

# SFM Svenska försäkringsförmedlares förening

Den 25 maj 2018 träder GDPR/Dataskyddsförordningen i kraft.

En del är dock oklart fortfarande och det råder lite olika åsikter kring diverse frågor i olika branscher. Förutom den praxis och sedvänja som kommer att växa fram kan klargöranden komma från olika håll, t ex från Datainspektionen, EU-kommissionen, den sk Artikel 29-gruppen och branschorganisationer. En av de frågor som diskuterats är vem som anses vara personuppgiftsansvarig och vem som är personuppgiftsbiträde.

## **PM angående personuppgiftsansvarig och personuppgiftsbiträde inom försäkringsdistribution enligt GDPR/Dataskyddsförordningen**

### **1. Inledning**

Denna pm är inte en riktlinje, inte en rekommendation, inte en policy eller annat liknande ställningstagande från SFM. Det är en pm med en mycket översiktlig sammanställning av vad SFM hittills tagit del av i kontakter med marknaden. Avsikten är inte att försöka bestämma vad som är rätt eller fel. Det finns alltför många olika slags affärsmodeller, olika slags försäkringsförmedlare, olika slags produkter och olika längd på kedjor mellan slutkund och försäkringsbolag för att i dagsläget kunna fastslå en generell princip. Det är upp till var och en som behandlar personuppgifter att ordentligt utvärdera och bedöma sin roll i vart och ett av de olika sammanhang man verkar, att själv ansvara för att avgöra och själv fatta beslut om man är att betrakta som personuppgiftsansvarig eller personuppgiftsbiträde, att känna till de skyldigheter man har i sin roll och i förekommande fall lämna information till registrerade personer, att själv ta ställning till om det är så "svart eller vitt" som en läsning av denna översiktliga pm kan ge intryck av, att utbilda sig i Dataskyddsförordningen och att anlita extern kompetens i dataskyddsfrågor när så behövs. Beroende på vilka eventuella synpunkter som lämnas på denna pm och beroende på hur sedvänja mm utvecklas på marknaden kan SFM komma att uppdatera dokumentet och eventuellt komma att ändra delar av det till statusen av en rekommendation.

Frågan om vem som anses vara personuppgiftsansvarig och vem som är personuppgiftsbiträde i samband med försäkringsförmedling har diskuterats en del på marknaden på senare tid.

Nedan följer en översiktlig sammanställning av de huvudprinciper som till övervägande del syns på marknaden utifrån de kontakter SFM haft med försäkringsförmedlare, försäkringsbolag och andra under våren 2018. Vi har delat upp det i dels relationen till kund, dels i relationen till försäkringsbolag. Det går att skriva mycket kring detta ämne men vi har valt att hålla en kortare längd på denna pm för att det skall vara mer lättillgängligt för alla slags läsare. Alla som läser detta är välkomna att sända synpunkter på texten till oss.

Nedan gäller för normalfallet av försäkringsförmedling och för den som benämns och har tillståndet "försäkringsförmedlare" – inte en anknuten och/eller sidoverksam försäkringsförmedlare. För anknuten och/eller sidoverksam försäkringsförmedlare kan principerna vara annorlunda.

Längst ner i detta dokument finner du information och länkar med text kring vad det innebär att vara personuppgiftsansvarig och personuppgiftsbiträde.

## **2. Principer i relationen mellan försäkringsförmedlare och försäkringsförmedlarens kund**

Försäkringsförmedlaren är personuppgiftsansvarig för behandlingen av personuppgifterna inom ramen för uppdraget denne har med sin kund, dvs de personuppgifter som försäkringsförmedlaren fått från kunden eller på annat sätt samlat in angående kunden. Detta görs inom det lagstadgade tillståndet för verksamheten "försäkringsförmedling" och försäkringsförmedlaren är den som normalt bestämmer ändamålet med behandlingen. Försäkringsförmedlaren är självständig i relation till sin kund, styrs inte av instruktioner i sitt utförande av förmedlingsuppdrag, måste utföra sitt förmedlingsuppdrag, och i det ta in och behandla personuppgifterna från en kund, inom ramen för vad som anges i lagen om försäkringsförmedling (och kommande lag om försäkringsdistribution), föreskrifter, förordningar och inom vad som anses vara god försäkringsförmedlingssed (och god försäkringsdistributionssed). Utöver regler för försäkringsförmedlarverksamhet har försäkringsförmedlaren ett självständigt/eget ansvar och skyldigheter att behandla personuppgifter också enligt andra regelverk, t ex kring penningtvätt. I många fall kan alltså inte en kund eller annan påverka den personuppgiftsansvarige försäkringsförmedlaren kring säkerhetsåtgärder, lagringsrutiner och annat.

I normalfallet klassas varken kunden eller försäkringsförmedlaren som personuppgiftsbiträde i relationen till varandra. Var och en är då personuppgiftsansvarig.

I de fall Försäkringsförmedlaren är personuppgiftsansvarig i relation till sin kund så föreligger inget gemensamt ansvar mellan försäkringsförmedlare och kunden i deras respektive roller som personuppgiftsansvariga. Var och en är personuppgiftsansvarig för de uppgifter som denne har/behandlar/bestämmer ändamålet för.

En part kan anses vara personuppgiftsbiträde om - parten inte längre bestämmer ändamålet med behandlingen av personuppgiften, - behandling av personuppgiften sker utanför ramen för den egna tillståndspliktiga verksamheten (t ex "försäkringsförmedling) och - behandling sker på uppdrag av annan/för annans räkning i sådant som denne "annan" skall göra enligt till exempel avtal eller lag.

Det påtalas diverse gränsfall, där aktörer på marknaden anser att en försäkringsförmedlare visst kan anses vara personuppgiftsbiträde för sin kund. De flesta anser dock att de fallen endast gäller när försäkringsförmedlaren utför uppdrag åt kunden, t ex för kundens personalavdelning, som ligger inom det som normalt bara ligger på en kund och utanför vad en försäkringsförmedlare normalt gör, t ex viss löneadministration som inte har med försäkringsförmedling att göra, dvs där förmedlaren utför uppdrag för kunden utanför vad som kan anses rymma inom avtalet om och begreppet försäkringsförmedling.

### Exemplet tjänstepension

En del på marknaden har övervägt om en försäkringsförmedlare, med ett bolag som kund, kan anses vara personuppgiftsbiträde när denne hanterar personuppgifter angående kundens/bolagets personal. SFM har sett en del argument som talar för att försäkringsförmedlaren skall anses vara personuppgiftsansvarig även för sådana personuppgifter i sådana uppdrag. SFM har bland annat sett resonemang enligt nedan;

I ett normalt tjänstepensionsuppdrag blir försäkringsförmedlaren personuppgiftsansvarig och inte personuppgiftsbiträde, trots att personuppgifter inte i alla fall tas emot direkt från den anställde i rådgivningsmöten utan alla eller delar av personuppgifterna tas emot från kunden angående kundens anställda. Försäkringsförmedlaren avgör vad som behöver samlas in enligt avtalet, lag mm, och har därmed kontroll över behandlingen av uppgifterna (bestämmer därmed ändamål och medel), vad som skall dokumenteras och sparas mm. Kunden kan i exemplet med en tjänstepensionsaffär

lämna för tjänstepensionsaffären nödvändiga personuppgifter om sina anställda till försäkringsförmedlaren med stöd av

-anställningsavtalet (eller annan överenskommelse) mellan kunden och de anställda att kunden skall förse de anställda med tjänstepension och för att uppfylla det åtagandet behöver kunden anlita en försäkringsförmedlare,

-genomförd intresseavvägning där kunden kan konstatera att relevanta personuppgifter om sina anställda kan lämnas till försäkringsförmedlaren och

-kunden har ingått avtal med försäkringsförmedlaren om "försäkringsförmedling", det är då nödvändigt att kunden lämnar personuppgifter om sina anställda till försäkringsförmedlaren så att försäkringsförmedlaren kan uppfylla avtalet med kunden.

Stöd i förordningen för ovan kan finnas genom en kombination av artikel 6 1. b) GDPR angående anställningsavtalet och artikel 6 1. f) i GDPR där kunden genomför en intresseavvägning som ger stöd för att lämna de anställdas personuppgifter till försäkringsförmedlaren. Vad avser intresseavvägningen i artikel 6 1. f) i GDPR kan det konstateras att kundens och försäkringsförmedlarens intressen att följa avtal i detta fall (att kunden behöver överlämna personuppgifter om anställda för att ge anställda pension enligt avtal) kan vara starkare än skyddet för de anställdas intressen och rättigheter.

### **3. Principer i relationen mellan försäkringsförmedlare och försäkringsbolag**

De uppgifter som försäkringsförmedlaren lämnar till försäkringsbolaget och som försäkringsförmedlaren sedan har kvar, t ex rådgivningsdokumentation och kopia på försäkringsansökan, är försäkringsmedlaren personuppgiftsansvarig för. Försäkringsbolaget blir personuppgiftsansvarig för de uppgifter som denne har efter att ha tagit emot dem från försäkringsförmedlaren, direkt från kunden och ev från andra.

I normalfallet klassas varken försäkringsförmedlaren eller försäkringsbolaget som personuppgiftsbiträde i relation till varandra. Var och en är då personuppgiftsansvarig.

I de fall försäkringsförmedlaren är personuppgiftsansvarig i relation till försäkringsbolaget så föreligger inget gemensamt ansvar mellan försäkringsförmedlare och försäkringsbolaget i deras respektive roller som personuppgiftsansvariga. Var och en är personuppgiftsansvarig för de uppgifter som denne har/behandlar/bestämmer ändamålet för.

Som nämnts ovan i texten angående relationen mellan försäkringsförmedlare och kund kan en part anses vara personuppgiftsbiträde bara om - parten inte längre bestämmer ändamålet med behandlingen av personuppgiften, - behandling av personuppgiften sker utanför ramen för den egna tillståndspliktiga verksamheten (t ex "försäkringsförmedling) och - behandling sker på uppdrag av annan/för annans räkning i sådant som denne "annan" skall göra enligt till exempel avtal eller lag.

Med det sagt kan det förekomma särskilda avtalade överenskommelser mellan försäkringsförmedlare och försäkringsbolag, som avviker från vad ett normalt förmedlingsuppdrag innehåller, där försäkringsförmedlaren åtagit sig att utföra uppgifter för försäkringsbolagets räkning och då, för just de specifika delarna, kan anses vara personuppgiftsbiträde till försäkringsbolaget. I de lägena kan det vara befogat att en försäkringsförmedlare undertecknar ett personuppgiftsbiträdesavtal från försäkringsbolaget, ett avtal som avser just de specifika delarna.

Exempel som hörts på marknaden är om försäkringsförmedlaren utför skadereglering för ett försäkringsbolags räkning. Skadereglering ligger utom verksamheten "försäkringsförmedling" och istället inom verksamheten "försäkringsrörelse". Annat som nämnts är om ett försäkringsbolag avtalat med en försäkringsförmedlare att för försäkringsbolagets räkning arkivera vissa försäkringshandlingar som annars försäkringsbolaget skulle ha arkiverat.

#### **4. Annorlunda vid olika upplägg, till exempel vid gruppförsäkring?**

I vissa upplägg, till exempel när en försäkringsförmedlare medverkar i en gruppförsäkringsaffär (det kan dessutom vara kan vara fler parter inblandade än försäkringsförmedlaren, gruppföreträdaren (som även denne kan anses vara försäkringsförmedlare) och försäkringsbolaget) kan det vara nödvändigt att i avtal tydliggöra beskriva vem som gör vad, vem som hanterar vilka personuppgifter, vem eller vilka som skall informera slutkunderna (gruppmedlemmarna) och tydliggöra parternas syn på vem eller vilka som personuppgiftsansvariga och om någon eller några eventuellt kan anses vara personuppgiftsbiträde.

#### **5. Andra frågor kring personuppgiftsansvarig och personuppgiftsbiträde**

Ett undertecknande av ett personuppgiftsbiträdesavtal har ingen juridisk betydelse om det i en prövning av rollerna i efterhand visar sig att den som i avtalet pekas ut som personuppgiftsbiträde i själva verket är att anse som personuppgiftsansvarig; denne skulle då av Datainspektionen och andra ändå anses vara personuppgiftsansvarig.

I flera fall finns andra aktörer än kund, försäkringsförmedlare (en eller flera) och försäkringsbolag inblandade, där det kan vara fråga om så kallade underbiträden, till exempel olika centraler, bolag som håller i rådgivningsverktyg, mellanmän som medverkar i informationsöverföring mm. SFM ber om synpunkter på om och hur dessa situationer innebär några svårigheter ur ett Dataskyddsförordnings- och försäkringsförmedlarperspektiv.

#### **6. Vad innebär det att vara personuppgiftsansvarig och personuppgiftsbiträde?**

Den som är personuppgiftsansvarig skall uppfylla det som krävs enligt Dataskyddsförordningen. Det är viktigt att sätta sig in i regelverket och ta del av annan information, t ex på Datainspektionens hemsida.

Det kan noteras att bara för att en försäkringsförmedlare i många fall anses vara personuppgiftsansvarig så innebär det förstås inte att försäkringsförmedlaren skall spara all information denne behandlat. All information som inte behövs under eller efter ett uppdrag, eller åtgärd, skall återlämnas, till exempel till en kund eller ett försäkringsbolag, eller förstöras. Ett annat exempel är ett offertförfarande där ett försäkringsbolag av någon anledning fått personuppgifter från försäkringsförmedlare eller kund, om försäkringsbolaget i arbetet med att ta fram och lämna offerten anser sig vara personuppgiftsansvarig (och inte personuppgiftsbiträde till försäkringsförmedlaren eller kunden) så skall förstås försäkringsbolaget i normalfallet återlämna eller förstöra personuppgifterna efter att ha lämnat offert eller efter att upphandlingen är klar, i vart fall om det inte blev ett försäkringsavtal med det försäkringsbolaget.

**Text från Datainspektionen om förberedelser för personuppgiftsansvariga:**

<https://www.datainspektionen.se/dataskyddsreformen/forberedelser/forberedelser-for-personuppgiftsansvariga/>

**Text från Datainspektionen om förberedelser för personuppgiftsbiträde:**

<https://www.datainspektionen.se/dataskyddsreformen/forberedelser/forberedelser-for-personuppgiftsbitraden/>

**Länk till avsnittet i Dataskyddsförordningen angående personuppgiftsansvarig och personuppgiftsbiträde:**

<https://www.datainspektionen.se/dataskyddsreformen/dataskyddsförordningen/forordningstexten/#K4>

**Länk till hela Dataskyddsförordningen:**

<https://www.datainspektionen.se/dataskyddsreformen/dataskyddsförordningen/forordningstexten/>

**Andra bra länkar till Datainspektionen:**

Guide för företagare:

<https://www.datainspektionen.se/press/nyheter/2018/enkel-guide-underlattar-for-foretag-att-folja-gdpr/>

Frågor och svar:

<https://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/>

**Utbildning:**

Många utbildningsföretag har bra utbildningar angående dataskydd.

Även Datainspektionen har ibland utbildningar.

För medlemmar hos SFM finns viss utbildning kring Dataskyddsförordningen till rabatterat pris.

Kontakta [info@sfm.se](mailto:info@sfm.se) för mer information.