1 Avtal mellan personuppgiftsansvarig och personuppgiftsbiträde

Detta avtal är upprättat mellan nedanstående personuppgiftsansvarig samt nedanstående personuppgiftsbiträde som behandlar personuppgifter (i avtalet nedan sammantaget kallat Parterna) för personuppgiftsansvarigs räkning.

	Personuppgiftsansvarig	**Personuppgiftsbiträdet**
Namn:		Arbetshälsan Malung Sälen AB
Organisationsnummer:		556160-8067
Adress:		Moravägen 9 F, 782 31 Malung
Kontaktperson:		Björn Sjögren
E-postadress kontaktperson:		bjorn@arbetshalsan.se
Dataskyddsombud:		Björn Sjögren
E-postadress dataskyddsombud:		bjorn@arbetshalsan.se

Detta avtal utgör komplement till tecknat avtal avseende företagshälsovård, i detta avtal kallat Tjänsteavtalet, mellan personuppgiftsansvarig och personuppgiftsbiträde i rollerna som kund respektive leverantör.

1.1 Instruktioner

Personuppgiftsbiträdet behandlar personuppgifter för Personuppgiftsansvarig i enlighet med nedanstående tabell/tabeller.

Tabell 1 Beskrivning av personuppgiftsbehandling

Beskrivning av behandlingen	
Tjänst och ändamål med behandlingen:	Tjänst **Företagshälsa** inom ramen för Arbetshälsan Malung Sälens tjänste-katalog. Ändamål med behandlingen är att fullgöra det tjänsteavtal som ingåtts och möjliggöra kunds avrop av tjänster utifrån tjänstekatalogen.
Behandlingsaktiviteter:	**Bearbetning/Ändring** (av uppgifter införda i de system Personuppgifts-biträdet förvaltar) **Insamling** (vid kontroller, utredningar, friskvårdstjänster, sjuk/friskanmälan) **Lagring** (information i Företagsjournal, personregister av personuppgiftsansvariges anställda, register över behöriga användare) **Läsning** (vid friskvårdstjänster, kartläggningar, kontroller, undersökningar, utbildningar, sjuk/friskanmälan, utredningar; av information i Företagsjournal) **Radering** (efter avtalets slut eller vid annan överenskommelse med personuppgiftsansvarig) **Registrering** (vid friskvårdstjänster, kartläggningar, kontroller, sjuk/friskanmälningar, undersökningar, utbildningar, utredningar)
Kategorier av registrerade:	De vilka den Personuppgiftsansvarige avser omfattas av tjänsten.
Kategorier av personuppgifter:	Personnummer Namn Adress Telefonnummer E-postadress Arbetsplats och eventuell avdelning Uppgifter om hälsan inom ramen för sjuk/friskanmälan Uppgifter om hälsa inom ramen för utredningar och kontroller vilka utförs på uppdrag av den Personuppgiftsansvarige och som ej omfattas av sekretess av annan tillämplig lagstiftning.
Plats för behandling:	All behandling sker inom ramen för EU/EES
Lagringstid/gallringsfrist:	Personuppgifterna behandlas som längst fram till avtalets slut samt ytterligare 6 månader.

Säkerhetsåtgärder	
Fysisk åtkomst:	Inga personuppgifter hanteras eller bevaras regelmässigt på fysiska lagringsmedia, såsom papper. Endast behörig personal har fysisk åtkomst till servrar hos driftleverantör.
Åtkomst till system:	Endast behörig personal har åtkomst till de system som behövs för tjänsten.
Åtkomst till personuppgifter:	Endast behörig personal har åtkomst till personuppgifter. Behörighet styrs genom rolltilldelning baserad på arbetsuppgift.
Överföring av personuppgifter:	Överföring av personuppgifter sker ej till tredje land.
Behörighetsstyrning:	Behörighetsstyrning tillämpas utifrån användarroller för de IT-system där personuppgifter behandlas.
Kryptering av lagrat data:	Samtliga mobila arbetsstationer (mobiltelefoner, laptop-enheter) är krypterade.
Säker autentisering:	Programvara och system där personuppgifter hanteras nås enbart genom klienter inom Personuppgiftsbiträdets interna nätverk. Anslutning utifrån det fysiska interna nätverket är enbart möjligt genom 2-faktors autentisierad VPN.
Hantering av lagringsmedia:	Rutin för återlämning av lagringsmedia finns vid verksamheten.
Kapacitets- och kontinuitetsplanering:	Servrar, såväl front-end som bakomliggande databasservrar, är dimensionerade utifrån antalet användare och lastbalanserar. Samtliga servrar övervakas kontinuerligt. Säkerhetskopiering utförs schematiskt . Samtlig säkerhetskopiering kontrolleras och logg förs över lyckad/misslyckade aktiviteter. Test av återläsning sker schematiskt.
Separation av data (logisk/fysisk):	Logisk separation av data sker genom systemens rättighetssystem samt mellan servrar genom brandväggsregler.
Loggning:	Serveraktiviteter övervakas genom loggning av användning samt trafik. Aktivitet inom systemen som hanterar personuppgifter sker genom loggning av användaraktiviteter, så som inlogg, läsning samt ändring, i systemen.
Hantering av tekniska sårbarheter:	Servrar skyddas genom brandvägg, antivirus samt DNS-skydd. Säkerhetsuppdateringar hanteras manuellt och övervakas.
Redundans:	Servrarna är redundanta. Vid eventuella driftavbrott i front-end lyfts den felande servern ur och last balanseras till kvarvarande. Databasservrar nyttjar synkronisering samt failover genom en klusterlösning vilket medför redundans.
Dokumenterade driftrutiner:	Dokumenterade driftrutiner finns vid IT-avdelningen för servrar samt övrig IT-drift. Dokumenterade driftrutiner för system och programvara finns hos systemansvariga.
Oberoende granskning:	Inom ramen för certifieringsrevisioner samt uppföljande revisioner utifrån ISO 9001.

2 Innehåll och syfte

Detta avtal har upprättats för att uppfylla kraven på avtal mellan personuppgiftsansvarig och personuppgiftsbiträde i enlighet med artikel 28 i Dataskyddsförordningen (EU 2016/679).

3 Ansvar och instruktion

Den Personuppgiftsansvarige har ansvar för all behandling av personuppgifter som sker med anledning av Tjänsteavtalet.

Personuppgiftsbiträdet åtar sig att enbart behandla avtalade personuppgifter i enlighet med detta avtal, Tjänsteavtalet och den Personuppgiftsansvariges vid var tid meddelade dokumenterade instruktioner. Personuppgiftsbiträdet får inte behandla personuppgifterna som Personuppgiftsansvarig ansvarar för i något eget syfte jämte att tillhandahålla, underhålla och lämna support för leverans i enlighet med Tjänsteavtalet. Den Personuppgiftsansvarige ansvarar för att personuppgifter vilka ej omfattas av detta avtal, Tjänsteavtalet eller andra instruktioner inte behandlas inom ramen för tjänsten. Personuppgiftsbiträdet äger dock rätt att utan Personuppgiftsansvariges instruktion behandla personuppgifter om denna behandling krävs enligt unionsrätten eller enligt medlemsstat nationella rätt som Personuppgiftsbiträdet omfattas av, och i sådana fall skall Personuppgiftsbiträdet informera den Personuppgiftsansvarige om det rättsliga kravet innan uppgiften behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt.

Personuppgiftsbiträdet åtar sig vidare att behandla personuppgifterna enligt Dataskyddsförordningen, samt tillsynsmyndighetens, eller relevant EU-organs föreskrifter, ställningstaganden och rekommendationer på personuppgiftsområdet, nedan gemensamt benämnda ”Tillämplig lag”.

Personuppgiftsbiträdet får inte överföra några personuppgifter till land utanför EU/EES-området eller till land som inte omfattas av undantagen till förbud mot överföring till tredje land enligt Dataskyddsförordningen, utan att ha den Personuppgiftsansvariges skriftliga samtycke i förväg och ha säkerställt att sådan överföring sker i överensstämmelse med tillämplig lag.

För de fall Personuppgiftsbiträdet misstänker alternativt upptäcker säkerhetsöverträdelse så som obehörig åtkomst, förstörelse, ändring eller liknande av personuppgifter, eller om Personuppgiftsbiträdet av någon annan anledning inte kan uppfylla åtaganden i detta personuppgiftsbiträdesavtal, ska Personuppgiftsbiträdet omedelbart undersöka incidenten och vidta lämpliga åtgärder för att läka incidenten och förhindra upprepning, och tillhandahålla Personuppgiftsansvarig en beskrivning av incidenten. Personuppgiftsbiträdet skall utan onödigt dröjsmål, och senast inom 24 timmar, påbörja incidentrapportering till personuppgiftsansvarig.

Beskrivning av incidenten ska åtminstone:

- Beskriva personuppgiftsincidentens art inbegripet, om så möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgifter som berörs
- Förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas
- Beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
- Beskriva de åtgärder som personuppgiftsbiträdet har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella effekter.

Personuppgiftsbiträdet ska informera Personuppgiftsansvarige om Personuppgiftsbiträdet får kännedom om att personuppgifter behandlats i strid med Personuppgiftsansvariges instruktioner eller detta personuppgiftsbiträdesavtal.

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska Personuppgiftsbiträdet före behandlingen utförs vara Personuppgiftsansvarig behjälplig vid en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

4 Säkerhet och sekretess

Personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som åtminstone överensstämmer med Tillämplig lag och är lämplig med beaktande av:

- Vilka tekniska möjligheter som står till förfogande med beaktande av den senaste teknikutvecklingen
- Kostnaden som genomförandet medför
- Riskerna förknippade med personuppgiftsbehandlingen, med hänsyn tagen till bl.a.
    - Konsekvenserna av förlust av riktighet, konfidentialitet och tillgänglighet till personuppgifterna vid såväl lagring och informationsöverföring som vid andra behandlingsaktiviteter
    - Syftet med behandlingen i förhållande till riskerna
    - Hur känsliga personuppgifterna är för fysiska personers rättigheter och friheter
    - Mängden personuppgifter som behandlas
    - Utsattheten hos de kategorier av registrerade som personuppgifterna avser

Avtalade åtgärder, vilka uppfyller denna punkt, ska åstadkomma en säkerhetsnivå som Personuppgiftsansvarig efter samråd med personuppgiftsombudet/dataskyddsombudet bedömer lämplig.

Personuppgiftsbiträdet skall vid utformandet av lämpliga säkerhetsåtgärder beakta allmänt vedertagna principer för informationssäkerhet genom tillämpning av ISO/IEC 27001 eller motsvarande standard.

Personuppgiftsbiträdet ska regelbundet och systematiskt utvärdera verkan av de säkerhetsåtgärder som vidtas för att skydda personuppgiftsbehandlingen som utförs för personuppgiftsansvarigs räkning.

Personuppgiftsbiträdet skall omedelbart meddela Personuppgiftsansvarig i händelse av att säkerheten ej kan upprätthållas avseende personuppgiftsbehandlingen.

Samtliga ändringar av tekniska och organisatoriska åtgärder ska dokumenteras av Personuppgiftsbiträdet.

Åtgärderna som vidtas skall inkludera följande åtgärdsområden i enlighet med Dataskyddsförordningen:

- pseudonymisering och kryptering av personuppgifter
- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna
- förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Personuppgiftsbiträdet ska säkerställa att behörighetsstyrningen är korrekt och att konfidentialitet iakttas. Personuppgiftsbiträdet ska vidta de åtgärder som erfordras för att säkerställa att den mottagna informationen endast delges de personer inom den egna organisationen som berörs av ändamålet med Tjänsteavtalet. Personuppgiftsbiträdet ska tillse att samtliga anställda, konsulter, underleverantörer och övriga som Personuppgiftsbiträdet svarar för och som behandlar personuppgifterna är bundna av ett erforderligt sekretessåtagande samt att de är informerade om hur behandling av personuppgifterna får ske. Personuppgiftsbiträdet ansvarar för att de personer som har åtkomst till personuppgifterna är informerade och hur de får behandla personuppgifterna i enlighet med instruktioner från Personuppgiftsansvarig.

5 Personuppgiftsansvarigs rätt till granskning av personuppgiftsbiträde

Personuppgiftsansvarige äger rätt att själv eller genom tredje man, genomföra revision gentemot Personuppgiftsbiträdet eller på annat sätt kontrollera att Personuppgiftsbiträdets behandling av personuppgifter följer detta personuppgiftsbiträdesavtal. Vid sådan revision eller kontroll ska Personuppgiftsbiträdet ge Personuppgiftsansvarige den assistans som behövs för genomförande av revision.

Personuppgiftsbiträdet ska på begäran av Personuppgiftsansvarige tillhandahålla all tillgänglig information avseende behandlingen av personuppgifter för att Personuppgiftsansvarige ska kunna uppfylla sina skyldigheter som personuppgiftsansvarig enligt Tillämplig lag.

För de fall registrerade personer, tillsynsmyndigheten eller annan tredje man begär information från Personuppgiftsansvarige eller Personuppgiftsbiträdet rörande behandlingen av personuppgifter ska Parterna samverka och utbyta information i nödvändig utsträckning. Personuppgiftsbiträdet får inte lämna ut personuppgifter eller information om behandlingen av personuppgifter utan medgivande i förväg från Personuppgiftsansvarig utom för det fall föreläggande finns därom från relevant myndighet eller om Personuppgiftsbiträdet är nödgad därtill enligt tvingande lagstiftning.

Personuppgiftsbiträdet ska vara Personuppgiftsansvarig behjälplig genom lämpliga tekniska och organisatoriska åtgärder, så att Personuppgiftsansvarig kan fullgöra sin skyldighet avseende de registrerades rättigheter i enlighet med kapitel III i Dataskyddsförordningen.

6 Anlitande av underbiträde

Personuppgiftsbiträde har rätt att anlita underbiträden för att leverera tjänst i enlighet med Tjänsteavtalet.

Om Personuppgiftsbiträdet anlitar underbiträde enligt villkoren i Tjänsteavtalet, har Personuppgiftsbiträdet mandat och skyldighet att ingå särskilt personuppgiftsbiträdesavtal med sådant underbiträde vad avser underbiträdets behandling av personuppgifter. I sådant avtal ska föreskrivas att underbiträdet har motsvarande skyldigheter som Personuppgiftsbiträdet har enligt detta personuppgiftsbiträdesavtal. Om underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd skall Personuppgiftsbiträdet vara fullt ansvarig gentemot den Personuppgiftsansvariga för utförandet av underbiträdets skyldigheter.

Personuppgiftsbiträdet ska på Personuppgiftsansvariges begäran tillhandahålla kopia av de delar av Personuppgiftsbiträdets avtal med underbiträde som krävs för att utvisa att Personuppgiftsbiträdet uppfyllt sina åtaganden enligt detta personuppgiftsbiträdesavtal.

Personuppgiftsbiträdet ska vid var tid föra en korrekt och uppdaterad lista utvisande vilka underbiträden som anlitats för behandlingen av personuppgifter och var dessa är geografiskt belägna. Personuppgiftsbiträdet ska vidare på Personuppgiftsansvariges begäran utan dröjsmål tillhandahålla kontaktuppgifter till de underbiträden som behandlar personuppgifter.

7 Tvist, tillämplig lag och skadestånd

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

I händelse av att Personuppgiftsansvarig blir ersättningsskyldig gentemot tredje man till följd av Personuppgiftsbiträdets bristande efterlevnad av detta avtal eller Tjänsteavtalet skall Personuppgiftsansvarig hållas skadelös genom att Personuppgiftsbiträde till fullo ersätter Personuppgiftsansvarig för den skada som uppstått.

8 Avtalets ikraftträdande, upphörande, ändringar och överlåtelse

Detta personuppgiftsbiträdesavtal träder i kraft när det undertecknats av båda Parter och gäller därefter mellan Parterna så länge Personuppgiftsbiträdet behandlar Personuppgifter för den Personuppgiftsansvarige i enlighet med Tjänsteavtalet. Detta personuppgiftsbiträdesavtal upphör automatiskt att gälla utan föregående uppsägning 6 månader efter att Tjänsteavtalet upphör att gälla. Under perioden efter Tjänsteavtalets upphörande begränsas Personuppgiftsbiträdets behandling till lagring samt radering.

Ändringar och tillägg till detta avtal ska, för att vara giltiga, göras skriftligen och undertecknas av båda Parter. Sådana ändringar och tillägg till avtalet träder i kraft efter båda Parters undertecknande om inget annat är överenskommet. Denna punkt förhindrar inte att Personuppgiftsansvarig kan ändra eller utfärda ytterligare instruktioner i enlighet med vad som framgår av detta avtal.

Överlåtelse av detta personuppgiftsbiträdesavtal får ske i enlighet med bestämmelserna för överlåtelse i Tjänsteavtalet och endast i samband med överlåtelse av Tjänsteavtalet.

Detta avtal har upprättats i var sitt exemplar för Personuppgiftsansvarig respektive Personuppgiftsbiträde.

För Personuppgiftsansvarig:

_____

Namnförtydligande

För Personuppgiftsbiträde:

_____

Björn Sjögren, VD
Namnförtydligande
Malung 2018-05-25