Försäkringskassan

Personuppgiftsbiträdesavtal

Bilaga 2 till Överenskommelse avseende
användning av Uppföljning Finsam

Personuppgiftsbiträdesavtal

1. Avtalsparter

Personuppgiftsansvarig:
Försäkringskassan
103 51 Stockholm
E-post: kundcenterpartner@forsakringskassan.se
Organisationsnummer: 202100-5521

Personuppgiftsbiträde

Organisationens namn	Organisationsnummer
Adress	
Postnummer	Postadress
E-post till kontaktpersonn	

2. Avtalets syfte och innehåll

Avtalet reglerar personuppgiftsbiträdets behandling av personuppgifter för Försäkringskassans räkning enligt enligt parternas Överenskommelse avseende användning av Uppföljning Finsam.

Avtalet har upprättats för att uppfylla de krav som framgår av artikel 28 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad EU:s dataskyddsförordning (GDPR).

Avtalet utgörs av detta avtal och Försäkringskassans bilaga med instruktioner för personuppgiftsbehandlingen m.m.

3. Definitioner

Med **Dataskyddslagstiftning** avses EU:s dataskyddsförordning och sådan kompletterande nationell lagstiftning i anslutning till dataskyddsförordningen som behandlingen av personuppgifter omfattas av. Dataskyddsrättsliga begrepp i detta avtal används med samma innebörd som i dataskyddslagstiftningen (GDPR).

Med **personuppgiftsansvarig** avses den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandling av personuppgifter.

Med **personuppgiftsbiträde** avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Med **personuppgifter** avses all information som direkt eller indirekt går att härleda till en identifierbar levande person.

Med **behandling av personuppgifter** avses varje åtgärd eller serie av åtgärder som vidtas i frågan om personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning, ändring, användning, utlämnande, spridning eller annat tillhandahållande av uppgifter, sammanställning, samkörning, blockering, utplåning eller förstöring.

Med **utplåna** avses att de aktuella personuppgifterna förstörs så att de inte kan återskapas.

Med **personuppgiftsincident** avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

4. Personuppgiftsansvarigs åtagande

Försäkringskassan är personuppgiftsansvarig för all behandling av personuppgifterna. Tillämpliga författningsbestämmelser för behandlingen finns i EU:s dataskyddsförordning, lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Personuppgiftsansvarig ska utan dröjsmål informera personuppgiftsbiträdet om förändringar i behandlingen vilka påverkar personuppgiftsbiträdets skyldigheter.

5. Personuppgiftsbiträdets åtagande

Personuppgiftsbiträdet garanterar att dennes verksamhet bedrivs på sätt som säkerställer att dataskyddslagstiftningens krav på lämpliga tekniska och organisatoriska åtgärder uppfylls och att den registrerades rättigheter, friheter och intressen skyddas. Personuppgiftsbiträdet garanterar vidare att det har tillräcklig kunskap och förfogar över tillräckliga resurser för att dataskyddslagstiftningens krav ska kunna tillgodoses.

Personuppgiftsbiträdet, och den som arbetar under personuppgiftsbiträdets ledning, får endast behandla personuppgifterna i enlighet med tillämpliga författningsbestämmelser, detta avtal och de instruktioner som Försäkringskassan lämnar. Personuppgiftsbiträdet ansvarar för att den som arbetar under personuppgiftsbiträdets ledning informeras om detta.

Om personuppgiftsbiträdet bedömer att de instruktioner som lämnats strider mot tillämplig dataskyddslagstiftning ska personuppgiftsbiträdet omedelbart informera Försäkringskassan om detta.

Om personuppgiftsbiträdet anser sig sakna tillräckliga instruktioner för personuppgiftsbehandlingen, ska personuppgiftsbiträdet utan dröjsmål informera Försäkringskassan om detta och invänta de instruktioner som Försäkringskassan bedömer vara nödvändiga.

Personuppgiftsbiträdet ska vara Försäkringskassan behjälplig genom lämpliga tekniska och organisatoriska åtgärder så att Försäkringskassan kan fullgöra sin skyldighet avseende de registrerades rättigheter i enlighet med kapitel III i EU:s dataskyddsförordning, t.ex. rätten till information, rättelse eller radering. Om det till personuppgiftsbiträdet kommer in en begäran från den registrerade om utövande av en sådan rättighet ska personuppgiftsbiträdet utan dröjsmål vidarebefordra begäran till Försäkringskassan.

Personuppgiftsbiträdet ska utan dröjsmål informera Försäkringskassan om eventuella kontakter med tillsynsmyndigheten som rör, eller kan vara av betydelse för, personuppgiftsbiträdets behandling av personuppgifter. Åtagandet gäller inte om biträdet är förbjudet att lämna den aktuella informationen enligt tvingande lagstiftning. Personuppgiftsbiträdet har inte rätt att företräda Försäkringskassan eller agera för dess räkning gentemot tillsynsmyndigheten

6. Säkerhetsåtgärder

Personuppgiftsbiträdet är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som följer av EU:s dataskyddsförordning och övrig dataskyddslagstiftning och detta avtal. Personuppgiftsbiträdet ska också vidta de särskilda säkerhetsåtgärder som framgår av instruktionerna för personuppgiftsbehandling i bilagan.

Personuppgiftsbiträdet ska även iaktta de instruktioner och andra föreskrifter om säkerhet som meddelas av behörig tillsynsmyndighet.

Personuppgiftsbiträdet ska informera Försäkringskassan om förändringar, förhållanden eller andra omständigheter som kan påverka vidtagna informationssäkerhetsåtgärder eller behovet av sådana skydd.

Personuppgiftsbiträdet ska omgående underrätta Försäkringskassan vid upptäckt av personuppgiftsincidenter. Underrättelsen ska innehålla den information som krävs för att Försäkringskassan ska kunna fullgöra sina skyldigheter vid personuppgiftsincidenter enligt EU:s dataskyddsförordning.

Personuppgiftsbiträdet ska i övrigt bistå Försäkringskassan med att fullgöra skyldigheter enligt dataskyddsförordningen avseende säkerhet för personuppgifter, konsekvensbedömning avseende dataskydd samt förhandssamråd. Detta ska ske med beaktande av typen av behandling som utförs enligt avtalet och den information som personuppgiftsbiträdet har att tillgå.

Kraven på säkerhetsåtgärder och säkerhetsnivåer är fastställda med utgångspunkt i av Försäkringskassan genomförd riskanalys och informationsklassning.

Försäkringskassan kan följa upp risker och säkerhetsklassning varje år och vid förändringar. Kraven på säkerhetsåtgärder och fastställda säkerhetsnivåer som gäller för personuppgiftsbiträdet kan förändras i samband med uppföljningen.

7. Underbiträden

Personuppgiftsbiträdet får inte utan Försäkringskassans skriftliga förhandstillstånd anlita ett annat personuppgiftsbiträde (underbiträde) för behandling av Försäkringskassans personuppgifter.

Om personuppgiftsbiträdet anlitar ett underbiträde ska ett skriftligt avtal mellan personuppgiftsbiträdet och underbiträdet träffas. I ett sådant avtal ska föreskrivas att underbiträdet har samma skyldigheter som personuppgiftsbiträdet har enligt detta avtal.

Försäkringskassan har i bilagan till detta avtal angivit vilka underbiträden som är godkända vid personuppgiftsbiträdesavtalets ikraftträdande.

Personuppgiftsbiträdet ska på Försäkringskassans begäran tillhandahålla kopia av de delar av personuppgiftsbiträdets avtal med underbiträdet som krävs för att utvisa att personuppgiftsbiträdet har uppfyllt sina åtaganden enligt detta personuppgiftsbiträdesavtal.

Personuppgiftsbiträdet ska föra en förteckning över vilka underbiträden som har anlitats. Av förteckningen ska det framgå i vilka länder underbiträdet behandlar personuppgifterna och vilka typer av behandlingar som underbiträdet utför. Personuppgiftsbiträdet ska vidare på Försäkringskassans begäran utan dröjsmål

tillhandahålla kontaktuppgifter till de underbiträden som behandlar personuppgifter.

8. Överföring av personuppgifter till tredje land

Personuppgiftsbiträdet har inte rätt att i något avseende behandla personuppgifter i tredje land utan uttryckligt skriftligt godkännande från Försäkringskassan.

9. Uppföljning av behandlingen (revision och besök)

Försäkringskassan har rätt att kontrollera att de säkerhetsrelaterade bestämmelserna i detta personuppgiftsbiträdesavtal följs och att behandlingen i övrigt uppfyller de krav som ställs i avtalet.

Vid en sådan kontroll kan Försäkringskassan komma att biträdas av en representant från tredje part. Personuppgiftsbiträdet ska ge Försäkringskassan tillgång till all nödvändig information samt möjliggöra och bidra till granskningen. Den som granskar personuppgiftsbiträdets verksamhet ska iaktta regler om sekretess för personuppgiftsbiträdets affärs- och driftsförhållanden.

10. Sekretess och tystnadsplikt

Personuppgiftsbiträdet, och den som arbetar under personuppgiftsbiträdets ledning, får inte muntligen, genom utlämnande av handling eller på något annat sätt för obehöriga röja de uppgifter som han eller hon tar del av i samband med behandlingen av personuppgifter i enlighet med detta avtal. De får inte heller själva använda eller utnyttja uppgifterna för egen del. Tystnadsplikten gäller även uppgifter om Försäkringskassans förhållanden som personuppgiftsbiträdet, och den som arbetar under personuppgiftsbiträdets ledning, får kännedom om i samband med uppdragets utförande.

Tystnadsplikten gäller även efter att avtalet har upphört att gälla.

Personuppgiftsbiträdet ska säkerställa att samtliga som arbetar under personuppgiftsbiträdets ledning informeras om och har åttagit sig att iaktta den tystnadsplikt som gäller enligt detta avtal.

Sekretess och tystnadsplikt enligt denna punkt hindrar inte att personuppgiftsbiträdet fullgör de skyldigheter som följer av tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400).

11. Ansvar för skada

Personuppgiftsbiträdet ska hålla Försäkringskassan skadelös i händelse av att skada som är hänförlig till personuppgiftsbiträdets behandling av personuppgifter i strid med detta avtal eller instruktion från Försäkringskassan.

12. Ändring av avtalet

Försäkringskassan får i den mån det behövs för att efterleva tillämplig dataskyddslagstiftning ändra innehållet i detta personuppgiftsbiträdesavtal. Ändringar ska dokumenteras i ett tilläggsavtal som ska undertecknas av båda parter.

13. Avtalets giltighetstid

Detta avtal träder i kraft vid undertecknandet och gäller så länge personuppgiftsbiträdet behandlar personuppgifter för Försäkringskassans räkning eller detta avtal ersätts med annat nytt avtal.

14. Tvist

Tvist angående tolkning eller tillämpning av detta avtal ska avgöras enligt svensk lag och huvudavtalets bestämmelse om tvist.

15. Underskrift

Detta avtal har upprättats i två (2) likalydande exemplar varav parterna tagit var sitt.

Part

Ort	Datum
Namnteckning (behörig företrädare)	
Namnförtydligande	

Försäkringskassan

Ort	Datum
Namnteckning (behörig företrädare)	
Namnförtydligande	

Bilaga till personuppgiftsbiträdesavtal

Denna bilaga innehåller instruktioner till personuppgiftsbiträdet samt uppgift om i vilka länder personuppgifterna behandlas och godkända underbiträden vid avtalets ikraftträdande.

Instruktioner för personuppgiftsbehandling

1. Registrerade

Personuppgifter som rör följande kategorier av registrerade får behandlas av personuppgiftsbiträdet: För- och efternamn för deltagaransvariga.

2. Typ av uppgifter som ska behandlas

De personuppgifter som får behandlas av personuppgiftsbiträdet är personuppgifter för deltagaransvarig i syfte att koppla hen till eller ifrån insats där hen har eller hade ett uppdrag.

3. Känsliga personuppgifter (i förekommande fall).

Behandlingen rör följande känsliga personuppgifter: Ej aktuellt.

4. Behandling

Personuppgifterna kommer att behandlas på följande sätt:
Medarbetare som arbetar för ett samordningsförbund med uppdrag att registrera uppgifter om samordningsförbundet i Uppföljning Finsam har rollen förbundsadministratör i Uppföljning Finsam. Förbundsadministratören har även till uppgift att utföra en personuppgiftsbehandling som består i att koppla deltagaransvariga till de insatser där de har sina uppdrag att registrera deltagare i insatserna.

5. Ändamål med behandlingen

Behandlingen av personuppgifterna sker i syfte att tilldela deltagaransvarig åtkomst för registrering av deltagare i de insatser där hen har ett uppdrag.

6. Särskilda instruktioner angående behandlingen

Vid behandlingen av personuppgifter ska personuppgiftsbiträdet särskilt beakta:

Information som hanteras i systemet får inte laddas ner, kopieras, spridas vidare eller i övrigt återges på något vis, utöver den information som erhålls genom nerladdningsbara rapporter som exponeras av systemet eller som publiceras av Försäkringskassan

7. Tekniska och organisatoriska säkerhetsåtgärder

Detta avsnitt utgör särskilda instruktioner till personuppgiftsbiträdet avseende tekniska och organisatoriska säkerhetsåtgärder, utöver vad som anges i avtalets avsnitt 6.

Personuppgiftsbiträde förbinder sig till att hantera systemet i enlighet med Överenskommelsen avseende användning av uppföljningssystemet Uppföljning Finsam och att inte låta någon utan tillbörlig behörighet få tillgång till uppgifterna i systemet.

Beskrivning av rutiner för

Behandling av personuppgifter inom Sverige, EU/EES eller tredje land

Inga personuppgifter ska överföras till tredje land.

Godkända underbiträden vid det här avtalets ikraftträdande

Inga underbiträden får anlitas.

Loggning

Användarnas aktiviteter i Uppföljning Finsam loggas av Försäkringskassan.