SFM SVENSKA FÖRSÄKRINGSFÖRMEDLARES FÖRENING

Dataskydds- och IT-policy

Svenska försäkringsförmedlares förening (SFM)

Org nr: 802013-9054
Adress: Apelbergsgatan 36, 111 37 Stockholm

Ansvarig för dataskyddsfrågor: Karin Lindblad, VD
E-post: karin.lindblad@sfm.se
Tel: 076 140 95 36

Version 1.0
4 maj 2018

SFM SVENSKA FÖRSÄKRINGSFÖRMEDLARES FÖRENING

Förord

Detta dokument är särskilt skapat inför Dataskyddsförordningen (även kallat GDPR) som träder i kraft den 25 maj 2018.

SFM har under åren gjort det yttersta för att behandla personuppgifter om medlemmar och andra med största försiktighet och respekt och skall fortsätta med det även under kommande regelverk. SFM skall följa Dataskyddsförordningen, andra regler och den sedvänja samt praxis som kan anses gälla för en förening av vårt slag.

Denna policy innehåller dels SFM´s inställning till skyddet av personuppgifter och dels diverse handlingsregler för vår verksamhet. Policyn riktar sig främst till anställda inom SFM, SFM´s styrelse, eventuella underleverantörer och naturligtvis till de personer som är medlemmar hos SFM och personer på bolag som är medlemmar hos SFM.

Policyn skall löpande uppdateras efter behov beroende på hur föreningens verksamhet utvecklas, förändringar i medlemmars och andra registrerades intressen och beroende på hur lagar, föreskrifter, andra regler, sedvänja samt praxis ändras.

SFM har under det senaste året arbetat med att förbereda sig för Dataskyddsförordningen. Detta har skett genom utbildning av personal, inventering av register, förstörande av personuppgifter som inte längre behövs (såväl i pappersform som på data), genomgång av avtal och ändring av dessa där det behövts, för skapande av denna dataskydds- och IT-policy mm.

I detta dokument använder vi normalt ordet Dataskyddsförordningen och inte GDPR.

SFM är nu förberedda för Dataskyddsförordningen på det sätt som krävs av en förening av vårt slag.

Karin Lindblad, VD
Stockholm den 4 maj 2018

SFM SVENSKA FÖRSÄKRINGSFÖRMEDLARES FÖRENING

1. Om de personuppgifter som SFM behandlar

1.1 Registrerade personer

De personuppgifter SFM behandlar rör i huvudsak personer som är medlemmar eller har varit medlemmar i SFM. Det kan vara fråga om följande personer; - person som söker eller tidigare sökt medlemskap, -person på bolag som söker eller tidigare sökt medlemskap, - person som är medlem eller är anställd i bolag som är medlem, -person som tidigare varit medlem eller person på bolag som tidigare varit medlem. När vi i denna policy skriver orden medlem eller medlemmar avser vi de slags personer som nämns i ovan.

SFM´s personal kan i dator, mobil, andra tekniska hjälpmedel, utskrifter, andra papper och anteckningar ha personuppgifter på affärskontakter, vänner och anhöriga och andra personer som de behöver ha kontakt med i sin verksamhet inom SFM och för sitt privatliv.

SFM behandlar endast personuppgifter på personer inom kretsarna nämnda i föregående stycken ovan och på personer som är eller har varit anställda hos SFM. Samtliga dessa personer kallas i Dataskyddsförordningens terminologi för registrerad eller registrerade.

1.2 Vilka slags personuppgifter och vad har SFM för grund för att behandla dessa?

I fråga om medlemmar är det normalt endast fråga om namn, personnummer, adress, meritförteckning, arbetsgivare och andra uppgifter som typiskt sett behövs för bedrivande av föreningens verksamhet, debitering av avgifter mm.

SFM har laglig grund för behandlingen, bland annat eftersom SFM behöver uppgifterna för att kunna hantera ett medlemsregister, samla in avgifter från medlemmar, som gruppföreträdare förse försäkringsgivare uppgifter om anslutna medlemmar, hantera disciplinärenden och annat som SFM har rätt att göra enligt föreningens stadgar. Medlemskap i SFM är frivilligt, det föreligger avtalsliknande relation mellan medlemmen och SFM, medlemskap söks aktivt av medlem och såväl kommande som existerande medlemmar får information om hur personuppgiftsbehandlingen sker enligt lag och information om SFM´s stadgar. SFM´s stadgar är att jämföra med avtalsvillkor.

Den enda typen av känslig personuppgift som SFM i undantagsfall kan komma att behandla är uppgift som rör medlems eller sökandes brott eller brottsmisstankar angående denne. Dessa kan uppkomma i samband med medlemsansökan eller i samband med disciplinärende. I de fallen skall SFM begära samtycke av personen. Om uppgifter av dylikt känsligt slag sänds via e-post skall det ske genom låsta e-postmeddelanden som kan öppnas via lösenord. SFM skall förstöra uppgiften så snart uppgiften inte längre är nödvändig för ärendet. Om personen inte beviljar samtycke kan det innebära att SFM inte kan behandla alla för ärendet nödvändiga uppgifter. Det kan leda till att SFM inte kan avgöra om personen eller bolaget (om det är ett bolag som är föremål för ärende) uppfyller SFM´s stadgar vilket i sin tur kan leda till att SFM´s styrelse måste avsluta den personens eller det bolagets medlemskap alternativt inte bevilja något medlemskap.

1.3 Information till registrerade

Medlemmar har via ansökan till SFM fått information om SFM's personuppgiftsbehandling på det sätt som krävs enligt Personuppgiftslagen (PuL). Senast den 25 maj 2018 lämnas information enligt Dataskyddsförordningen på medlemsansökan, i nyhetsbrev till samtliga existerande medlemmar och på SFM´s hemsida. Informationen innehåller bland annat de rättigheter en medlem har i fråga om information, möjligheten till rättelse av felaktig personuppgift mm.

Beslut i viktiga frågor och ärenden som kommer från medlemmar eller andra registrerade skall VD förankra med SFM´s egna jurist eller med extern jurist. Det gäller till exempel begäran om rättelse av personuppgift eller begäran om radering av personuppgift.

1.4 Mer om registren med personuppgifter

De personuppgifter SFM har finns i olika register. Såväl i pappersform som på data. SFM har en förteckning över samtliga register och var de finns. Varje register har regler för varför uppgiften behöver sparas innehållande en förklaring av ändamålet med behandlingar, hur länge uppgifter i registret skall sparas och att uppgift därefter skall förstöras. Den tid som uppgifter inom respektive register skall sparas beror dels på hur länge personen är medlem i SFM, bokföringslagen, det ansvar SFM har som gruppföreträdare inom försäkring mm.

Register med namn på samtliga bolag som är medlemmar i SFM finns på den öppna delen av SFM´s hemsida. I detta för allmänheten tillgängliga register kan kontaktuppgifter till ett bolags kontaktperson förekomma.

SFM använder inte själva, och låter inte utomstående använda, personuppgifter insamlade av SFM till marknadsföring för sådant som ligger utanför den verksamhet som föreningen bedriver.

Inga personuppgifter lagras i annat land än Sverige.

De personuppgifter på affärskontakter, vänner och anhöriga med mera som SFM´s personal har i dator, mobil, andra tekniska hjälpmedel, i utskrifter, andra papper och anteckningar skall förstöras när de inte längre behövs.

2. Bolag, personal och andra som kan ta del av personuppgifter som SFM behandlar

SFM delar vissa personuppgifter med det helägda bolaget SFM Service AB, 556539-6248. Endast för verksamheten nödvändiga uppgifter delas. Det kan vara fråga om administration av medlemsavgift, premie till ansvarsförsäkring, avgift för utbildning och annat som rör SFM´s verksamhet. SFM Service AB utför endast uppdrag åt SFM. SFM Service AB är personuppgiftsbiträde till SFM och parterna har ingått ett personuppgiftsbiträdesavtal.

SFM kan i vissa disciplinärenden som kommit till SFM´s kansli behöva dela vissa personuppgifter med InsureSec AB om ärendet skall prövas av InsureSec´s disciplinnämnd, allt enligt stöd i SFM´s stadgar. SFM och InsureSec AB delar i övrigt inga personuppgifter mellan varandra.

SFM kan anlita externt företag för IT-stöd, bokföringsfirma, revisor och annat för sin verksamhet. Endast absolut nödvändiga personuppgifter delas med dessa. I samtliga dessa fall har SFM ett personuppgiftsbiträdesavtal när så krävs enligt Dataskyddsförordningen.

På SFM´s kansli finns personal som tar del av personuppgifter. Dessa anställda kan även komma att utföra vissa uppgifter för SFM Service AB. Därutöver kan SFM komma att anställa extra personal från tid till annan. Samtliga anställda har endast tillgång till de personuppgifter som är nödvändiga för den anställdes arbete. VD skall tillse att personal har de instruktioner och den kunskap som krävs för att följa Dataskyddsförordningen och följa denna dataskydds- och IT-policy.

SFM´s styrelseledamöter kan i samband med behandling av medlemsansökningar och i samband med disciplinärenden komma att ta del av personuppgifter. Samtliga styrelseledamöter får endast tillgång till absolut nödvändiga personuppgifter i respektive ärende och alla styrelseledamöter måste förstöra samtliga personuppgifter de fått från SFM så snart ett ärende är avslutat.

I samband med antagande av nya medlemmar sänder SFM namn på sökanden och namn på sökandens arbetsgivare till en vid krets av personer inom försäkringsbranschen för eventuella kommentarer. Ett slags remissförfarande. SFM skall i samband med detta utskick begära att mottagaren förstör e-postmeddelande eller dokument med dessa namn efter det att remissperioden är slut.

Utöver det som anges ovan delar SFM inga personuppgifter med något annat företag eller organisation, vare sig sådant som ägs av SFM eller ej, eller någon annan person.

3. Inköp av IT-varor och IT-tjänster

Inköp av IT-varor och IT-tjänster skall göras med stor omsorg. SFM skall vid behov ta hjälp av extern expertis för att kunna avgöra vad för slags inköp som är lämpliga. Vid köp av annat än enklare utrustning skall kontroll göras av att leverantören har god vandel och att leverantören har en dataskydds- och IT-policy som uppfyller alla gällande regler för dennes verksamhet och att denne intygar att policyn uppdateras och följs.

4. Löpande avtal angående IT-tjänster

SFM använder extern leverantör för vissa IT-stöd. Externt stöd kan få insyn i personuppgifter. Externt stöd kan dock aldrig få insyn i känsliga personuppgifter.
I de fall det krävs enligt Dataskyddsförordningen skall SFM se till att det finns ett personuppgiftsbiträdesavtal mellan SFM som personuppgiftsansvarig och extern IT-firma.
Avtal med externt företag skall löpande utvärderas i syfte att utröna om det finns nya eller ändrade risker i samband med att externt stöd får del av personuppgifter hos SFM.

5. Användning av IT-system, datorer, mobiler och andra tekniska hjälpmedel samt andra ställen där personuppgifter kan finnas

SFM skall för register innehållande personuppgifter ha säkra IT-system. För tillträde till system, datorer mm skall var och en av de som använder dessa behöva säkra lösenord för tillträde. SFM skall i sina system ha uppdaterade skydd mot virus och andra säkerhetshot. VD skall tillse att det finns rutiner för säker lagring och back-up. VD har ansvar för att personal får instruktioner om vad som är lämpligt i fråga om uttalanden om SFM och dess verksamhet i sociala medier eller andra medier. SFM får aldrig omtala en medlem utan dennes samtycke i sociala medier eller andra medier.

En anställd får använda SFM´s dator och mobil även i privata angelägenheter så länge det inte påverkar den anställdes utförande av arbetet, så länge inga personuppgifter som SFM ansvarar för används i privata sammanhang, så länge det inte är fråga om brottslig verksamhet och sådan

aktivitet som kan anses vara omoralisk och som enligt arbetsrättslig praxis skulle kunna leda till varning, uppsägning eller avsked. SFM´s policy om ickediskriminering skall alltid följas.

En anställd får inte inneha några uppgifter om SFM´s verksamhet och dess medlemmar på någon privatägd dator, privat mobil eller annan privat elektronisk utrustning. När en anställd avslutar sin anställning skall dator, mobil och annan teknisk utrustning som ägs av SFM återlämnas. Alla privata personuppgifter i denna utrustning skall kastas innan den återlämnas till SFM.

Datorer och annan teknisk utrustning samt personuppgifter som finns i pappersform skall utanför kontorstid förvaras inom SFM´s låsta och larmade lokaler och inte förvaras i anställds bostad eller på annat ställe annat än då det behövs vid tillfälligt arbete utanför SFM´s lokal.

Om dator, mobil eller annan teknisk utrustning, innehållande personuppgifter som SFM ansvarar för, tappas bort skall SFM omedelbart vidtaga åtgärder för att minska risken för spridning av personuppgifter.

SFM skall ha ett avtal om tillgång till omedelbar hjälp av expertis/kvalificerad IT-support om det kommer till SFM´s kännedom om att intrång sker eller har skett från utomstående i SFM´s register eller om det finns risk för läckage av personuppgifter på annat sätt.

6. Åtgärder vid brott mot Dataskyddsförordningen

Personal skall informera VD så snart ett brott mot Dataskyddsförordningen upptäcks, eller så snart det finns risk för att ett sådant skulle ske. VD skall skyndsamt behandla ärendet. Om personuppgifter inte behandlats på rätt sätt skall berörda personer, till exempel berörda medlemmar, informeras snarast när så krävs enligt Dataskyddsförordningen. VD skall snarast informera styrelsen och all den personal som kan beröras. VD skall i övrigt vidtaga alla nödvändiga åtgärder som behövs för att begränsa skadan och för att återställa verksamheten så att Dataskyddsförordningen och denna dataskydds- och IT-policy följs. VD skall, om så krävs enligt Dataskyddsförordningen, informera relevant myndighet på det sätt och inom de tider som krävs.

VD skall dokumentera vad som hänt, orsaken, hur det upptäcktes, hur det åtgärdades och vilka övriga åtgärder som vidtogs i saken. Förutom den första inledande informationen som VD skall lämna till styrelsen skall VD sedan presentera hela ärendet för styrelsen och redogöra för hur det kan undvikas i framtiden. VD skall i alla beslut och åtgärder av vikt som vidtas i samband med ett brott mot Dataskyddsförordningen förankra dessa med SFM´s egna jurist eller med extern jurist.

Om inte VD finns tillgänglig för att vidtaga ovan nämnda åtgärder skall VD se till att annan person på SFM´s kansli har instruktion om att vid dylika händelser snarast informera styrelsen. Styrelsen skall sedan utse person som för SFM´s räkning snarast vidtar de åtgärder VD skall vidtaga enligt ovan.

7. **Dataskyddsombud (”Data Protection Officer / DPO”)**

Efter genomgång av de regler som gäller för om en organisation skall utse en DPO eller ej så har SFM har kommit fram till att SFM inte behöver utse en sådan. Föreningen behandlar inte personuppgifter av sådant slag och i sådan utsträckning som gör att en DPO behöver utses.

8. Uppdatering av denna policy

VD skall minst en gång per år utvärdera om denna dataskydds- och IT-policy behöver ändras. VD skall utreda och ändra text i policyn när så behövs beroende på hur föreningens verksamhet utvecklas, förändringar i medlemmars och andra registrerades intressen och beroende på hur lagar, föreskrifter, andra regler, sedvänja samt praxis ändras.

Medlemmar skall informeras om ändring i denna policy genom nyhetsbrev och genom att ändrad policy läggs ut på SFM´s hemsida. Styrelsen skall antaga nya versioner av denna policy.