat att inga sådana som kan påverka Bolaget negativt föreligger.

Utöver ovan har funktionen mottagit och granskat Bolagets intressekonfliktsregister.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

Kunskap och kompetens hos anställda

Granskning av Bolagets interna rutiner och riktlinjer för kunskap och kompetens. Kontrollen har syftat till att säkerställa att Bolaget har vidtagit rimliga åtgärder för att efterleva kunskaps- och fortbildningskravet i försäkringsdistributionsregelverket (IDD).

Bolaget har redogjort för sina interna rutiner för fortbildning och kunskapstest som omfattar de anställda som direkt deltar i Bolagets försäkringsdistribution. Bolaget bedöms ha goda rutiner för löpande fortbildning. Bolagets anställda ska därtill avlägga kunskapstest under hösten 2026.

Funktionen för regelefterlevnad bedömer sammantaget att Bolaget har goda rutiner och riktlinjer för att säkerställa efterlevnad av kraven på kunskap och kompetens enligt IDD.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

Fit & proper

Uppföljning av styrelsens samlade kompetens. Kontrollen har syftat till att säkerställa att Bolagets styrelse efterlever kraven som ställs i Solvens II-regelverket på styrelsens samlade kompetens, samt följa upp om det finns behov av kompetensutveckling.

Bolagets styrelse har under år 2026 genomfört den årliga ”fit & proper”-övningen där samtliga styrelseledamöter skattat dels sin egen enskilda kunskap och kompetens, dels styrelsens samlade kompetens. I denna övning identifieras eventuella behov av kompetensutveckling och att Bolaget följer upp och justerar styrelsens utbildningsplan för kommande år. Under hösten kommer årets fit & proper att genomgås och fastställas av styrelsen.

Funktionen för regelefterlevnad har inte haft några synpunkter med anledning av kontrollen.

Uppföljning av tidigare kontroller

Därtill har funktionen för regelefterlevnad följt upp tidigare rekommendationer avseende Bolagets arbete med IKT och informationssäkerhet.

Funktionen för regelefterlevnad har huvudsakligen inte haft några synpunkter med anledning av kontrollen, men noterar att vissa tilläggsavtal med IKT-leverantörer ännu inte är klara samt att vissa leverantörer uppvisat svårighet med att efterleva redan uppdaterade IKT-avtal.

Funktionen för regelefterlevnad har för avsikt att följa upp detta under det fjärde kvartalet.

2.3. Råd och stöd

Funktionen för regelefterlevnad har under perioden funnits tillgänglig för att svara på frågor och lämna råd och stöd till Bolagets anställda.

3. Funktionen för regelefterlevnads bedömning

De oklarheter som funktionen för regelefterlevnad noterat framgår under avsnitt 2.2. ovan. Funktionen för regelefterlevnad har i övrigt vid fullgörandet av sitt uppdrag inte funnit något som innebär att Bolaget sammantaget inte lever upp till de krav som uppställs i de lagar, förordningar, föreskrifter och allmänna råd som gäller för Bolagets tillståndspliktiga verksamhet.

Stockholm den 23 oktober 2026



Johan Grenefalk

1 Översikt regelefterlevnad för kvartal 3, 2026

	Område	*Kontroll*	*Anmärkning*
	Övrig regelefterlevnad	Intressekonflikter.	*Ingen anmärkning*
		Kompetens och kunskapsnivå hos personalen (IDD).	*Ingen anmärkning*
		Kompetens och kunskapsnivå hos styrelsen (fit & proper) inkl. samlad kompetens.	*Ingen anmärkning*

*Denna matris syftar till att ge Bolaget en överblick över resultatet av utförd kontroll av Bolagets regelefterlevnad samt återge vilka åtgärder som Bolaget rekommenderas att vidta eller som är under arbete. Denna färgskala är inte kopplad till den riskmatris som har tillsänts Bolaget som bilaga till årsplanen.

2 Översikt regelefterlevnad från föregående kontroller

	Kvartal	*Område*	*Kontroll*	*Anmärkning*
	Q1 2026	Anpassning till nya eller förändrade regelverk (fokuskontroll)	Europaparlamentets och Rådets förordning om digital operativ motståndskraft för finanssektorn (DORA).	Visst arbete kvarstår alltjämt med Bolagets IKT-avtal, se notering i tillhörande kvartalsrapport, avsnitt 2.2.

*Denna matris syftar till att ge Bolaget en överblick över föregående kontroller där funktionen för regelefterlevnad har haft anmärkningar eller synpunkter som inte är hanterade eller som är under arbete och som funktionen för regelefterlevnad avser att följa upp.

3 Färggradering

	Utförd kontroll har inte föranlett någon anmärkning.
	Utförd kontroll har föranlett mindre anmärkning eller synpunkt. Åtgärd rekommenderas eller är under arbete.
	Sannolikhet för att regelavvikelse inträffar. Åtgärd behöver vidtas inom kort.
	Regelavvikelse har uppmärksammats vid utförd kontroll. Åtgärd behöver vidtas snarast.

Nyhetsbrev

Ang. Nya nationella råd och rekommendationer om cybersäkerhetshot från avancerad AI

---

2 juli 2026

1. Bakgrund

AI förändrar sällan vilka typer av cyberangrepp som förekommer. Nationellt cybersäkerhetscenter, nedan NCSC, bedömer att AI främst kommer att förstärka befintliga angreppsmetoder, snarare än att skapa helt nya. När organisationer använder AI uppstår en ny cyberattackyta eftersom systemen är kontextberoende och tolkar input. Det gör dem sårbara för angrepp, särskilt när de kopplas till interna system, får tillgång till verksamhetsdata eller får möjlighet att agera autonomt. Grundläggande cybersäkerhetsprinciper gäller därför fortsatt, men de måste fungera bättre än någonsin och kompletteras med flexibilitet att utveckla nya förmågor. Insatser som begränsar angriparens möjligheter och ökar motståndskraften i verksamhetens system bör därför prioriteras.

2. Rekommendationer för beslutsfattare och organisationer

NCSC rekommenderar att cyberrisker hanteras som en ledningsfråga. Det innebär bl.a. att en verksamhet behöver ha ett tydligt ägarskap för system, informationstillgångar och AI-lösningar. Bristande underhåll, gamla och icke uppdaterade system samt oklart systemägarskap kan medföra affärsrisker med direkta konsekvenser för verksamhetens kontinuitet.

Verksamheten behöver även hålla hot- och riskanalyser uppdaterade utifrån såväl AI-förstärkta angrepp som risker kopplade till den egna användningen av AI. Det bör även finnas tillräckliga resurser och reservkapacitet för att leveranser ska kunna upprätthållas och att personal inte överbelastas.

NCSC lyfter även behovet av tydlig styrning av AI-användningen. Organisationer bör besluta vilka AI-verktyg som får användas, vilken information verktygen får hantera och när mänskligt godkännande krävs. Detta är särskilt viktigt eftersom avsaknad av beslut och policy ökar risken för skugg-IT.

,

Vid upphandling bör säkerhetskrav ställas, kontinuitets- och utträdesplaner säkras och efterlevnaden följas upp. Beredskapen kan därutöver stärkas genom samverkan i kunskapshöjande nätverk samt övningar som omfattar AI-förstärkta angrepp och manipulation.

3. Tekniska rekommendationer

På den tekniska sidan betonar NCSC att grundläggande cyberhygien fortsatt är avgörande och att den bör etableras genom NCSC:s tio rekommenderade säkerhetsåtgärder. Ju mer avancerade och AI-drivna hoten blir, desto viktigare blir grunderna, eftersom många avancerade angrepp bygger vidare på kända metoder.

AI kan förkorta tiden från att en sårbarhet blir känd till att den utnyttjas och därmed även tiden för att hinna åtgärda sårbarheten. Särskild prioritet bör därför ges till internetexponerade och affärskritiska system. Den internetexponerade attackytan bör samtidigt minska. Ju färre tjänster och system som är exponerade mot internet, desto färre vägar finns det att utnyttja.

Säkerhet bör även byggas in genom hela AI-systemets livscykel, från design och utveckling till drift och avveckling. I grunden är detta samma principer som gäller för övrigt, men AI tillför nya angreppsytor. Agentiska system bör begränsas eftersom de kan agera självständigt och därmed medföra risker. Systemen bör inte få tillgång till mer data än vad som faktiskt behövs. Tydliga behörighetsgränser bör sättas och mänsklig bekräftelse krävas innan känsliga eller irreversibla åtgärder utförs. Agentsystem med bred åtkomst och svag tillsyn utgör ett betydande riskscenario.

AI gör phising, röstkloning och falska dokument mer trovärdiga, vilket innebär att tidigare varningstecken inte längre är tillräckliga. NCSC rekommenderar därför löpande utbildning med realistiska och tydliga exempel. Organisationer bör kartlägga kritiska leverantörer och komponenter samt bevaka kända sårbarheter.

HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av NCSC bedömningar rekommenderar HSA Söderqvist Advokatbyrå att organisationer prioriterar följande åtgärder.

- Säkerställ styrning och ansvar. Cyberrisker och användningen av AI bör hanteras på ledningsnivå. Fastställ ett tydligt ansvar för verksamhetens system, informationstillgångar och AI-lösningar, och säkerställ att hot- och riskanalyser som omfattar både AI-förstärkta angrepp och risker kopplade till den egna användningen

,

av AI är säkrade. Upprätta därtill skriftliga styrdokument för användandet av AI-verktyg där användandet och den uppföljande kontrollen, tydligt regleras.

- Inför en tydlig och kontrollerad AI-användning. Fastställ vilka AI-verktyg som får användas, vilken information som får delas med dem och i vilka situationer mänskligt godkännande krävs. Särskild försiktighet bör iakttas när AI-system får tillgång till interna system, verksamhetsdata eller möjligheten att agera självständigt.
- Prioritera de grundläggande skyddsåtgärderna. Säkerställ skyndsam uppdatering av internetexponerade och affärskritiska system samt löpande kontroller av den internetexponerade attackytan. Begränsa samtidigt behörigheter och åtkomst till vad som är nödvändigt, särskilt för agentiska system.
- Stärkt beredskap i hela verksamheten. Säkerställ återkommande utbildning och som omfattar AI-förstärkta angrepp. Ställ även tydliga säkerhetskrav på leverantörer, följ upp kritiska externa komponenter och bevaka kända sårbarheter i leverantörskedjan.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta HSA Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. Förslag om elektroniska meddelanden vid försäkringsavtal (Ds 2026:7)

---

21 augusti 2026

1. Sammanfattning

Detta nyhetsbrev belyser promemorian ”Elektroniska meddelanden vid försäkringsavtal (Ds 2026:7)”, som överlämnats till Justitiedepartementet efter en särskild utredning om formkraven i försäkringsavtalslagen (2005:104), nedan FAL. Bakgrunden är att FAL innehåller varierande och delvis oklara krav på hur meddelanden från försäkringsbolag till försäkringstagare ska utformas, vilket den ökade digitaliseringen av försäkringsverksamheten aktualiserar.

Förslaget innebär att en ny bestämmelse om formkrav för vissa meddelanden från försäkringsbolaget införs i 1 kap. 9 § FAL. Enligt förslaget ska sådana meddelanden från försäkringsbolag som påverkar rättigheter eller förpliktelser enligt ett gällande avtal om individuell försäkring, så kallade påbud (till exempel uppsägning, hävning eller villkorsändring). Sådana meddelanden ska kunna sändas med post eller elektroniskt, förutsatt att försäkringstagaren omedelbart kan ta del av dem. Motsvarande ska gälla vid gruppförsäkring när ett meddelande med sådan verkan ska sändas till en gruppmedlem personligen. Ren information och påminnelser omfattas inte av den nya regeln så FAL:s och lagen (2018:1219) om försäkringsdistributions, nedan LFD, befintliga informationsregler lämnas oförändrade.

Vidare föreslås att ett förmånstagarförordnande, liksom återkallelse eller ändring av ett sådant, ska kunna göras genom ett elektroniskt meddelande som undertecknas med avancerad elektronisk underskrift enligt eIDAS-förordningen, som ett alternativ till dagens krav på egenhändigt undertecknande i pappersform.

De föreslagna reglerna föreslås träda i kraft den 1 juli 2027 och ska som utgångspunkt inte gälla för avtal som ingåtts före ikraftträdandet och som inte förnyats därefter. Förslaget har skickats på remiss till berörda remissinstanser och svar ska lämnas senast den 28 augusti 2026.

,

2. Förslaget och skälen för det

Den föreslagna huvudregeln innebär att meddelanden som utgör påbud, det vill säga rättshandlingar som medför rättsverkningar för mottagaren (till exempel uppsägning, hävning, preskriptionsavbrott eller villkorsändring), ska skickas med post eller elektroniskt så att försäkringstagaren omedelbart kan ta del av dem. Det ska gälla oavsett om FAL eller annan författning föreskriver en viss form, till exempel skriftlighet. Det räcker dock inte att enbart hänvisa till en webbplats eller till försäkringstagarens "Mina sidor", eftersom en sådan ordning inte säkerställer att försäkringstagaren omedelbart uppmärksammar meddelandet och kan vidta åtgärder för att bevara sitt skydd.

Utredningen har övervägt men avstått från att låta försäkringstagare vid konsument- och personförsäkring välja kommunikationssätt, med motiveringen att andelen försäkringstagare som har svårt att hantera elektronisk kommunikation minskar och att branschen redan i praktiken anpassar sig efter försäkringstagarens behov. Regeln föreslås vara tvingande i den delen som avser att försäkringstagaren omedelbart ska kunna ta del av meddelandet, men parterna kan avtala om huruvida kommunikationen ska ske per post eller elektroniskt.

När det gäller förmånstagarförordnanden föreslås ett tillägg till 14 kap. 3 § FAL som, utöver dagens krav på egenhändigt undertecknat meddelande i pappersform, tillåter elektroniskt undertecknande med avancerad elektronisk underskrift enligt artikel 3 i eIDAS-förordningen. Förslaget svarar mot ett önskemål som Svensk Försäkring framställt och bedöms inte medföra minskad rättssäkerhet jämfört med egenhändigt undertecknande.

3. Dataskydd

Förslaget innebär att försäkringsbolagen ska behandla personuppgifter i syfte att kommunicera med försäkringstagare i avtalsfrågor, vilket i allt väsentligt rör uppgifter som bolagen redan behandlar idag. Den rättsliga grunden för behandlingen är i första hand att den är nödvändig för att fullgöra avtalet med försäkringstagaren enligt artikel 6.1 b i dataskyddsförordningen. Förslaget bedöms inte medföra några betydande förändringar av försäkringsbolagens nuvarande personuppgiftsbehandling eller innebära ett ökat intrång i den personliga integriteten.

Förslaget bedöms dock kunna begränsas till personuppgifter som inte utgör känsliga personuppgifter. Det bör typiskt sett inte finnas anledning att låta ett elektroniskt påbud till försäkringstagaren innehålla sådana uppgifter. Om det i ett enskilt fall är nödvändigt att behandla känsliga personuppgifter krävs stöd enligt artikel 9.2 i dataskyddsförordningen.

,

4. HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av förslaget rekommenderar HSA Söderqvist Advokatbyrå att försäkringsbolagen fortsätter att sända påbud, såsom uppsägning, hävning och villkorsändring, direkt till försäkringstagaren, till exempel per post eller via e-post, så att försäkringstagaren omedelbart kan ta del av meddelandet. Försäkringsbolagen ska inte enbart hänvisa till en webbplats eller kundportal för denna typ av meddelanden. Ren information och påminnelser omfattas inte av den föreslagna regeln. För dessa meddelanden gäller även fortsättningsvis de informations- och formkrav som följer av FAL och LFD. Försäkringsbolagen bör även säkerställa att elektroniska påbud inte innehåller känsliga personuppgifter utan särskilt stöd i artikel 9.2 i dataskyddsförordningen.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta HSA Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. IMY klargör ansvarsroller enligt GDPR vid finjustering av AI

---

28 augusti 2026

1. Bakgrund

AI har på kort tid blivit en central del av många verksamheters digitala utveckling. Samtidigt har frågor om dataskydd och ansvarsfördelning blivit alltmer aktuella, särskilt när AI-modeller anpassas eller finjusteras med hjälp av data som kan innehålla personuppgifter. För att ge vägledning på området har Integritetsskyddsmyndigheten, nedan IMY, publicerat en rapport som analyserar vilka roller olika aktörer kan ha enligt GDPR vid finjustering av AI-applikationer. Rapporten har tagits fram inom ramen för IMY:s regulatoriska sandlåda och syftar till att skapa större tydlighet för både leverantörer och användare av AI-tjänster.

2. Den faktiska behandlingen avgör ansvaret

Ett av rapportens viktigaste budskap är att ansvarsfördelningen enligt GDPR inte avgörs av vilken teknik som används eller vad parterna väljer att kalla sig i ett avtal. Istället är det den faktiska behandlingen av personuppgifter som är avgörande. Bedömningen måste utgå från vem som bestämmer varför personuppgifter behandlas och vilka väsentliga beslut som fattas kring behandlingen. Detta innebär att organisationer behöver göra en korrekt analys av varje behandlingsaktivitet i ett AI-projekt och inte enbart förlita sig på generella antaganden om roller och ansvar.

2.1. När leverantören är personuppgiftsansvarig

IMY konstaterar att en AI-leverantör ofta blir personuppgiftsansvarig när denne använder personuppgifter för att utveckla eller förbättra sina egna produkter och tjänster. Om leverantören exempelvis finjusterar sin AI-modell för att förbättra dess prestanda eller utveckla nya funktioner för framtida kunder är det leverantören som bestämmer ändamålet med behandlingen. I sådana situationer ansvarar leverantören för att det finns en giltig rättlig grund för behandlingen och att samtliga krav enligt GDPR uppfylls.

För många organisationer innebär detta att användningen av kunddata för egen produktionsutveckling kräver en mer genomtänkt dataskyddsanalys än vad som tidigare varit fallet.

,

2.2. När leverantören agerar som personuppgiftsbiträde

I andra situationer sker behandlingen enbart på uppdrag av kunden. Om en AI-modell finjusteras för en specifik kunds verksamhet och kunden bestämmer både syftet med behandlingen och vilka uppgifter som ska användas, är det normalt kunden som är personuppgiftsansvarig. Leverantören agerar då som personuppgiftsbiträde och får endast behandla uppgifterna enligt kundens dokumenterade instruktioner.

Rapporten understryker vikten av att ansvarsfördelningen tydligt regleras genom personuppgiftsbiträdesavtal och att det finns en gemensam förståelse för vilka instruktioner som gäller under hela utvecklings- och förvaltningsprocessen.

2.3. När gemensamt personuppgiftsansvar uppstår

IMY lyfter även fram att det finns situationer där varken kunden eller leverantören ensamma bestämmer över behandlingen. I gemensamma utvecklingsprojekt eller innovationssamarbeten kan båda parter påverka såväl syftet med behandlingen som de viktigaste besluten kring hur den ska genomföras. Då kan ett gemensamt personuppgiftsansvar uppstå. Enbart det förhållandet att parterna samarbetar eller har ett gemensamt ekonomiskt intresse är dock inte tillräckligt.

Ett sådant ansvar innebär att parterna tillsammans måste komma överens om hur GDPR-skyldigheterna ska fördelas och säkerställa att de registrerade får tydlig information om vem som ansvarar för vad.

2.4. Konsekvenser för organisationer som använder AI

En viktig slutsats i rapporten är att samma aktör kan ha olika roller i olika delar av samma AI-projekt. En leverantör kan exempelvis vara personuppgiftsbiträde när en kundanpassad modell utvecklas, men samtidigt vara personuppgiftsansvarig när data används för att förbättra den egna tjänsten. Detta innebär att ansvarsfördelningen måste analyseras löpande och dokumenteras på ett strukturerat sätt.

Mot denna bakgrund rekommenderar HSA Söderqvist Advokatbyrå att dataskyddsfrågorna beaktas redan vid utveckling och upphandling av AI-lösningar.

3. HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av IMY:s vägledning bör personuppgiftsansvariga genomföra en noggrann kartläggning av alla behandlingsaktiviteter som förekommer i samband med AI-utveckling, finjustering och användning. Det är viktigt att redan i planeringsfasen identifiera vilka

,

personuppgifter som behandlas, vilka aktörer som är involverade och vilka syften behandlingen ska uppfylla. Det räcker inte med att avtalsmässigt kalla sig för exempelvis personuppgiftsbiträde, eftersom det är den faktiska kontrollen över syfte och användning av personuppgifter som avgör rollen enligt GDPR.

Härtill bör personuppgiftsansvariga redan från början tydligt definiera ansvarsfördelningen mellan kund och leverantör, särskilt vid finjustering av AI-modeller och projekt där flera parter bidrar till utvecklingen av AI-lösningar, eftersom dessa situationer ofta innebär mer komplexa avtalsförhållanden.

Slutligen bör dataskyddsfrågorna integreras i organisationens övergripande AI-styrning. Genom att kombinera juridisk och teknisk kompetens kan organisationer skapa förutsättningar för en ansvarsfull användning av AI som både främjar innovation och säkerställer efterlevnad av GDPR.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta HSA Söderqvist Advokatbyrå.

Nyhetsbrev

Ang. Finansinspektionen ger AIFM Capital anmärkning och sanktionsavgift för brister i fondhotellsverksamhet

---

16 september 2026

1. Bakgrund

AIFM Capital AB (AIFMC) är ett fondbolag med tillstånd att driva verksamhet enligt lagen (2004:46) om värdepappersfonder (LVF) och att förvalta alternativa investeringsfonder enligt lagen (2013:561) om förvaltare av alternativa investeringsfonder. En central del av bolagets verksamhet utgörs av ett så kallat fondhotell, en affärsmodell där juridiska personer som saknar eget fondbolagstillstånd ges möjlighet att förvalta fonder med stöd av AIFMC:s tillstånd. Dessa aktörer, så kallade initiativtagare, ges i uppdrag att sköta portföljförvaltningen medan AIFMC behåller det yttersta ansvaret för att verksamheten uppfyller fondregelverkets krav.

Under undersökningsperioden januari 2021 till september 2023 förvaltade AIFMC som mest 30 fonder, varav upp till 13 fonders förvaltning var utlagd på initiativtagare. I september 2023 inledde Finansinspektionen en undersökning av bolagets fondverksamhet. Undersökningen avgränsades till att avse AIFMC:s verksamhet som fondbolag enligt LVF och resulterade i det nu meddelade beslutet om anmärkning och sanktionsavgift.

2. Finansinspektionens iakttagelser

Finansinspektionen identifierade två huvudsakliga brister i AIFMC:s verksamhet.

Brister vid ingående av uppdragsavtal. Under undersökningsperioden ingick AIFMC uppdragsavtal om portföljförvaltning med Ericsson & Partners Förmögenhetsförvaltning AB avseende fonden Ericsson & Partner Edge samt med Case Kapitalförvaltning AB avseende ett antal fonder under varumärket Case. Bolagets interna regler, de så kallade uppdragsinstruktionerna, föreskrev att styrelsen skulle fatta beslut om att ingå uppdragsavtal och att styrelsen dessförinnan skulle ta del av ett avtalsutkast och beslutsunderlag som enligt instruktionerna borde redogöra för bland annat risker och finansiella fördelar.

,

Finansinspektionen konstaterar att avtalet med Ericsson & Partners Förmögenhetsförvaltning undertecknades av bolagets verkställande direktör utan föregående styrelsebeslut och utan att styrelsen hade fått tillgång till det underlag som uppdragsinstruktionen krävde. Avseende Case undertecknade den verkställande direktören uppdragsavtalet på morgonen den 12 maj 2022, innan styrelsen samma dag hade hållit möte. Det styrelsebeslut som sedermera fattades den 8 juni 2022 föregicks inte av ett avtalsutkast, utan styrelsen presenterades ett redan undertecknat avtal jämte ett due diligence-formulär som saknade AIFMC:s egna bedömningar. AIFMC:s invändning att det aktiebolagsrättsliga mandatet från styrelsemötet den 12 maj 2022 inkluderade ett beslut om att ingå uppdragsavtal med Case vann inte gehör hos Finansinspektionen.

Brister i uppföljningen av den utlagda förvaltningen. Fondbolaget är skyldigt att säkerställa att uppdragstagaren utför det utlagda arbetet effektivt och ska enligt Finansinspektionen ägna tillräcklig uppmärksamhet åt frågan om fondandelsägarna får så god avkastning som möjligt i förhållande till den på förhand angivna riskprofilen. Finansinspektionen konstaterar att AIFMC:s uppföljning var uppdelad i en kvalitativ del och en förvaltningsuppföljning, men att delarna varken var för sig eller tillsammans gav styrelsen ett tillräckligt underlag för att bedöma om avkastningen var rimlig i förhållande till respektive fonds riskprofil.

Den kvalitativa uppföljningen fokuserade på formella aspekter av uppdragsförhållandet, såsom regelefterlevnad hos uppdragstagaren och organisatoriska förändringar, men behandlade inte fondernas värdeutveckling. Förvaltningsuppföljningen, som avsåg värdeutvecklingen, omfattade bland annat navkurssättningsrapporter, kvartalsrapporter, vd-rapporter och, från april 2023, månadsrapporter. Styrelsen fick del av månadsrapporterna för april och augusti 2023. Rapporteringen brast enligt Finansinspektionen i flera avseenden: kvartalsrapporterna saknade analys i förhållande till fondernas mål och risknivåer, månadsrapporternas färgmarkeringssystem bedömdes i vissa fall vara direkt missvisande, och de samlade rapporterna innehöll inte information om sambandet mellan fondernas avkastning och deras risknivåer. Av de aktuella fonderna hade flera presterat väsentligt sämre än sin jämförelsenorm sedan start, utan att detta föranlett dokumenterade diskussioner eller ställningstaganden i styrelseprotokollen.

3. Rättslig bedömning och sanktion

Finansinspektionen finner att AIFMC överträdde 14 kap. 2 § första stycket Finansinspektionens föreskrifter (FFFS 2013:9) om värdepappersfonder genom att inte handla med den skicklighet, omsorg och aktsamhet som krävs vid ingående och hantering av uppdragsavtal avseende fondverksamheten. Bolaget åsidosatte även 14 kap. 2 § andra stycket 1 samma föreskrifter genom att inte säkerställa att uppdragstagarna utförde det utlagda arbetet effektivt. Därtill konstateras överträdelse av 2 kap. 17 f § LVF, som kräver att

,

ett fondbolag driver sin verksamhet på ett hederligt, rättvist och professionellt sätt och har tillräckliga resurser och rutiner för att verksamheten ska fungera väl.

Överträdelserna bedöms inte vara av den allvarlighetsgrad som motiverar återkallelse av tillstånd eller varning. Finansinspektionen beaktar att inga konkreta skador till följd av överträdelserna kunnat konstateras och att bolaget har vidtagit åtgärder för att undvika att liknande överträdelser sker igen. Sanktionen bestäms till en anmärkning förenad med en sanktionsavgift om 2 000 000 kronor. Vid graderingen av överträdelserna har Finansinspektionen utgått från tio procent av koncernens omsättning om drygt 100 miljoner kronor. Avgiften har bestämts med hänsyn till överträdelsernas allvar, bolagets grad av ansvar, finansiella ställning och vidtagna åtgärder. Avgiften har dessutom satts ned något med hänsyn till att handläggningen av ärendet dragit ut på tiden.

HSA Söderqvist Advokatbyrås rekommendationer

Mot bakgrund av beslutet rekommenderar HSA Söderqvist Advokatbyrå att fondbolag som lägger ut portföljförvaltning särskilt beaktar följande:

- Säkerställ att interna beslutsrutiner följs och att uppdragsavtal föregås av en dokumenterad bedömning av uppdragstagaren, riskerna och fondandelsägarnas intressen.
- Följ upp fondernas avkastning i förhållande till mål och risknivåer. Säkerställ att ansvariga beslutsfattare får ett tillräckligt underlag.
- Fastställ när brister ska föranleda åtgärder och vem som beslutar om dem. Dokumentera uppföljningen och de ställningstaganden som görs.

Har ni frågor med anledning av det ovanstående är ni välkomna att kontakta HSA Söderqvist Advokatbyrå.